HACKING COUNTERMEASURE FRAMEWORK FOR OMAN COMPUTER EMERGENCY READINESS TEAM USING DELPHI APPROACH

SAID BIN KHALFAN BIN SAID AL-WAHAIBI

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

JUNE 2022

DEDICATION

To my beloved parents and family

ACKNOWLEDGEMENT

I would like to thank the individuals who supported this challenging work. Certainly, the success of this study would not have been possible without the valuable input, feedback and support from Assoc. Prof. Dr. Norafida Binti Ithnin and Prof. Dr. Othman bin Ibrahim. I would like to extend my thanks to Prof. Ali Al-Badi, Prof. Saqib Ali, Assoc. Prof. Haitham Al-Synani from Sultan Quaboos University, Prof. Dr. Ahmed Al-Nomani and Prof. Dr. Joseph Mani from the College of Business and Sciences for their continuous support throughout this research work. Also, I would like to thank Dr. Salim Al-Ruzaiki the Head of Information Technology Authority Oman, Eng. Bader Al-Salehi the General Director Oman CERT, Dr. Amirudin bin Abdul Wahab the CEO Cyber Security Malaysia, Dr. Ankit Fadia cyber security expert and author of best-selling cyber security books, and Eng. Ruhama M. Zain the cyber security expert at Cyber Security Malaysia for reviewing this research. Moreover, I would like to thank Assoc. Prof. Abdullah Abukishik, Assoc. Prof. Atta ur Rehman Khan from Sohar University and Prof. Basant Komar from the College of Business and Sciences for validating research instruments. In addition, I would like to thank UTM staff for validation of this work, especially Prof. Abdul Samed the Dean of School of Computing, Dr. Mehrbakhsh Nilashi and Mrs. Nizamra Binti Masdar. Thank you all for your special effort.

ABSTRACT

Recent security attacks have breached some of the most secure networks around the world causing damages, stealing information, and data corruption. This devastating situation has led security experts to question the effectiveness and reliability of the present security controls against the hacking attacks. Thus, there is a need to prevent systems hacking and fulfil managerial concerns about security risks. This research focuses on the design and development of Hacking Countermeasure Framework (HCF) using Delphi method that combines quantitative and qualitative research questionnaires to address problems associated with the lack of hacking anticipation, hiding and deception, and Defense-in-Breadth (DiB) techniques. This research was conducted via an online, anonymous, and asynchronous six-round Delphi methodology adapted from the classical Delphi method with a pre-selected security experts panel. The study was arranged in four Delphi phases. Phase one covers analysis of studies that have used pre-Delphi to explore hacking threats and the provided recommendations for anti-hacking. Phase two covers derivation of factors for identifying anti-hacking factors and their relationships. Phase three covers development of a framework to prevent systems hacking and fulfil managerial concerns regarding security risks. Finally, phase four covers validation of the research deliverables using triangulation with five processes, namely study cases, interviews, discussion workshop, review and quality assurance by cyber security experts, and approval by CERTs. The findings of this research confirms the importance of hacking anticipation, hiding and deception, and DiB in a hacking countermeasure process and provides enticing clues regarding the role of these three factors in the hacking countermeasures. Despite recent calls for the replacement of Defense-in-Depth (DiD), this research also confirms that DiD plays a vital role in anti-hacking processes. Moreover, a clear linkage is identified between hacking risk assessment, anti-hacking auditing, and anti-hacking compliance. Furthermore, the validation of framework confirms that hacking countermeasure improves through the induced solutions for DiB, and deception and hiding techniques. The HCF is useful for both academia and industry and can contribute to theory and practice of hacking anticipation, DiB, and hiding and deception..

ABSTRAK

Serangan keselamatan baru-baru ini telah memusnahkan beberapa rangkaian paling selamat di seluruh dunia yang menyebabkan kerosakan, kecurian maklumat, dan rasuah data. Keadaan yang sukar ini telah menyebabkan pakar keselamatan mempersoalkan keberkesanan dan kebolehpercayaan kawalan keselamatan sekarang terhadap serangan penggodaman. Oleh itu, terdapat keperluan untuk mencegah sistem penggodaman dan memenuhi keprihatinan pengurusan tentang risiko keselamatan. Penyelidikan ini memberi tumpuan kepada reka bentuk dan pembangunan rangka kerja tindak balas penggodam menggunakan kaedah Delphi yang menggabungkan soal selidik penyelidikan kuantitatif dan kualitatif untuk menangani masalah yang berkaitan dengan kekurangan jangkaan penggodaman, persembunyian dan penipuan, dan teknik Pertahanan-Meluas (DiB). Penyelidikan ini dijalankan melalui metodologi Delphi enam pusingan secara dalam talian, tanpa nama dan tak segerak yang diadaptasi daripada kaedah Delphi klasik yang telah digunakan oleh pakar keselamatan sebelum ini. Penyelidikan ini terdiri daripada empat fasa Delphi. Fasa satu meliputi analisis kajian yang telah menggunakan pra-Delphi untuk meneroka ancaman penggodaman dan pengesyoran yang disediakan untuk anti-penggodaman. Fasa dua meliputi terbitan faktor untuk mengenal pasti faktor anti-penggodaman dan hubungannya. Fasa tiga meliputi pembangunan rangka kerja untuk mencegah penggodaman sistem dan memenuhi kebimbangan pengurusan mengenai risiko keselamatan. Akhir sekali, fasa empat meliputi pengesahan hasil penyelidikan menggunakan triangulasi dengan lima proses, iaitu kes kajian, temu bual, bengkel perbincangan, semakan dan jaminan kualiti oleh pakar keselamatan siber, dan kelulusan oleh CERT. Penemuan penyelidikan ini mengesahkan kepentingan jangkaan penggodaman, persembunyian dan penipuan, dan DiB dalam proses tindakan balas penggodaman serta memberikan petunjuk menarik mengenai peranan ketiga-tiga komponen ini dalam tindakan balas penggodaman. Walaupun terdapat cadangan untuk menggantikan Pertahanan-Mendalam (DiD), penyelidikan ini telah mengesahkan bahawa DiD memainkan peranan penting dalam proses anti-penggodaman. Selain itu, kaitan yang jelas dikenal pasti antara penilaian risiko penggodaman, pengauditan anti-penggodaman dan pematuhan anti-penggodaman. Tambahan pula, pengesahan rangka kerja mengesahkan bahawa tindakan balas penggodaman bertambah baik melalui penyelesaian teraruh untuk DiB, dan teknik penipuan dan penyembunyian. Rangka kerja yang dibangunkan ini berguna untuk kedua-dua akademia dan industri dan boleh menyumbang kepada teori dan amalan jangkaan penggodaman, DiB, dan persembunyian dan penipuan.

TABLE OF CONTENTS

TITLE			PAGE
	DECLARATION		**iii**
	DEDICATION		**iv**
	ACKNOWLEDGEMENT		**v**
	ABSTRACT		**vi**
	ABSTRAK		**vii**
	TABLE OF CONTENTS		**viii**
	LIST OF TABLES		**xiii**
	LIST OF FIGURES		**xvii**
	LIST OF ABBREVIATIONS		**xx**
	LIST OF APPENDICES		**xxiii**
CHAPTER 1	**INTRODUCTION**		**1**
1.1	Introduction		1
1.2	Problem Background		7
	1.2.1	Missing anti-hacking factors addressing susceptibility to hacking risks	13
	1.2.2	Missing anti-hacking relationships that close hacking gaps	15
	1.2.3	Missing framework structures that prevent systems' hacking	19
1.3	Statement of problem		22
1.4	The research motivation		25
1.5	The aim of the research		25
1.6	Objectives of the study		26
1.7	Scope of the study		27
1.8	Significance of the study		28
1.9	Thesis organization		29
1.10	Summary		30

CHAPTER 2	**LITERATURE REVIEW**	**31**
2.1	Introduction	31
2.2	Hacking	31
2.3	Hacking countermeasure	35
	2.3.1 Information security standards and compliances	36
	2.3.1.1 Information security standards	36
	2.3.1.2 Information security compliances	38
	2.3.2 Defense-in-Depth frameworks	41
2.4	Research gap in existing standards and defense-in-depth	52
2.5	Hacking countermeasure factors	56
	2.5.1 Awareness/knowledge of systems & local systems risk	59
	2.5.1.1 Hacking anticipation	60
	2.5.1.2 Hacking steps characteristics	68
	2.5.1.3 The hack back action	71
	2.5.2 Existing actions taken to effectively secure systems	73
	2.5.2.1 Defense-in-Depth (DID)	74
	2.5.2.2 Defense-in- Breadth (DIB)	76
	2.5.2.3 Hiding and Deception	81
	2.5.2.3.1 Obfuscating the source-destination nodes	83
	2.5.2.3.2 Honeypots	86
	2.5.2.3.2 Hiding and deception outcome summary	87
	2.5.2.4 Anti-hacking incident management and event handling	88
	2.5.3 Industry susceptibility to hacking risk	93
	2.5.4 Summary literature review for hacking countermeasure	94
2.6	Framework design	99
2.7	Research approach	101

2.8	Summary	106
CHAPTER 3	**RESEARCH METHODOLOGY**	**109**
3.1	Introduction	109
3.2	Selected research methodology	109
3.3	Research design and operational framework	111
	3.3.1 Phase one building nature of reality and knowledge	116
	3.3.2 Phase two deriving factors relationships	119
	3.3.3 Phase three derivation of framework guide	120
	3.3.4 Phase four research documentation, verification & generalization	122
	3.3.5 Research deliverables	124
3.4	Research sample and data gathering techniques	109
	3.4.1 Problem identification and study approach design	129
	3.4.2 Selecting participants and preparing Delphi surveys	131
	3.4.3 Data collection instrumentations and analyzing meeting requirements	136
3.5	Assessment of validity and reliability	137
	3.5.1 Validity and reliability for quantitative data	138
	3.5.2 Validity and reliability for qualitative data	142
	3.5.3 Validity and reliability for hybrid method	143
	3.5.4 Validity and reliability of Delphi method	147
3.6	Summary	152
CHAPTER 4	**DEVELOPMENT OF HACKING COUNTERMEASURE FRAMEWORK**	**155**
4.1	Introduction	155
4.2	Phase one building nature of reality and knowledge	156
4.3	Phase two deriving factors relationships	158
	4.3.1 Delphi round-1 for deriving hacking countermeasure factors	160
	4.3.2 Delphi round-2 for deriving tactics taken to effectively secure systems	167

4.3.2.1 Deriving tactics related to Defense-in-Depth 168
4.3.2.2 Deriving tactics related to Defense-in-Breadth 170
4.3.2.3 Deriving tactics related to hiding and deception 172
4.3.2.4 Deriving tactics related to anti-hacking Incident management 173
4.3.3 Delphi round-3 for deriving tactics related to susceptibility to industry risk 175
4.3.3.1 Deriving tactics related to hacking risks assessment 175
4.3.3.2 Deriving tactics related to anti-hacking auditing 177
4.3.3.3 Deriving tactics related to anti-hacking compliance 178
4.4 Phase three derivation of framework guide 180
4.4.1 Delphi round-4 for deriving countermeasures relationships to the hacking steps 181
4.4.2 Delphi round-5 for developing the final framework model 184
4.4.3 Delphi round-6 for verifying the hacking countermeasure framework model 189
4.4.4 Derivation of framework modules 194
4.4.5 Integrating deliverables from Delphi round-5 into the modules 195
4.4.6 Development of auditing procedures and anti-hacking cheat sheets 197
4.5 Summary 201

CHAPTER 5 RESEARCH VALIDATIONS AND RESULTS ANALYSIS 203
5.1 Introduction 203
5.2 The research validations case study 204
5.2.1 Part A: Validation of framework model 205
5.2.2 Part B: Validation of the hacking countermeasure framework-1 211

5.2.3 Part C: Validation of the hacking countermeasure framework-2 215
5.2.4 Part D: Feedback for future development 221
5.2.5 Analysis summary 223
5.3 Comparison HCF with existing infosec frameworks 227
5.4 Research discussion workshop 229
5.5 Cyber security experts judgments and testimonials 229
5.6 Framework approval by CERTs 231
5.7 Research validity and reliability assessment 232
5.8 Findings 237
5.9 Summary 239

CHAPTER 6 CONCLUSION 239
6.1 Achievements 239
6.2 Discussion and future developments 245
6.3 Research contribution and impact 250
6.4 Future developments 253

REFERENCES 239

LIST OF TABLES

TABLE NO.	TITLE	PAGE
Table 2.1	PCI Principles, Requirements, and Milestone and Goals	40
Table 2.2	Features of Sample Infosec Frameworks	45
Table 2.3	Defense-In-Depth Frameworks Summary Limitations-1	51
Table 2.4	Defense-In-Depth Frameworks Summary Limitations-2	51
Table 2.5	Research Gap within Existing Frameworks-1	53
Table 2.6	Research Gap within Existing Frameworks-2	53
Table 2.7	Outcome Deliverables from the Initial Survey	54
Table 2.8	The Hacking Steps Representing Hacking Anticipation	68
Table 2.9	Hacking Attacks Action for Sample Top Most Attacks	70
Table 2.10	The Hacking Tools	72
Table 2.11	Sample Items for Hacking Anticipation Variable	72
Table 2.12	Defense-in-Depth Tools and Techniques	75
Table 2.13	Table of Identified Variables in the Literature	95
Table 2.14	Table of Identified Variables and Measures	98
Table 2.15	Information Security Frameworks Types	100
Table 2.16	Framework Architecture	101
Table 3.1	Research Plan Using Delphi Methods	114
Table 3.2	Plan for Research Deliverables	124
Table 3.3	Sample PhD Dissertations and IS/IT Studies Using the Delphi Method	133
Table 3.4	Hybrid Method Inference Quality	147
Table 3.5	Participated Research Sample	149
Table 4.1	Pre-Delphi Results	157
Table 4.2	Delphi Round-1 Outcome Summary for Derived Hacking Countermeasure Factors	162
Table 4.3	Delphi Round-1 Outcome Summary of Derived Defense Layers in Defense-in-Depth	163

Table 4.4	Delphi Round-1 Outcome Summary on Deriving Hacking Steps	165
Table 4.5	Delphi Round-2 Outcome Summary on Defense-in-Depth (DiD)	169
Table 4.6	Delphi Round-2 Outcome Summary on Defense-in-Breadth (DiB)	171
Table 4.7	Delphi Round-2 Outcome Summary on Hiding and Deception	172
Table 4.8	Delphi Round-2 Outcome Summary on Incident Management and Event Handling	173
Table 4.9	Delphi Round-3 Outcome Summary on Hacking Risk Assessment	176
Table 4.10	Delphi Round-3 Outcome Summary on Anti-hacking Auditing	177
Table 4.11	Delphi Round-3 Outcome Summary on Anti-hacking Compliance	179
Table 4.12	Result of Delphi Round-4 Relationship of Hacking Countermeasure Factors to the Hacking Steps	182
Table 4.13	Descriptive Analysis for Delphi Round-4 Results	183
Table 4.14	Delphi Round-5 Outcome Summary on Relationships of the Derived Anti-hacking Tactics to Hacking Steps (AWindow of Derived Defense-In-Depth Tactics for Gaining Access Hacking Step)	185
Table 4.15	Table Summary of Derived Defense Tactics in Delphi Round-5	186
Table 4.16	Delphi Round-6 Outcome Summary on Verifying the Hacking Countermeasure Framework Model	190
Table 4.17	Derivation of Auditing Procedure from Delphi Round-5	198
Table 5.1	Case Study (a1) Results	206
Table 5.2	Case Study (a2) Results	207
Table 5.3	Case Study (a3) Results	209
Table 5.4	Case Study Validation Process (Summary of Part A)	210
Table 5.5	Case Study (b1) Results	211
Table 5.6	Case Study (b2) Results	212
Table 5.7	Case Study (b3) Results	213

Table 5.8	Case Study Validation Process (Summary of Part B)	215
Table 5.9	Case Study (c1) Results	216
Table 5.10	Case Study (c2) Results	217
Table 5.11	Case Study (c3) Results	218
Table 5.12	Case Study (c4) Results	219
Table 5.13	Case Study Validation Process (Summary of Part C)	221
Table 5.14	Final Case Study Descriptive Statistics-1	224
Table 5.15	Final Case Study Descriptive Statistics-2	225
Table 5.16	Summary for the Case Study Validation Process	226
Table 5.17	Comparison of HCF to Existing Frameworks-1	227
Table 5.18	Comparison of HCF to Existing Frameworks-2	228
Table 5.19	Research Validity and Reliability Summary	235
Table 5.17	Comparison of HCF to Existing Frameworks-1	227
Table A-1	Sample Hacking Incidents in 2020 and 2021	339
Table A-2	Hacking Generations	344
Table A-3	Items for Hacking Anticipation	345
Table A-4	Sample Items for Defense-in-Depth	349
Table A-5	Items for Defense-in-Breadth	351
Table A-6	Items for Hiding and Deception	352
Table A-7	Sample Items for Anti-hacking Incident Management and Event Handling	354
Table A-8	Sample Items for Hacking Risk Assessment	357
Table A-9	Sample Items for Anti-hacking Auditing and Penetration Testing	358
Table A-10	Sample Items for Anti-hacking Compliance	361
Table A-11	Items for Verification of the Framework model	362
Table A-12	Items for Case Studies for Verification of the Hacking Countermeasure Framework	362
Table C-1	Case Study Questionnaire Responses (Part A)	411
Table C-2	Case Study Questionnaire Responses (Part B)	412

Table C-3	Case Study Questionnaire Responses (Part C)	413
Table C-4	Case Study Questionnaire Responses (Part D).	415
Table C-5	Summary Responses of the Interview Survey for the Final Research Validation	417

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
Figure 2.1	ISO/IEC 27002:2013 (ISO/IEC, 2021b)	37
Figure 2.2	Common Modules in Existing Frameworks	48
Figure 2.3	Missing Factors in Existing Frameworks	54
Figure 2.4	Research Model in Straub and Welke (1998)	59
Figure 2.5	Hacking Anticipation Model as Given by McClure et al. (2012)	64
Figure 2.6	Cyber Kill-Chain Model as Given by Dell SecureWorks (2014)	66
Figure 2.7	Research Theoretical Model Through the Lenses of the Model of Systems Risk from Straub and Welke (1998)	97
Figure 3.1	Three-Round Delphi Process Adopted from Skulmoski et al. (2007)	110
Figure 3.2	Research Conceptual Framework	111
Figure 3.3	Research Operational Framework (Adapted from Skulmoski et al. (2007))	116
Figure 3.4	Research Literature Review for Building Nature of Reality and Knowledge	118
Figure 3.6	Research Activities for the Derivation of Framework Guid	122
Figure 3.6	Research Communicative and Pragmatic Validation	123
Figure 4.1	Mind-Map for Coding Deliverables in Phases Two and Three	159
Figure 4.2	The Basic Framework with Initial Factors	159
Figure 4.3	The Derived Countermeasure Factors from Delphi Round-1	164
Figure 4.4	The Basic Framework Updated With Delphi Round-1 Findings-1	164
Figure 4.5	Comparative Graphs for the Hacking Steps from Delphi Round-1	165
Figure 4.6	The Basic Framework Architecture Updated With Delphi Round-1 Findings-2	166

Figure 4.7	The Framework Architecture	167
Figure 4.8	Consensus for Defense-in-Depth Factor	170
Figure 4.9	Consensus for Defense-in-Breadth Factor	171
Figure 4.10	Consensus for Hiding & Deception Factor	173
Figure 4.11	Consensus for Incident Management and Event Handling Factor	174
Figure 4.12	Consensus for Hacking Risk Assessment Factor	177
Figure 4.13	Consensus for Anti-hacking Auditing	178
Figure 4.14	Consensus for Anti-hacking Compliance Factor	180
Figure 4.15	The Framework Architecture With Factors Mapping	183
Figure 4.16	Results for Derived Defense Tactics from Delphi Round-5	187
Figure 4.17	The Framework Architecture With Modules Representation	187
Figure 4.18	Hacking Countermeasure Framework Model	188
Figure 4.19	Hacking Countermeasure Framework Model–Single Hacking Step	189
Figure 4.20	Summary for the Framework model in Delphi Round-6	191
Figure 4.21	Hacking Countermeasure Framework Integrity	192
Figure 4.22	Operational Concept of the Framework Model	193
Figure 4.23	The Framework Modules	195
Figure 4.24	Document Mapping for the Hacking Countermeasure Framework	196
Figure 4.25	Hacking Countermeasure Framework (Sample Page 1 from 48)	197
Figure 4.26	Results Graphical Comparison for Auditing Procedures	199
Figure 4.27	Screen Shots of Google Survey Tool for the Delphi Questionnaires	199
Figure 4.28	Security Auditing Anti-Hacking Cheat Sheet (Image of a Sample Page 1 from 27)	200
Figure 5.1	Existing Frameworks Main Modules and the Newly Introduced Hacking Countermeasures	228
Figure 5.2	Research Quality Approval by the Cyber Security Expert Ankit Fadia	230

Figure 5.3 Research Practicality and Efficiency Approval by Malaysia CERT 231

Figure 5.4 Research Practicality and Efficiency Approval by the Oman CERT 232

LIST OF ABBREVIATIONS

ACL	-	Access Control List
AES	-	Advanced Encryption Standard
ANONYRING	-	Using anonymous ring
AODV	-	Ad-hoc On Demand Distance Vector
API	-	Application Programming Interface
AS	-	Authentication Server
AV	-	Anti-Virus system
BS	-	British Standard
CGI	-	Common Gate Interface
C-I-A	-	Confidentiality, Integrity and Availability
CobiT	-	Control Objectives for Information and related Technology
COSO	-	Committee of Sponsoring Organizations
CPM	-	Change-Point Monitoring
CSRF	-	Cross Site Request Forgery
CUSUM	-	Cumulative Sum
DES	-	Data Encryption Standard
DID	-	Defense-in-Depth
DIB	-	Defense-in-Breadth
DNT	-	Do-Not-Track
DOS	-	Denial of Service
DDOS	-	Distributed Denial of Service
DSP	-	Digital Signal Processing
ES_PIPE	-	Efficient Secure Pipe
FSNSs	-	Facebook-style Social Network Systems
FSMO	-	Flexible Single Master Operator
FW	-	Firewall
GEO-RBAC	-	Geographic – Role Based Access Control
GLBA	-	Gramm-Leach-Bliley
HABE	-	Hierarchical Attribute-Based Encryption

HCF	-	Hacking Countermeasure Framework
HIDS	-	Host-based Intrusion Detection Systems
HTTPS	-	Hypertext Transfer Protocol Secure
IBE	-	Identity Based Encryption
IDM	-	Identity Management
IDS	-	Intrusion Detection System
Infosec	-	Information Security
IPACF	-	Identity-Based Privacy-Protected Access Control Filter
IPS	-	Intrusion Prevention System
ISMS	-	Information Security Management System
ISN	-	Initial Sequence Numbers
ISO/IEC	-	International Organization for Standardization (ISO) and by the International Electro technical Commission
ITiL	-	Information Technology Infrastructure Library
ITM	-	Internet Threat Monitoring
LAP	-	Lightweight Anonymity and Privacy
MANET	-	Mobile Ad Hoc Network
MD5/MD7	-	Message Digest
NAT	-	Network Address Translation
NMAP	-	Network Mapper
PCI DSS	-	Payment Card Industry Data Security Standard
PDCA	-	Plan-Do-Check-Act
POPA	-	Principle Of Privilege Attenuation
OCERT	-	Oman Computer Emergency Readiness Team
QSR	-	Qualitative Statistical Research package (NVivo 11™)
PTSW	-	Password-Transaction Secure Window
RED	-	Randomized, Efficient, and Distributed (RED) protocol
RFID	-	Radio Frequency Identification
RSA	-	Rivest-Shamir-Adleman
RTT	-	Round Trip Time
SDLC	-	System Development Life Cycle
SECLOUD	-	Source and destination SEClusion using CLOUDs
SET	-	Secure Electronic Transfer

SHA	-	Secure Hash Algorithm
SIEM	-	Security Incident and Event Manager
SOX	-	Sarbanes-Oxley
SPF	-	Sender Policy Framework
SPSS	-	Statistical Package for the Social Sciences
SSH	-	Secure Shell
SSL	-	Secure Sockets Layer
TLS	-	Transport Layer Security
TOCTTOU	-	Time-Of-Check-To-Time-Of-Use)
Tor	-	The Onion Router
VPN	-	Virtual Private Network
WEP	-	Wired Equivalent Privacy
WPA	-	Wi-Fi Protected Access
XACML	-	eXtensible Access Control Mark-up Language

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
Appendix A	Definitions and Previous Studies	339
Appendix B	Delphi Questionnaires	363
Appendix C	Study Case and Documents for Final Research Validation	403
Appendix D	Sample Data Collection	422

CHAPTER 1

INTRODUCTION

1.1 Introduction

Public and private sector operations and daily work are automated into e-government or e-business environment like telemedicine, aeronautics, land and railway and teleworking including criminal records tracking and checking social security (Toapanta *et al.*, 2020). Economy also depends on the web, for example, banks transactions to and from financial departments are done electronically in hundreds of billions of US dollars per day, and trillions of US dollars are sent daily worldwide via electronic transfer (Serror *et al.*, 2021). Defense sector is heavily dependent on information systems too, starting from voice over IP communications, transmitting military sensitive information regarding all types of logistics, precision weapons guidance systems, nuclear power, to securities transactions, aerospace and much more (Al-Qutayri *et al.*, 2010; Christina, 2011; Toapanta *et al.*, 2020). The problem here is these information systems are insecure and susceptible to hacking, and these services have been facing continuing destructive hacking attacks over the years (Satish *et al.*, 2007; Levy, 2010; Saha *et al.*, 2021). Michelle (2010), Nunna and Marapareddy (2020) and Yonemura *et al.* (2021) announce that all government departments and agencies whether civil or military are facing increasing destructive hacking attacks, and threatened to be closed down at any time.

Around 66% of organizations are breached they remain unaware for months (Verizon, 2014). The security attacks continue to escalate world-wide making it very hard to detect or prevent (Masters, 2015; Olenick, 2015). According to Lazarte (2016), the number of complaints related to internet breaches in the United Kingdom alone has acceded 2000% in the past three years. Irwin (2021) reported 84 incidents in August 2021 that account for 61 million records breach, in addition to the mobile network hack, which affected 53 million customers and 40 million records. According to

Privacyrights (2017), the top most frequent cause of data breaches is hacking attacks, and among 41% of the total breaches, 37% attacks are generated from within the organization. In 2017, CynoSure Prime (2017) reported that 320 million hashes have been exposed. In addition, the attacks get repeated in a variety of ways and reside in systems unnoticeably causing losses in billions of US dollars (IBM, 2021; Masters, 2017). According to Shackleford (2016), this issue is becoming worse with the increase of sophisticated attacks, making it vital to develop new models that can predict attackers' behavior.

Heubl (2019) stated that it is simple to hack web-connected Internet of Things devices and critical infrastructure. In 2020, Bajak (2020) confirmed that millions of smart devices are vulnerable to hacking. Purple Security (2021) reported that hacking using ransomware worldwide rose 350% in 2018, and new victims will be every 11 seconds with estimated annual cost of $6 trillion, also 70% of organizations say that security risk increased significantly, and 69% of organizations don't believe the threats can be blocked by their protection systems. In fact, 61% of organizations have experienced hacking incidents. The education industry is ranked last in cyber security preparedness out of 17 major industries. However, 41% of higher education cyber security incidents and breaches were caused by social engineering attacks and 43% have had student data attacked, including dissertation materials and exam results, whereas 25% have experienced critical intellectual property theft, and 28% have had grant holder research data attacked. Also, 87% have experienced at least one successful hacking attack, and 83% believe hacking attacks are increasing in frequency and sophistication. 79% universities have experienced damage to reputation, almost 74% have had to halt a valuable research project as a result of a hacking attack, and 77% also say a hacker breach has the potential to impact national security, due to the potentially sensitive nature of the information which could been compromised. 64% don't believe their existing IT infrastructure will protect them against hacking attacks, 27% see the current security of their data center as 'inadequate' and in urgent need of updating, 85% of universities agree that more funding must be given to IT security to protect critical research IP, and On average, 30% of users in the education industry have fallen for phishing emails. The education sector accounted for 13% of all data security breaches during the first half of 2017, resulting in the compromise of some 32 million personal records.

In addition, 67% of financial institutions reported an increase in hacking attacks over the past year, and 26% of financial enterprises faced a destructive attack, and 79% of financial CISOs said hackers are deploying more sophisticated attacks. Also, 70% of financial institutions said they are most concerned about financially motivated attackers. In 2018 there were 80,000 hacking attacks per day or over 30 million attacks per year. 83% of global infosec respondents experienced phishing attacks in 2018, an increase from 76% in 2017. In 2017, hacking cyber-crime costs accelerated nearly 23% more than 2016 with an average about $11.7 million. The damage costs is $11.5 billion in 2019, and in 2020, it is over $1 trillion. However the damage related to hacking cybercrime is projected to hit $6 trillion annually in 2021.

The list of hacking attacks is so large, but giving samples in 2018 Cathy pacific was hacked and 9.4 million accounts compromised, and cyber attackers hacked into international computer systems and compromised five hundred million accounts. Also in March 2018, over 300 universities worldwide suffered from a giant hacking attack organized by Iranian hackers. According to the official information, 31 terabytes of "valuable intellectual property and data" was exposed. In 2019, Maryland Department of Labour was breached by hackers who illegally accessed names and social security numbers belonging to 78,000 people, also Captical One had over 106 million records stolen containing personal and financial information. In 2020 is Magellan Health was hacked by a ransomware and data breach stating that 365,000 patients were affected in the sophisticated hacking attack, and on an average 89% of healthcare organization had patient data lost or stolen in the past two years. In 2021 are the Kaseya suffered a ransomware hacking attack compromising up to 1500 companies with a staggering ransom note of $70 million, and Saudi Aramco data breach exposing sensitive data on employees and technical specifications of the organization. The hacker group ZeroX demanded a payment of $50 million. The U.S. government spend $15 billion on cyber security related activities in 2019 up 4% over the previous year, however, in 2021, the United States faced 38% of the hacking attacks putting it the number one target for targeted hacking attacks, with nearly 60 million Americans have been affected by identity theft (Purple Security, 2021).

The above reports are also supported by Imperva (2021d) who already observed hacking threats increase with over trillions attack requests analysed and billions successful attacks, and as per Lohrmann (2021) recent report found that the average cost of a data breach rose to $4.2M per incident. Also Irwin (2021) said that in month August 2021 84 incidents accounted for 60,865,828 breached records, in addition to the mobile network hack, which affected 53 million customers and 40 million records in the same month. Hill and Swinhoe (2021) stated that hacking affect hundreds of millions or even billions of people at a time as hackers exploit the data-dependencies of daily life. How large hacking is in the future might remain speculation, but as this list of the biggest data breaches of the 21st Century indicates, hacking have already reached enormous magnitudes. The following is just a sample, LinkedIn Date in June 2021 impacted 700 million users, Sina Weibo in March 2020 impacted 538 million accounts, Facebook in April 2019 impact 533 million users, and Marriott International (Starwood) in September 2018 impacted 500 million customers. Also, CSIS (2021) focussed on incidents since 2006 on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars, which included attacks on Centers for Medicare and Medicaid Services and NSO Pegasus spy where “Zeroclick”, Ukrainian energy outages, and eStuxnet attack at Iranian nuclear power plant. As reported by Purple Security (2021), in 2017, the average number of breached records by country was 24,089. The nation with the most breaches annually was India with over 33k files; the US had 28.5k. Moreover, 54% of companies are experiencing an industrial control system security incident, and the estimated total will be 33 billion hacked records by 2023. This list increases highly to include all aspects of life such infrastructure, nuclear power, education, health, finance, defense systems and private life as shown in Table A-1 in Appendix A.

To help secure services, the Open Web Application Security Project (OWASP) OWASP (2021b) has designed web applications and services security guide, which provides best practices and countermeasures to most common attacks. Yuill *et al.* (2006) propose a technique for dealing with security attacks which uses deception to hide assets from hackers. Denning (2007b) focus on the ethics of cyber conflict and analyzed hackers’ ethics. McClure *et al.* (2012) provide a breakdown of hacking procedures and structured hacking procedures into nine processes. They provided sample hacking attacks and countermeasures within each hacking stage. Similar anti-hacking approaches have been also adopted by Subramanian *et al.* (2021), Hartmann and Steup (2020), Dargahi *et al.* (2020), Lee *et al.* (2020), Marin *et al.* (2020), Toapanta *et al.* (2020), Cho *et al.* (2020) and Java *et al.* (2019).

At every attack, researchers are recommending new security solutions to cater for the newly encountered sophisticated attacks. However, over the past years scientists have been working on countermeasures against hacking attacks, and despite this, the systems are not just getting compromised by new attacks, but old onces are repeated over and over again in other ways. In addition, with technology advancement, the security breaches are increasing and becoming more sophisticated and aggressive (IC3, 2021; CVE Mitre, 21; OWASP, 2020; Breach, 2010; Scambray *et al.*, 2010; Levy, 2010). It is because most of the information security best practice models are not based on hacking countermeasure, but built upon certain compliance requirements that suit specific scope of businesses (Aldrich, 2009). Dyer *et al.* (2012) showed that as traffic analysis is possible, TLS, SSL, SSH, IPsec and other network security mechanisms are insecure, and same is reported by IspartNersllc (2021), Akhmetzyanova *et al.* (2020) and Kozachok *et al.* (2019). In addition, Sanchez and Korunka (2019), Nakasone (2019) and Harrison *et al.* (2010) mentioned that the source of hacking attacks is not just from individual criminals, but also from organized terrorist groups and foreign governments.

The devastating security status led many security experts to question Defense-in-Depth ability to defend security attacks. For example, Prescott (2012) conducted field surveys and concluded that information security defense mechanisms based on Defense-in-Depth cannot withstand against security attacks, and security professional must adopt new models for anti-hacking. This research conclusion about Defense-in-Depth was supported by multiple testimonials and references. Bratus (2007) stated that security professionals must give away traditional thinking, and anticipate hackers thinking instead. Regarding Defense-in-Breadth, Amoroso (2013, 2017) gave community suggestions to handle the security issues. Recent attacks have helped to gain new supporters, such as Scott (2014), Robinson (2015), Kewley and Lowry (2015), Cho and Ben-Asher (2017), Igbe (2017), Cicotte (2017), Filkins (2017), Chen (2020), Cho and Ben-Asher (2018), Stokes and Childress (2020), Lee *et al.* (2020) and Reddy *et al.* (2021), for Prescott's call for new framework, replacing Defence-in-Depth (DiD) or at least to adopt Defense-in-Breadth (DiB) along with Defense-in-Depth.

Further, according to Dargahi *et al.* (2020), Toapanta *et al.* (2020), Cho *et al.* (2020), Java *et al.* (2019), Summers (2015), Madden (2015), Summers *et al.* (2014), Graham (2013), Kimbell (2011), Mahmood *et al.* (2010), Wiles (2010), Yoo *et al.* (2006), Boland and Collopy (2004), and Buchanan (1992), to be able to prevent hacking, hackers' activities and cognitive skills must be analyzed and utilized in designing hacking countermeasures, which is missing in the present information security frameworks and compliances.

On the other hand, Oman does not have a national cyber security strategy, but has paid much attention to cyber security public awareness, training, and security incident recovery. Due to the necessity of addressing risks and security threats in Oman's cyberspace, the government of the Sultanate of Oman officially launched Oman Computer Emergency Readiness Team (OCERT) in April 2010. OCERT was developed to build trust between the Omani government and citizens with regards to e-government services. In addition, OCERT provides awareness, training and auditing services upon request. This initiative was introduced due to the considerable number of Omani citizens who are unaware of their exposure to security risks (Alkaabi, 2014). Alkaabi (2014) conducted a comparative study of sharing sensitive information among friends and relatives between the Gulf Cooperation Council (GCC) countries including Oman, Kingdom of Saudi Arabia (KSA), and United Arab Emirate (UAE). The study revealed cultural similarities of sharing sensitive information with friends and family members, which can lead to security preaches. The study by Alkaabi (2014) urged a development of a new framework that can protect from security preaches. In 2019, Oman Computer Emergency Response Team (OCERT) was very much improved with the introduction of a new information security framework that covered issencial security requirements as given in E-Oman (2019).

Although this research provides a solution to a global security issue, it pays great attention to the requirements of Oman Computer Emergency Response Team (OCERT) in OCERT (2021) and E-Oman (2019). In an attempt to develop a new framework for sustained cyber-siege defense, this research contributes towards a working solution for the security problem, and as such converting Computer Emergency Response Teams to Computer Emergency Readiness Teams. As this research concentrates on technical hacking, countermeasure tools and techniques, and management practices, the resultant output is a technical and administrative hacking countermeasure security framework. This research fulfills the missing hacking countermeasure gap found in information security frameworks. Moreover, it sets a baseline design to develop a proactive security solution to protect information systems by continuously guarding against hacking activities. It serves as a guide for information security specialists considering hacking countermeasure approaches to their information systems security design, and sets major guidelines for future research in the field of hacking countermeasures.

This chapter provides an introduction of the research, which begins with problem background and highlighting defensive measures in the existing information security systems. The chapter sets problem statement, and the main questions that put a roadmap for the final research deliverables. In addition, the chapter defines objectives and scope, and highlights the benefits of this research.

1.2 Problem Background

Hacking is defined by Gavel et al. (2020) as “the expertise in any field that can be used for both ethical and unethical purposes. Those who perform hacking are known as Hackers. Therefore, hackers are classified as per their working and as per their knowledge. The ethical hackers are also known as white hat hackers. Ethical hackers use their hacking techniques for providing security legally. Generally white hat hackers are legally authorized hackers that work for Government”. Similarly, McClure (2012), Follis and Adam (2020a), and Malwarebytes (2021) explane hacking as the activities performed by black hat hackers seeking compromise of digital equipment on entire networks, such as computers, tablets, smartphones and all other network devices. On the other hand, white hat hackers use their knowledge and experience to improve information security and prevent hacking attacks by finding systems’ vulnerabilities and providing solution recommendations. Also The Economic Times Security (2021) says “hacking is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorized access to or control over computer network security systems for some illicit purpose”.

Hackers are intelligent and highly skilled in computers, and all kinds of hacking are illegal. Compromising security systems requires more intelligence and experience than making them. In general computer hackers are categorized into black hat, white hat, and grey hat hackers. Black hat hackers are also called crackers who conduct hacking to control systems for personal profit. Black hat hackers steal, destroy or prevent authorized users from accessing their systems. This is done by searching for vulnerabilities in networks and network connected devices. On the other hand, white hat hackers are sometimes called ethical hackers who are professionals perform hacking to check the security of security systems for the sake of hardening systems against hacking attacks. However, grey hat hackers are curious people who have basic hacking skills enabling them to compromise systems to discover potential security weaknesses, then they notify network admins with the weaknesses discovered (The Economic Times Security, 2021). Also, Countermeasure is the tools and techniques used to defend assaults before, during and after the attacks had happened, and prevention is the process that takes place before attacks and used to prevent it from happening, which is regarded as an early stage of countermeasure (Subramanian *et al.*, 2021; Chesti *et al.*, 2020; Cappelli *et al.*, 2020; Liu *et al.*, 2018).

Dargahi et al. (2020) and Chesti et al. (2020) stated that despite the availability of AI-based solutions, anomaly detection and other advanced solution, hacking attacks using crypto-ransomware and other techniques are spreading. Bratus (2007), Schwab and Poujol (2018) and Follis and Adam (2020b) state that anti-hacking is a critical requirement for organizations' reputation, effective operations, and financial stability. However, available security controls can cater to limited risks due to the limitations in processes and procedures that govern the operations of the security tools. In contrast, hackers gain new knowledge of systems vulnerabilities and Information Technology (IT) personal does not have that knowledge (Bajak, 2020; Fonyi, 2020; Goebel *et al.*, 2019). As a result, hackers are granted authorized access to systems to execute administrative level tasks, hide themselves, and resist preventive measures (Subramanian, 2021; Hartmann and Steup, 2020; Burgess *et al.,* 2017; Shackleford, 2016; Masters, 2015; Olenick, 2015; Denning and Denning, 2010; Geer, 2006).

In addition, hacking steps represent anticipation and can vary in type and number of hacking steps or processes from three to nine steps or processes, for example, three steps given by Zadig (2016), five steps by Schifreen (2006), six steps by Microsoft (2020), Dell SecureWorks (2014) adopted what is called Cyber Kill-Chain model which has seven steps, also seven steps by Tipton and Krause (2007), seven steps by Barnes (2002), and nine hacking model as given by McClure *et al.* (2012). Thus, procedures, activities, innovations and tools differ from one hacking assoult to the other, therefore, characteristics, symptoms, and losses of the attacks also vary (Lee *et al*., 2020; Dargahi *et al*., 2020).

On the other hand, Defense-in-Depth (DiD) provides security protection in a layered form like an onion (Sattarova and Tao-hoon, 2007; HP, 2007; Eric, 2011). This approach uses multilayer defense systems, if hackers break one layer, they face the following in in-depth security (May *et al*., 2012; US-CERT, 2021b). Despite the advances in Defense-in-Depth techniques, hacking attacks are increasing enormously. It is because hackers are always ahead in discovering system vulnerabilities, which open doors for various hacking attacks (Lohrmann, 2021; Statista, 2020; Benoît *et al*., 2010; Rachana, 2010; Sami, 2009; Norman and Mark, 2009; Geer, 2006). Accordingly to Breach (2009), McClure *et al.* (2012), Haque and Chowdhury (2018), Heubl (2019) and Pham *et al.* (2020) researchers are developing advanced security controls, but hackers are also using highly sophisticated techniques using advanced automated hacking tools. It is noteworthy that the reported incidents represent just a fraction of hacking incidents, otherwise, security breaches and associated losses are increasing on daily basis (Lohrmann, 2021; Imperva, 2021d; Oracle, 2020; Alvarez et al, 2017, Verizon, 2017a, Prescott, 2012; Russinovich and Schmidt, 2011; Levy, 2010; Clarke, 2009).

In general, most available security solutions concentrate on the choice of tackling single threat at a time, such as introducing some kind of Authentication, Authorization, and Accounting (AAA) capabilities. These capabilities facilitate foundations to perform some kind of a Defense-in-Depth system. Recently, with the increase in attacks from the insiders, security approaches being used are losing supporters. Toapanta *et al.* (2020), Marin *et al.* (2020), Saxena *et al.* (2020), Cappelli *et al.* (2020), Homoliak *et al.* (2019), Liu *et al.* (2018) and Telstra (2017), Norman

(2010) and Harrison *et al.* (2010) show that conventional protection approach may reduce security risks and liability costs, but most likely will not prevent hacking from happening. Anti-hacking maybe possible if the right tools are used with the right techniques and procedures, however, with Defense-in-Depth systems, this is just a wish that is not based on reality (Lee *et al.*, 2020; Dargahi *et al.* 2020; Cicotte, 2017; Cho and Ben-Asher 2017; Shackleford, 2016; Robinson, 2015; Scott, 2014; Prescott, 2012).

As present information security frameworks rely on Defense-in-Depth techniques for the provision of the various security requirements, having healthy information system does not mean that there is no danger. Knowing that Defense-in-Depth tools have many limitations, it is just a matter of time for hackers' to hack due to the inherited common shortcomings in information security solutions that are based on Defense-in-Depth (Prescott, 2012). In this regard, Prescott (2012) also got number of testimonials and incidents supporting an argument regarding failure of Defense-in-Depth approach against hacking attacks, and suggests to adopt Defense-in-Breadth instead. This argument by Prescott (2012) regarding Defense-in-Depth and Defense-in-Breadth was also supported by Lee *et al.* (2020), Stokes and Childress (2020), Cho and Ben-Asher (2018), Cicotte (2017), Amoroso (2017), Shackleford (2016), Robinson (2015), and Scott (2014).

There are some of the problems that affect Defense-in-Depth security tools and techniques. It is related with the inherited shortcomings within the Defense-in-Depth tools and techniques associated (Imperva, 2021a; Amoroso, 2017; Shackleford, 2016; Prescott, 2012; Cox, 2012; Vijayan, 2009). Examples of these shortcomings include, firstly, anti-malware limitations in the malicious codes and zero-day attacks are not blocked by a signature-based detection technology, and malwares encrypt themselves and disable a wide variety of antivirus and security software (IBM, 2021; Chesti *et al.*, 2020; Mercaldo and Santone (2020); Masters, 2015; Olenick, 2015). Secondly, filtering limitations, if attacks are application driven inside a valid connection, then the attacks and malicious codes are not blocked (Campion *et al.*, 2021; Hamadouche *et al.*, 2020; Eskandari *et al.*, 2020; Botacin *et al.*, 2019; Alvarez *et al*, 2017; Shackleford, 2016; Hongxin *et al.*, 2012; Qian and Mao, 2012; Cox, 2012; Awasthi, 2010). Thirdly, patch delivery limitations with regard to too many vulnerabilities and patches to evaluate and test before deployment (Fonyi, 2020; Goebel *et al.*, 2019; Shackleford, 2016; Dey *et al.*, 2015; Jang and Brumley, 2012; Johnson, 2008). Fourthly, it is becoming increasingly difficult to contain contagions, as new threats with new tricks and unknown motives are looming (Hamadouche *et al.*, 2020; Botacin *et al.*, 2019; Shackleford, 2016; Meyers and Harris, 2009). Alvarez *et al.* *(* 2017) state that with Defense-in-Depth, it is becoming hard to manage and configure, and can be complex to configure and manage, which is supported by Toapanta *et al.* (2020).

The fifth limitation is that current information security solutions rely on human factor (Yonemura *et al.*, 2021; Witjes and Wentland, 2021; Cappelli *et al.*, 2020; Aggarwal *et al.*, 2019; Liu *et al.*, 2018;, Alvarez *et al.*, 2017; Shackleford, 2016; Prescott, 2012; Cox, 2012; Vijayan, 2009). Sixthly, present security solutions lack ability to maintain effective access control, as access point technologies are easily bypassed (Saxena and Alam, 2021; Rakhra *et al.*, 2020; Wang-R *et al.*, 2012; Cox, 2012; Anwar *et al.*, 2010; RSA, 2010; Vijayan, 2009). Also, recent attacks prove that continuously increasing breaches are due to the ineffectiveness of hacking prevention in the existing Defense-in-Depth access controls (IBM, 2021; Bajak, 2020; Heubl, 2019; Masters, 2017; Privacyrights, 2017; Telstra, 2017; Shackleford, 2016; SANS Institute, 2015; Data Loss Database, 2015; Verizon, 2014). Seventhly, secure links have limitations as IspartNersllc (2021) reported since 2015, SSL/early TLS encryption protocols were deemed as no longer secure. For example, TLS, SSL, SSH, IPsec etc., are popular mechanisms but it is possible to analyze their traffic (OWASP, 2021c; OWASP, 2021d; Akhmetzyanova *et al.*, 2020; Kozachok *et al.* 2019; Michael, 2015; Dyer *et al.*, 2012; McClure *et al.*, 2012). Reports show over 320 million hashes were exposed in 2017 (CynoSure Prime, 2017), also Hill and Swinhoe (2021) show increasing hacking attacks over the years starting with Marriott International (Starwood) in September 2018 impacted 500 million customers, Facebook in April 2019 impact 533 million users, Sina Weibo in March 2020 impacted 538 million accounts, and LinkedIn the impact was 700 million users in June 2021.

Considering the aforementioned problems, it is evident that the available practice models are weak and they limit the proper use of Defense-in-Depth security tool and techniques. Hackers have been successful in their attacks continuously and repeatedly over the years, because they first discover systems vulnerabilities and then use these vulnerabilities to attack (Fonyi, 2020; Goebel *et al*.,2019; Goebel *et al*., 2019; Casey, 2011; Goodin, 2011; Lennon, 2011; Storm, 2011; Denning and Denning, 2010). This implies that available security tools and management techniques can only prevent normal users from unauthorized access to certain systems or services. They tries their level best to reinforce security against hackers to some extents by not making it too easy to break though, thereby reducing damages when it happens. In fact, the problem is that most of the security tools available, conduct preventive measures against known threats, and take corrective actions after incidents.

The derivatives above on the effectiveness of Defense-in-Depth against hacking are not criticizing the security tools. Damiani *et al. (*2011) states that advanced research in this field should not be neglected as some security building blocks are now firmly in place for some vulnerabilities. In fact, the tools mentioned in the above are essential security pillars in any security solution. This analysis came from a practical experience to highlight vulnerabilities concerning the deployment and use of such tools, for the sake of raising alarms on security holes that may open the door for hackers. The limitations of Defense-in-Depth approach and the information security frameworks adopting it against hacking attacks is due to the unsuitability of these frameworks for anti-hacking, the shortcomings within the defense tools, and the vulnerabilities associated with operating systems and applications software (Pham *et al*., 2020; Haque and Chowdhury, 2018; Cox, 2012; Prescott, 2012; Vijayan, 2009).

With respect to solutions that provide features for behavioral analysis, which are useful for providing hacking detections and some countermeasures, there is no single framework that fits for all organizational needs and objectives (Monarchi and Puhr, 1992; Calder, 2008; Kirvan, 2020; CSO, 2021). This statement is still valid as Prescott (2012) stresses that Defense-in-Depth solutions are still incomplete, because successful hacking attacks and associated losses are increasing. Also, the skills and efforts required are decreasing due to the dependency on Defense-in-Depth only. Prescott (2012), Scott (2014), Robinson (2015), Kewley and Lowry (2015), Cho and Ben-Asher (2017), Igbe (2017), Cicotte (2017), Filkins (2017), Haque and Chowdhury (2018), Pham *et al.* (2020) and Infosecurity Magazine. (2021) conclude continuing with Defense-in-Depth only as anti-hacking is not an option, which is also supported by articles like Subramanian *et al.* (2021), Hartmann and Steup (2020), Dargahi *et al.*

(2020), Lee *et al.* (2020), Marin *et al.* (2020), Toapanta *et al.* (2020), Cho *et al.* (2020) and Java *et al.* (2019).

For an information security framework to be successful, it must rely on, first, strong leadership support and a comprehensive body of effective and efficient information technology security policies and procedures. Secondly, comprehensive body of effective and efficient hacking countermeasures that promote public trust, ensure continuity of services, comply with legal requirements, protect system assets, and recognize risks and threats (OSU, 2016). Complying with this requirement, Karen (2010) in his research shows that in order to fulfill information security challenges with regard to hacking, organizations must have the ability to ensure that their infosec solutions cover all information systems factors, anti-hacking best practices, services, and products that can mitigate hacking risks. In addition, Filkins (2017) and Cox (2012) stressed that to support anti-hacking requirement, hacking countermeasure solutions should be addressed to the core problem, and that is, to have 100% vulnerability free hardware and software. This is not feasible at all and can never be achieved, as critical vulnerabilities are increasing dramatically, and hackers are simply moving on to new attack surfaces. Bajak (2020) said millions of smart devices are vulnerable to hacking. In addition, Saha *et al.* (2021) stated that cyber-physical systems and Internet-of-Things devices are increasingly deployed in multiple functionalities. These devices are inherently insecure due to software, hardware, and network vulnerabilities, therefore presenting large number of security holes that can be hacked. Hence, having 100% vulnerability free system is again not an option to be considered for anti-hacking. In addition to the limitations within defence-in-depth mentioned above, there are three main problems that are discussed below.

1.2.1 Missing Anti-Hacking Factors Addressing Susceptibility To Hacking Risks

Awareness and knowledge of systems and local system risks is an essential security requirement, and there are many studies and recommendations to resolve this issue. Scientists like Bratus (2007) stated that security professionals must give away traditional thinking, and anticipate hackers thinking instead. According to Sun Tzu and Cleary (2005) and Lancor and Workman (2007), one of the main best practice for hacking countermeasure is to know your enemy. Mahmood *et al.* (2010) states that without better and truer understanding the antisocial behavior that lead to hacking, the most effective countermeasures cannot be readily designed. Ability to understand hackers' behavior in various circumstances helps slowing the attack, limiting the impact of hacking breaches, and lessening the damages caused by hackers (Mahmood *et al.,* 2010). Bratus *et al.* (2010), McClure *et al.* (2012), Afroz *et al.* (2012), Wu (2014), Trabelsi and McCoey (2016), Java *et al.* (2019) and Toapanta *et al* (2020), Marin *et al.* (2020) recommend departing from the traditional thinking to hackers mind to anticipate hacking.

Flow (2017) emphasizes that one major requirement for hacking countermeasure is anticipating what hackers are doing and then counteract accordingly. Similarly, Cox (2012) stated it is impossible to block all vulnerabilities or detect new ones, but firm security policy and proper configuration may be the best option. Summers *et al.* (2014) state that hackers are adept to re-engineering ambiguous problems for bringing inventive solutions, idea iterations, and envision probable solutions. Therefore, investigating hackers' activities and motivations brings new insights into how to avoid becoming hackers' target. Summers (2015) suggests deepening knowledge of emergent fields of hacking activities to gain further understanding of hackers mind as strategic organizational capabilities. Researchers like Subramanian *et al.* (2021), Hartmann and Steup (2020), Dargahi *et al.*, (2020), Lee *et al.* (2020), Marin *et al.* (2020), Summers (2015), Madden (2015), Graham (2013), Kimbell (2011), Wiles (2010), Yoo *et al.* (2006), Boland & Collopy (2004), and Buchanan (1992) recommend exploring hackers thinking in designing and planning for hacking activities to deepen information about hackers' way of thinking in solving problems and to improve hacking countermeasure designs. Moreover, Summers (2015) showed that there is a need for developing assessment to measure hackers traits and their existing cognitive skills, in addition to the requirement to examine the nature of association between hackers' traits, cognitive skills and hacking. Examples of exploring hacking anticipation are given by McClure *et al.* (2012), Dell Secureworks (2014) and Microsoft (2020) who structured hacking anticipation into hacking steps and gave detailed procedures for hacking steps. In addition, experts such as Subramanian *et al.* (2021), Purple Security (2021), Imperva (2021a), Hartmann and Steup (2020), Dargahi *et al.* (2020), Lee *et al.* (2020), Marin *et al.* (2020), Toapanta *et al.* (2020), Cho *et al.* (2020), Microsoft (2020), Java *et al.* (2019), ACSC (2018), Burgess *et al.* (2017), Blackmer (2017), Grimes (2017), Melone (2017) and Amoroso (2017) also recommend hacking anticipation as a mean for awareness and knowledge of systems and local systems risks. Hence, from the literature review above, a sub research question is derived as shown below:

Sub-question 1: How to apply hacking anticipation techniques in the most effective way to give the highest possible positive impact on hacking perception and countermeasure?

1.2.2 Missing Anti-Hacking Relationships That Close Hacking Gaps

Researchers believe that Defense-in-Depth cannot defend against hacking attacks, and are introducing other approaches to effectively secure systems against hacking. One approach is given by Prescott (2012) who concluded that defense mechanisms based on Defense-in-Depth cannot withstand hacking attacks, and security professionals must adopt new models for anti-hacking. Prescott (2012, 2011) supported this conclusion with many evidences on the weaknesses of Defense-in-Depth against hacking attacks. He recommends Defense-in-Breadth (DiB) with overlapping defense layers that complement one another. Also, in the Defense-in-Breadth arena Amoroso (2017) provided suggestions for community on how to handle security issues. The Defense-in-Breadth approach is also recommended by Scott (2014) who stated that Defense-in-Depth uses independent methods organized in layers of defense tactics to defend against certain targeted attacks. Traditional information security has pursued this Defense-in-Depth approach for a very long time, which is being threatened due to the introduction of billions of new connections, protocols, and instrumentations that contain vulnerabilities both in depth and breadth. Hence, Defense-in-Depth and Breadth are essential anti-hacking requirements as they both consider the unique challenges and synchronize different tools to strategically address them (Scott, 2014).

Robinson (2015) recommends extending defense mechanisms to cover both Defense-in-Depth and Defense-in-Breadth to care for vulnerability threats from outside the organizations, such as malwares, Trojans and other hacking activities, and calls for both Defense-in-Depth and Breadth approaches to be used together. To assess the ability of Defense-in-Breadth to defend against hacking, Kewley and Lowry (2015) conducted a series of experiments on the DARPA Information Assurance (IA) program and showed that Defense-in-Breadth is equally important as Defense-in-Depth, and using Defense-in-Depth without Defense-in-Breadth is strictly ineffective for a sophisticated adversary. They recommended that Defense-in-Depth and Defense-in-Breadth must be used together. In addition, Cho and Ben-Asher (2017) developed a probability Defense-in-Breadth model using Stochastic Petri nets and found out that Defense-in-Breadth outperforms Defense-in-Depth by minimizing attack success while maximizing system lifetime.

Furthermore, Igbe (2017) documented that Defense-in-Depth has done a good job in the past, but as technology evolves, especially with the advent of cloud based work place, Defense-in-Depth has shown some shortcomings. Thus, there is a requirement to revise Defense-in-Depth tools and techniques. It is noteworthy, that the intention is not to throw Defense-in-Depth, but to keep tools and techniques that are still effective and augments it based on the nature of new requirements. Defense-in-Breadth is about implementing multiple security controls at every layer reference of the Open Systems Interconnection model (OSI). It is also about automation of the security controls and processes, thus, Defense-in-Depth and Defense-in-Breadth should be used simultaneously. With proper security controls, such as Defense-in-Depth and Defense-in-Breadth, coupled with best security practices, the number of successful attacks will reduce (Igbe, 2017). These recommendations are also supported by Filkins (2017) who states that, to countermeasure hacking, two security requirements must be accomplished, i.e., compliance with hacking countermeasure policy, and Defense-in-Breadth must contract with other partners.

Similarly, the recommendation to introduce Defense-in-Breadth in parallel with Defense-in-Depth is also suggested by Cicotte (2017), stating that most recent breaches are occurring at application layer and to ensure ever-expanding perimeter is protected, organizations must have Defense-in-Breadth together with Defense-in-Depth. In fact, due to the continuous increase in cybercrime, such as APTs, malware, and ransomware, Cicotte (2017) advices to build a new solid security framework from scratch instead of trying to enhance the existing frameworks. Thus, in addition to the two main research questions, it is also important to set sub-research questions. They will help develop solutions to fill the identified gap in the hacking countermeasures, and facilitate in finding answers. In addition, the recommendation for Defence-in-Breadth is also given by Reddy *et al.* (2021), Stokes and Childress (2020), Lee *et al.* (2020), Chen (2020), Cho and Ben-Asher (2018)., Trump (2018), Uhr (2017), Alfor and Greven (2017), and Healy (2017).

Sub-question-2: How to apply Defense-in-Depth techniques in the most effective way to give the highest possible positive impact on hacking perception and countermeasure?

Sub-question-3: How to apply Defense-in-Breadth *techniques in the most effective way to give the highest possible positive impact on hacking perception and countermeasure?*

Another approach that is believed effective in securing systems against hacking attacks is given by Dahbu *et al. (*2017), Gartzke & Lindsay (2015), Yuill *et al. (*2006) and Denning (2007b), who show that hiding and deception is a technique that is usually used by hackers in compromising systems, but also can be used to counteract hacking activities. In addition, Imperva (2017a) and Amoroso (2017) have suggested deception as one of the main hacking countermeasure requirements to be used, and introduced hiding and deception as a school that brings complementary techniques to strengthen hacking countermeasure. According to Almeshekah and Spafford (2016), many computer defenses that use deception are merely based on ad-hoc attempts to incorporate deceptive elements in their design.

One of the first technical hiding deception frameworks was designed by Bell and Whaley (1991) who presented the general deception model. Also, Yuill *et al.* (2006) have proposed a way of dealing with security attacks using deception to hide things from hackers, which is a very important parameter in hacking countermeasures. In year 2007, Denning (2007b) has published a paper on the ethics of cyber conflict, where the author analyzed hackers' ethics, and talked about the hacking procedures. In 2014, Almeshekah and Spafford (2014) presented a framework for planning and integrating deception in information security defenses. This framework was based on the deception model of Bell and Whaley (1991). In 2016, Almeshekah and Spafford (2016) proposed three general phases for deceptive factors, namely planning, implementing and integrating, and finally monitoring and evaluating. Different experts, such as Basak *et al.* (2021), Ferguson-Walter (2020), Huang and Zhu (2019), Al Amin *et al.* (2019), Amoroso (2017), Dahbu *et al.* (2017), Gartzke & Lindsay (2015), Zager and Zager (2015) and AlKaabi (2014) recommend deception, which implies that Hiding and Deception is one of the main important hacking countermeasure factors.

Hacking Anticipation, Defense-in-Breadth and Hiding and Deception as main hacking countermeasure factors are also recommended to be combined together for stronger and more effective defense against hacking. According to Imperva (2017a), rising attacks shows that four out of five organizations breached in 2016 were due to weaknesses in the mobile services, secure applications, patch management, cyber insurance, antiviruses etc. To overcome this problem, Imperva (2017a) recommends the followings: i) Specialized countermeasures should be added to complement existing defenses, ii) Shift from establishing baseline security postures for determining the type of cyber threats and other obstacles for security, iii) Reduce attack surface and use an overlapping set of detection-focused countermeasure to mitigate the residual risk, iv) Apply behavior analysis, and v) Use deception techniques. Also Imperva (2021a) brought similar recommendations.

The aforementioned recommendations (two to four), are contained within hacking anticipation as per Prescott (2012), McClure *et al.* (2012) and Dell SecureWorks (2014). Also, the recommendation one and five in Imperva (2017a) refers to Defense-in-Breadth and hiding and deception factors, respectively. These three recommended factors are also supported by Amoroso (2017), who brings three main requirements to countermeasure hacking saying that traditional defense systems are based on signature processing and they are ineffective in detecting APTs and hacking activities. To provide more effective solutions, he recommends applying heuristics behavioral, followed by breadth virtualization, and finally, create new security features, such as deception, which well supported by Kulkarni *et al.* (2021), Alshammari *et al.* (2020), Al Amin *et al.* (2020), Efendi *et al.* (2019), Aggarwal *et al.* (2019). This review delivers the following sub-question.

> *Sub-question-4: How to apply hiding and deception techniques in the most effective way to give the highest possible positive impact on hacking perception and countermeasure?*

In addition, Incident Management (IM) and Event Handling is also regarded as one of the main countermeasure factors that should be included in any information security solution (Boyle and Panko, 2021; Lamar university, 2021; Olzak, 2017; Luttgens *et al.,* 2014; Prescott, 2012; Panko, 2011; Tutton, 2010; Michael, 2010; George and Sokratis, 2010; Gregory, 2007; Williams, 2006). This also raises a fifth research sub question as follows.

> *Sub-question-5: How to apply incident management and event handling techniques in the most effective way to give the highest possible positive impact on hacking perception and countermeasure?*

1.2.3 Missing Framework Structures That Prevent Systems' Hacking

Breaches negatively impact reputation, confidence, regulatory aspects, financial costs, and cause losses that ere direct and indirect. Industry is becoming susceptible to industry risks with the increase of sophisticated hacking attacks, making it vital to develop new models that can predict attackers' behavior (Shackleford, 2016; Dover, 2016; Burgess *et al.,* 2017). Recent security attacks are of global nature and target sensitive areas causing severe damages and losses. This forces security experts to explore new security solutions other than Defense-in-Depth.

Considering the aforementioned discussions (in Sections 1.2.1 and 1.2.2), experts such as Scott (2014), Robinson (2015), Kewley and Lowry (2015), Cho and Ben-Asher (2017), Igbe (2017), Cicotte (2017) and Filkins (2017) agree on two main points, i) Defense-in-Depth has limitations and cannot provide defense as a stand-alone, ii) while keeping Defense-in-Depth, it is must to have Defense-in-Breadth. Experts like Prescott (2012) Cicotte (2017), Amoroso (2017) and Imperva (2021b) advice developing a new framework. In addition, experts such as Microsoft (2020), Burgess *et al.* (2017), Blackmer (2017), Grimes (2017), Melone (2017), Flow (2017), Amoroso (2017), Trabelsi and McCoey (2016), Madden (2015), Dell Secureworks (2014), Wu (2014), McClure *et al.* (2012) and Mahmood *et al.* (2010) also recommend hacking anticipation, and experts such as Basak *et al.* (2021), Kulkarni *et al.* (2021), Ferguson-Walter (2020), Alshammari *et al.* (2020), Al Amin *et al.* (2020), Efendi *et al.* (2019), Huang and Zhu (2019), Aggarwal *et al.* (2019), Al Amin *et al.* (2019) , Amoroso (2017), Dahbu *et al.* (2017), Almeshekah and Spafford (2016), Gartzke & Lindsay (2015), Zager and Zager (2015), AlKaabi (2014), Almeshekah and Spafford (2014) and Yuill *et al.* (2006) recommend hiding and deception. Thus, missing any one of these three countermeasure factors (hacking anticipation, Defense-in-Breadth or hiding and deception) will induce weakness in defending against hacking. Furthermore, there are some other hacking countermeasure factors that are currently in use, namely risk assessment, auditing, penetration testing, and compliance.

Loch *et al.* (1992) reported that security threat risk is the effect of a wide range of forces that are capable of inducing adverse consequences. This threat is dynamic that varies over time to adjust to various preventive and deterrent measures (Yeh and Chang, 2007; Schuessler, 2009). According to Blumstein (1978) General deterrence theory posits that people will not commit crimes when the risk of getting caught is high and severe penalties are applied. Logan and Clarksons (2005) suggest security assessment, continuous network monitoring and also planning and consultations with others in the field as major security requirements. Risks assessment has also been recommended as a major security requirement by Saha *et al.* (2021), Lee *et al.* (2020), Ponemon (2018), McNab (2017), Teixeira *et al.* (2015), Summers (2015), AlKaabi

(2014), Zhanshan (2011), Nayot *et al.* (2011), Basuki *et al.* (2010), Singaravel *et al.* (2010), Jeffrey *et al.* (2009), Denning (2007a), and Judith *et al.* (2007). Similary, auditing and penetration testing is an essential security requirement that has been suggested in many resources, such as PCI-DSS (2020), Long (2020), Wahsheh and Mekonnen (2019), NIST (2018), Trabelsi and McCoey (2016), EC-Council (2016b), Summers (2015), Kim (2014), and Shackleford (2012). Also, the importance of following information security standards and compliance is strongly stressed by many, such as ISO/IEC (2021a,b,c), ITG (2021), Drake (2021), PCI-DSS (2021c), Mirtsch *et al.* (2020), Kirvan (2020), Lachapelle and Bislimi (2016), Mathew *et al.* (2011) and Jeff (2010).

These countermeasure factors have years of accumulated best practice experience and are very strongly recommended; as advised by Scott (2014), Robinson (2015), Kewley and Lowry (2015), Cho and Ben-Asher (2017), Igbe (2017), Cicotte (2017), Filkins (2017) and Amarendra *et al.* (2019). Thus, in addition to the previous five sub-questions, it is also a requirement to set sub-research questions that develop solutions to fill the identified gap in hacking countermeasure.

Sub-question-6: How to apply hacking risks assessment techniques in the most effective way to give the highest possible positive impact on hacking perception and countermeasure?

Sub-question-7: How to apply auditing and penetration testing techniques in the most effective way to give the highest possible positive impact on hacking perception and countermeasure?

Sub-question-8: How to apply standards and compliances techniques in the most effective way to give the highest possible positive impact on hacking perception and countermeasure?

Summarizing the analysis of hacking problem in this section, to countermeasure hacking, it is essential to, firstly, depart from the traditional thinking to hackers mind. (Subramanian *et al.*, 2021; Purple Security, 2021; Imperva, 2021a; Hartmann and Steup, 2020; Dargahi *et al.*, 2020; Lee *et al.*, 2020; Marin *et al.*, 2020;

Toapanta *et al.*, 2020; Cho *et al.*, 2020; Java *et al.*, 2019; ACSC, 2018; Burgess *et al.*, 2017; Blackmer, 2017; Grimes, 2017; Melone, 2017; Flow, 2017; Amoroso, 2017; Trabelsi and McCoey, 2016; Madden, 2015; Summers, 2015; Summers *et al.*, 2014; Dell Secureworks, 2014; Wu, 2014; Graham, 2013; Kimbell, 2011; McClure *et al.*, 2012; Afroz *et al.*, 2012; Mahmood *et al.*, 2010; Bratus *et al.*, 2010; Wiles, 2010; Vijayan, 2009; Bratus, 2007; Yoo *et al.*, 2006; Bolan & Collopy, 2004; Buchanan, 1992). Secondly, apply Defense-in-Breadth (Reddy *et al.*, 2021; Stokes and Childress, 2020; Lee *et al.*, 2020; Chen, 2020; Cho and Ben-Asher, 2018; Trump, 2018; Uhr, 2017; Alfor and Greven, 2017; Healy, 2017; Cho and Ben-Asher, 2017; Igbe, 2017; Cicotte, 2017; Shackleford, 2016; Dover, 2016; Kewley and Lowry, 2015; Robinson, 2015; Scott, 2014; Prescott, 2012; EMA, 2010; Harrison *et al.*, 2010; Aldrich, 2009). Thirdly, apply hiding and deception (Basak *et al.*, 2021; Kulkarni *et al.*, 2021; Huang and Zhu, 2019; Ferguson-Walter, 2020; Alshammari *et al.*, 2020; Al Amin *et al.*, 2020; Efendi *et al.*, 2019; Aggarwal *et al.*, 2019; Al Amin *et al.*, 2019; Amoroso, 2017; Imperva, 2017a; Dahbu *et al.*, 2017; Almeshekah and Spafford, 2016; Gartzke & Lindsay, 2015; Zager and Zager, 2015; AlKaabi, 2014; Almeshekah and Spafford, 2014; McClure *et al.*, 2012; Yuill *et al.*, 2006; Hinson, 2008). Finally, according to this research problem analysis and findings above, the following section derives the statement of problem.

1.3 Statement of the Problem

As a result of the hacking problem analysis provided in section 1.2 that highlighted the anti-hacking limitations and main problems within defence-in-depth is that the hacking problem still persists and there is no hacking countermeasure framework integrates hacking anticipation, Defence-in-Breadth and hiding and deception. Thus in an attempt to try to provide a solution for hacking countermeasure, this research is approaching an anti-hacking solution via anticipating hacking, using Defence-in-Breadth and applying the concept of hiding and deception. Therefore, this research aims for a state of the art information security solution in this challenging field, by answering the main research question and statement of problem that says **How to prevent systems hacking and fulfill managerial concern about systems**

hacking risk?. This also leads to finding answers for the following main research questions.

i) What anti-hacking factors can address organizations' susceptibility to hacking risk and effectively secure systems against hacking?

ii) What are the anti-hacking relationships that close the security gap causing hacking and improve organizations' anti-hacking needs

iii) What framework structure can best prevent systems' hacking and fulfill managerial concern about systems' hacking risk.

Furthermore, from the eight sub-research question that relate to the three main research questions above, there are eight hypothesis derived as follows.

Sub-question-1 relating to the first main research question: How to apply hacking anticipation techniques in the most effective way to give the highest possible positive impact on hacking perception and countermeasure?
Hypothesis 1: Applying hacking anticipation will have a positive impact on hacking perception and countermeasure.

Sub-question-2 relating to the second main research question: How to apply Defense-in-Depth techniques in the most effective way to give the highest possible positive impact on hacking perception and countermeasure?
Hypothesis-2: Using enhanced Defense-in-Depth will have a positive impact on hacking perception and countermeasure.

Sub-question-3 relating to the second main research question: How to apply Defense-in-Breadth *techniques in the most effective way to give the highest possible positive impact on hacking perception and countermeasure?*
Hypothesis-3: Applying Defense-in-Breadth *will have a positive impact on hacking perception and countermeasure.*

Sub-question-4 relating to the second main research question: How to apply hiding and deception techniques in the most effective way to give the highest possible positive impact on hacking perception and countermeasure?

Hypothesis-4: Using hiding and deception will have a positive impact on hacking perception and countermeasure.

Sub-question-5 relating to the second main research question: How to apply incident management and event handling techniques in the most effective way to give the highest possible positive impact on hacking perception and countermeasure?

Hypothesis-5: Using hacking incident management and event handling will have a positive impact on hacking perception and countermeasure.

Sub-question-6 relating to the third main research question: How to apply hacking risks assessment techniques in the most effective way to give the highest possible positive impact on hacking perception and countermeasure?

Hypothesis-6: Using hacking risk assessment will have a positive impact on hacking perception and countermeasure.

Sub-question-7 relating to the third main research question: How to apply auditing and penetration testing techniques in the most effective way to give the highest possible positive impact on hacking perception and countermeasure?

Hypothesis-7: Using anti-hacking auditing and penetration testing will have a positive impact on hacking perception and countermeasure.

Sub-question-8 relating to the third main research question: How to apply standards and compliances techniques in the most effective way to give the highest possible positive impact on hacking perception and countermeasure?

Hypothesis-8: Using anti-hacking standards and compliances will have a positive impact on hacking perception and countermeasure.

1.4 The Research Motivation

There are reports in section 1.1 and section 1.2 that showed more than 50% of companies and organisations experienced hacking security incident in year 2021. More than 33 billion hacked records are estimated by 2023, and hacking increases highly to include infrastructure, education, health, finance, defense systems, nuclear power, and all aspects of life. Furthermore, recent hacking attacks have increased the supporters for the call to adopt Defense-in-Breadth (DiB) together with Defense-in-Depth, or to develop a new anti-hacking framework replacing Defense-in-Depth (DiD). This call is motivating this research to develop a new Hacking Countermeasure Framework.

This thesis presents a new era in information system security, leading to the hart of the latest defense technique using "Hacking Countermeasure Framework". This thesis should also set major guide lines for future researches in this field; which can regarded as the necessary security pillar for all organizations. On the other hand, the study serves as a guide to network designers considering the security requirements of their information systems, taking hacking anticipation, defense-in-breadth, and hiding and deception approach to network security design. Hense, hacking problem is reduced through this research.

1.5 The Aim of the Research

The aim of this research is to develop Hacking Countermeasure Framework by anticipating hacking, and *As-To-Be* Defense-in-Depth capabilities against hacking, Defense-in-Breadth, and hiding and deception techniques to further enhance the hacking countermeasure capabilities.

1.6 Objectives of the Study

This research sets major guidelines for future researchers in the field of hacking countermeasure. In addition, the study serves as a guide for information security specialists considering hacking countermeasure approaches to their information systems security design. Other good approaches may exist, but this core study aims to fill the missing hacking countermeasure gap that is currently there in information security frameworks and best practice models. The objective of the study is to develop an anti-hacking security solution for protecting information systems by continuously guarding against hacking. As a result of the previous problem analysis and recommendations in section 1.2, the objectives are directed to design and develop Hacking Countermeasure Framework that directs countermeasures to hacking steps. Therefore, the objectives are summarized as follows.

i) To identify anti-hacking factors that can address organizations' susceptibility to hacking risk and effectively secure systems against hacking as per Delphi method.

ii) To derive the anti-hacking relationships that close the security gap causing hacking, and provide organizations' anti-hacking needs.

iii) To develop hacking countermeasure framework that prevents systems hacking and fulfills managerial concern about hacking risk.

iv) To validate the hacking countermeasure framework through a selected validation tools such are meeting satisfaction rate on Delphi, discussion workshops, research review, conducting interviews, frameworks comparison, and finally, approval of the framework by Computer Emergency Response Team (CERT).

1.7 Scope of the Study

For sake of conducting this research number of research methods were reviewed including Diffusion methodology, Design science, Quantitative method, Qualitative method, Mixed method and Delphi. However Delphi method was found most suitable for conducting this research due to special type of survey sample required to participate, and also due to the specific criteria that Delphi method features. According to Skulmoski *et al.* (2007) Delphi method is well suited for information systems research because Delphi is a fluid discipline ripe for research, and it is a structured process within which quantitative, qualitative, and mixed methodologies can be used, but, differs from the other research methods in three main things that maintain the reliability and validity, these are first the survey sample is preselected according to specific criteria, secondly, the sample size is much smaller, and thirdly, the Delphi case design.

This research is organized in four phases containing six Delphi rounds. Phase one, is building nature of reality and knowledge for analysing hacking problem, anti-hacking capability within Defense-in-Depth techniques, and identifying recommendations for anti-hacking. The deliverables of this phase serve as a feasibility study for this research, which is done via literature review, interviews and pre-Delphi surveys. Second phase first identifies anti-hacking factors that can address organizations' susceptibility to hacking risk and effectively secure systems against hacking. This provides deliverables for the first research question, first objective, and testing of the first hypothesis using Delphi round one. Also phase two derives What are the anti-hacking relationships that close the security gap causing hacking and improve organizations' anti-hacking needs for the second research question, second objective, and testing of the second to eighth hypothesis using Delphi rounds two and three. The third phase serves the derivation of framework structure to prevent systems hacking and fulfills managerial concern about hacking risk, it provides deliverables for the third research question and third objective using Delphi rounds four to six. Finally, phase four research documentation that verifies final research deliverables and fulfills the fourth research objective using study cases and generalization by contribution to knowledge and documentation through thesis write-up.

The scope of this research is concentrated on deriving a hacking countermeasure framework to further enhance the hacking countermeasure capabilities. The scope of the work is structured to cover the following.

i) This work is organizational investigation for hacking countermeasure.

ii) This research is conducted in the lenses of the model for managerial perceptions of security risk from Straub and Welke (1998).

iii) This research is using Delphi method for developing the Hacking Countermeasure Framework for securing organizations.

iv) The research is conducted using expert panel that is specialized in information security.

1.8 Significance of the Study

As shown in the problem background in Section 1.2, there is a significant increase in security holes in both hardware and software, and hackers are breaking into systems. Hackers are also always ahead in discovering system vulnerabilities, and consequently, information systems are continuously and successfully being attacked heavily on daily basis.

The significance of this research is very important in the attempt to design and develop a framework for hacking countermeasure. To do so, this research addresses identified hacking security gaps by introducing solutions based on hacking anticipation, Defense-in-Breadth, deception and hiding techniques. The research significance of this work are as follows:

i) This framework reduces hacking problem by integrating hacking anticipation, hiding and deception, and Defense-in-Breadth, and provides enticing clues regarding the role of these three factors in the hacking countermeasures.

ii) This framework shows that Defense-in-Depth (DiD) still plays an important role in hacking countermeasure.

iii) The deliverables of this research can be used as an add-on anti-hacking module for information security standards and compliances that are missing anti-hacking modules.

iv) This HCF is useful for both academia and industry and enhances theory and practice of hacking anticipation, Defense-in-Breadth, and hiding and deception.

v) This research sets an example in the use of Delphi method that involves Oman CERT, Malaysia CERT, and international key-informant cyber security experts from a variety of organizations that include military, security departments, public, and private organizations.

1.9 Thesis Organization

This thesis consists of six chapters. Chapter one provides a brief background of the problem and discusses available information security solutions with respect to limitations in defending against hacking attacks. The chapter provides statement of the problem, sets the aim and objectives of the study, and highlights the scope and the benefits of the study. Chapter two reviews the relevant literatures that relate to the information required to design and develop the hacking countermeasure framework, such as hacking steps, countermeasure factors, defense tactics and framework architecture. Chapter three provides research methodology, followed by chapter four which presents the actual research work to design and develop the hacking countermeasure framework for securing organizations. Chapter five covers the research validation and results analysis. Finally, chapter six concludes the thesis.

1.10 Summary

This chapter introduced hacking threats and highlighted the importance of design and development of hacking countermeasure framework. It provided problem statement, research objectives, scope of research, and benefits of the study. The literature review and research methodology for achieving the set objectives are discussed in chapter two and three, respectively.

REFERENCES

A. and Childress, M. (2020). Maturity Model Certification Explained What Defense Contractors Need To Know. *IDG Communications.* (USA).

Aameek, S., Ling, L. and Mustaque, A. (2008). Privacy analysis and enhancements for data sharing in *nix systems. International Journal of Information and Computer Security (USA). Vol. 2, No.4, pages 376 – 410.

Abay, N. C., Akcora C. G., Zhou, Y., Kantarcioglu, M. and Thuraisingham, B. (2019). Using deep learning to generate relational HoneyData. *Autonomous Cyber Deception*. Springer. pp. 3–19.

Abbes, T., Bouhoula, A. and Rusinowitch, M. (2010). Efficient decision tree for protocol analysis in intrusion detection. *International Journal of Security and Networks* (France). Vol. 5, No.4, pages 220 – 235.

Abdelrahman, D. Sumstega. (2011). Summarisation-based steganography methodology. *International Journal of Information and Computer Security* (USA). Vol. 4, No.3, pages 234–263.

ACSC. (2017). Strategies to Mitigate Cyber Security Incidents. Australian Cyber Security Centre. (Australia). Available from https://www.asd.gov.au/publications/Mitigation_Strategies_2017.pdf. Visited on: 20th October/2017.

ACSC. (2018). Protective Security Policy Framework-v2018.4. Australian Cyber Security Centre. (Australia). Available from https://www.protectivesecurity.gov.au. Visited on: 29th January/2021.

Adair, S., Hartstein, B., Richard, M. and Ligh, M. (2010). *Malware Analyst's Cookbook: Tools and Techniques for Fighting Malicious Code*. Wiley (USA).

Adel, B., Zouheir, T., Ezedin, B. and Mohammed-Anis, B. (2008). Firewall filtering rules analysis for anomalies detection. *International Journal of Security and Networks*. Vol. 3, No.3, pages 161-172.

Adin, S., Alexander, V., Anthony, L. and Eyal, De Lara. (2009). Proximity-based authentication of mobile devices. *International Journal of Security and Networks*. (Canada). Vol. 4, No.1/2, pages 4-16.

Adrian, L. (2010). *Best Practices for Tuning Database Audit Tools.* Guardium (USA).

Aedah Binti Abd Rehman (2014). *Multi model software process improvement framework.* Doctor of Philosophy. UTM. Malaysia.

Afroz, S., Brennan, M., and Greenstadt, R. (2012). Detecting Hoaxes, Frauds, and Deception in Writing Style Online. *33rd IEEE Symposium on security and privacy (S&P 2012).* IEEE computer society (USA). Pages 461-475.

Aggarwal, P., Gautam, A., Agarwal, V., Gonzalez, C. and Dutt, V. (2019). HackIt: A human-in-the-loop simulation 25 tool for realistic cyber deception experiments. *International Conference on Applied Human Factors and Ergonomics*. Springer, pp. 109–121.

Aggeliki, T., Maria, K., Spyros, K. and Evangelos, K. (2010). Aligning Security Awareness with Information Systems Security Management. *Journal of Information System Security*. Washington DC, USA: Information Institute Publishing. Volume 6, No.1, pages 36–54.

Aggelinos, George, Katsikas, and Sokratis. (2009). Integrating Disaster Recovery Plan Activitiesi into the System Development Life Cycle. *MCIS*. Paper 76.

Ajzen, I., & Madden, T. (1986). Prediction of Goal-Directed Behavior : Attitudes, Intentions, and Perceived Behavioral Control. *Journal of Experimental Social Psychology, 22, 453–474*

Akbar Nabiollahi (2012). *An integrated service architecture framework for information technology service management and enterprise architecture. Computer Science*. Doctor of Philosophy. UTM. Malaysia.

Akhmetzyanova, L., Alekseev, E., and Smyshlyaeva, E. (2020). On post-handshake authentication and external PSKs in TLS 1.3. *J Comput Virol Hack Tech 16*, 269–274. https://doi.org/10.1007/s11416-020-00352-0

Akhoondi, M., Yu, C. and Madhyastha, H. (2012). LASTor. A Low-Latency AS-Aware Tor Client. *33rd IEEE Symposium on security and privacy (S&P 2012).* IEEE computer society (USA). Pages 476–490.

Akram, Anastasia M. (2005). *Watch out for Spies*. Ray Publishing & Science (Syria).

Al Amin, M., Shetty, S., Njilla, L., Tosh, D. and Kamouha, C. (2019). Attacker capability based dynamic deception model for large-scale networks. *EAI Endorsed Transactions on Security and Safety*, vol. 6, no. 21.

Al Shidhani, Ali and Victor, C.M. Leung. (2011). Fast and Secure Reauthentications for 3GPP Subscribers during WiMAX-WLAN Handovers. *IEEE Transactions on Dependable and Secure Computing*. September/October. Vol. 8, no. 5, pages 699-713.

Aldrich, M. (2009). Hackers crack. *Chief Information Security Officer*. LLOYDS (UK).

Alejandro, P. and Loukas, L. (2011). Packet-Hiding Methods for Preventing Selective Jamming Attacks. *IEEE Transactions on Dependable and Secure Computing*. IEEE Computer Society (USA). Vol. 99, no. 1.

Alessandro, A. and Alessandra, D. (2007). Estimating the maximum information leakage. *International Journal of Information Security*. October. Volume 7, No. 3, pages 219-242.

Alex, B., Michael, S., Matthew, C. and Joseph, Z. (2010). A case study in hardware Trojan design and implementation. *International Journal of Information Security*. September. Volume 10, Number 1, pages 1-14.

Alexander J. and Kroposki M. (1999). Outcomes for community health nursing practice. *Journal of Nursing Administration* 29, 49-56.

Alexander, D. C. (2004). A Delphi study of the trends or events that will influence the future of California charter schools. Digital Abstracts International, 65 (10), 3629. (UMI No. 3150304).

Alexander, W. D. (2010). Choosing key sizes for cryptography. *Information Security Technical Report* (UK). February. Volume 15, Issue 1, pages 21-27.

Alfor, J. and Greve, C. (2017). Strategy in the public and private sectors: similarities, differences and changes. *Administrative Science,* 7 (35), 1-17

Al-Haidari, F., Sqalli, M., Salah, K. and Hamodi, J. (2009). An Entropy-Based Countermeasure against Intelligent DOS Attacks Targeting Firewalls. *IEEE International Symposium on Policies for Distributed Systems and Networks* (USA). Pages 41-44.

Alin, D., Richard, H., Avinash, V. and Kevin, K. Z. (2010). Policy-aware sender anonymity in location based services. *International Conference on Advanced Information Networking and Applications (AINA'06)*. Volume 1, pages 133-144.

AlKaabi, A. (2014). *Strategic framework to minimise information security risks in the UAE.* PhD (Information Systems), University of Bedfordshire Repository. UK.

Allan, T., Po-WahYau, and MacDonald, John A. (2010). Privacy threats in a mobile enterprise social network. *Information Security Technical Report* (UK). May. Volume 15, Issue 2, pages 57-66.

Allodi, L, Chotza, T., Panina, E. and Zannone. N. (2020). The Need for New Antiphishing Measures Against Spear-Phishing Attacks. *IEEE Security & Privacy, vol. 18, no. 2*. Pp. 23-34. Doi: 10.1109/MSEC.2019.2940952.

Allsopp, W. (2017). *Advanced Penetration Testing: Hacking the World's Most Secure Networks*. Wiley (USA). ISBN-13: 978-1119367680.

Almeshekah, Mohammed. H., and Spafford, Eugene. H. (2014). Planning and Integrating Deception into Computer Security Defenses. *New Security Paradigms Workshop (NSPW'14)*, (Victoria, BC, Canada).

Almeshekah, Mohammed. H., and Spafford, Eugene. H. (2016). Cyber Security Deception. *Springer*. Springer International Publishing (Switzerland) 2016-p25-52 (DOI 10.1007/978-3-319-32699-3_2)

Al-Qutayri, M., YeobYeun, C., and Khalifa, B. (2010). Framework for secure wireless health monitoring and remote access system. *International Journal of Internet Technology and Secured Transactions*. Vol. 2, No.3/4, pages 380–398.

Al-Shaer, E., Wei, J., Hamlen, K. W., and Wang, C. (2019). Towards intelligent cyber deception systems. *Autonomous Cyber Deception*. Springer, pp. 21–33.

Alshammari, A., Rawat, D. B., Garuba, M., Kamhoua, C. A. and Njilla, L. L. (2020). *Deception for Cyber Adversaries: Status, Challenges, and Perspectives*. Wiley Online Library, pp. 141–160.

Alvarez, M., Bradley, N. and Cobb, P. (2017) Threat Intelligence. *IBM XForce* (USA). Available at: https://assets.documentcloud.org/documents/3527813/IBM-XForce-Index-2017-FINAL.pdf. Visited on 30th Oct 2017

Al-Wahaibi, S. (2016). *Hacking Countermeasure Framework*. MSc (Computer Science), Universiti Technologi Malaysia. Skudai.

Amit, V. (2001). MalTRAK: Tracking and Eliminating Unknown Malware. *Computer Security Applications Conference*. December. Pages 311-321.

Amitabh, S. and Ben, S. (2008). One-Way Signature Chaining. a new paradigm for group cryptosystems. *International Journal of Information and Computer Security* (Australia). Vol. 2, No.3, pages 268-296.

Amoroso, E. (2013). *Cyber Attack: Protecting National Infrastructure*. Butterworth-Heinemann (USA).

Amoroso, E. (2017). *2017 TAG Cyber Security Annual*. TAG Cyber LLC (USA). Available at: https://www.imperva.com/docs/Volume-1-TAG-Cyber-Security-Annual-Fifty-Controls.pdf. Visited on: 20th October/2017.

Andrew L., Michael, D., Indrajit, R., Ramakrishna, T. and Hailin, W. (2008). Origins: an approach to trace fast spreading worms to their roots. *International Journal of Security and Networks* (USA). Vol. 3, No.1, pages 36–46.

Andrew S., Joseph, A. C. and Dinesh, S. D. (2008). Mitigating Consumer Perceptions of Privacy and Security Risks with the Use of Residual RFID Technologies through Governmental Trust. *Journal of Information System Security*. Washington DC, USA: Information Institute Publishing. Volume 4, Number 1, pages 41–65.

Andy, J. and Martin, T. (2010). Digital forensics and the issues of identity. *Information Security Technical Report* (UK). Volume 15, Issue 2, pages 67-71.

Antonietta, S., Neeli, R. P. and Dimitris, M. K. (2009). A Threat Analysis Methodology for Security Evaluation and Enhancement Planning. *International Conference on Emerging Security Information, Systems and Technologies.* Pages 262-267.

Anwar, A. H., Kamhoua, C., and Leslie, N. (2020). Honeypot allocation over attack graphs in cyber deception games. *International Conference on Computing, Networking and Communications (ICNC)*, pp. 502–506.

Anwar, M., Zhao, Z. and Fong, P. (2010). An access control model for Facebook-style social network systems. *University of Algary Technical Report 2010-959-08.* Alberta, Canada: University of Algary.

Arash, B., Kiyana, Z. and Shahriar, M. (2011). A framework for cyber war against international terrorism. *International Journal of Internet Technology and Secured Transactions*. Vol. 3, No.1, pages 29 – 39.

Arati, B., Vinod, G. and Liviu, I. (2011). Detecting Kernel-Level Rootkits Using Data Structure Invariants. *IEEE Transactions on Dependable and Secure Computing*. September/October. Vol. 8, no. 5, pages 670-684.

Artem, V., Jun, H. and Nargiza, B. (2008). *An Ontology Framework for Managing Security Attacks and Defences in Component Based Software Systems*. Australian Conference on Software Engineering (aswec 2008). Page 552-561.

Artemios, G. Voyiatzis, and Dimitrios, N. Serpanos. (2002). Active Hardware Attacks and Proactive Countermeasures. *IEEE Symposium on Computers and Communications (ISCC'02)*. Page 361.

Asaf, S., Robert, M., Yuval, E., and Chanan, G. (2009). Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey. *Information Security Technical Report*. February. Volume 14, Issue 1, Pages 16-29

Asaf, S., Yuval, F., Robert, M. and Yuval, E. (2011). Monitoring, analysis, and filtering system for purifying network traffic of known and unknown malicious content. *Security and Communication Networks*. August. John Wiley & Son Ltd (USA). Volume 4. Issue 8. pages 947–965.

Aubert, B.A., Rivard, S., and Patry, M. (2004). A transaction cost model of IT outsourcing. *Information & Management*, 41(7), 921-932.

Awais, S., Alessandro, G. and Sead, M. (2010). Security architecture and methodology for authorization of mobile agents. *International Journal of Internet Technology and Secured Transactions* (Sweden). Vol. 2, No.3/4, pages 271–290.

Awasthi, A. K. (2010). Remarks on the security of the strong proxy signature scheme with proxy signer privacy protection. *International Journal Information and Computer Security*. Vol. 4, No. 1, pages 24–29.

Bajak, Frank. (2020). *Research: Millions of smart devices vulnerable to hacking*. Apnews Publications. (USA). https://apnews.com/article/hacking-software-17d67bd69718c2d0d5f6e2493285abc2

Bakken, D., Parameswaran, R., Blough, D., Palmer, T., and Andy, A. (2004). Franz. Data Obfuscation: Anonymity and Desensitization of Usable Data Sets. *IEEE Security & Privacy* (USA). *Vol 2, Issue 6*. Pages 34-41.

Balachandran, V. and Emmanuel S. (2011). Software Code Obfuscation by Hiding Control Flow Information in Stack. *IEEE Workshop on Information Forensics and Security (WIFS)*. Pages 1-6.

Balsa, E., Troncoso, C. and Diaz, C. (2012). OB-PWS: Obfuscation-Based Private Web Search. *33rd IEEE Symposium on security and privacy (S&P 2012)*. IEEE computer society (USA). Pages 491-505.

Barmak, Meftah. (2010). One-third are victims of hacking. *Electronics Weekly* (USA). 16^{th} Jun. Iss. 2432, pages 8.

Barman, S. (2002). *Writing Information Security Policies*. New Riders (USA).

Barnes, C., Bautts, T., Lloyd, D., Ouellet, C., Postuns, J., Zudzian, D. and O'Farrel, N. (2002). *Hack Proofing Your Wireless Network*. Syngress (USA).

Baron, L. David. (2010). *Preventing attacks on a user's history through CSS*. Mozilla (USA).

Barrett, M. (2018), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, *NIST* Cybersecurity *Framework*. (USA). Available at: https://doi.org/10.6028/NIST.CSWP.04162018, https://www.nist.gov/cyberframework. Visited on: September 12, 2021.

Barry, A. C., Casey, G. C. and Chetan, S. S. (2009). An Exploratory Delphi Study among Small Business Executives on Adoption of Disaster Recovery Practices. *Journal of Information System Security*. Washington DC, USA: Information Institute Publishing. Volume 5, Number 1, pages 61–87.

Basak, A., Kamhoua, C. A., Gutierrez, S., Gutierrez, M., Anwar, A. H., and Kiekintveld, C. D. (2021). *Scalable Algorithms for Identifying Stealthy Attackers in a Game Theoretic Framework Using Deception*. Wiley Online Library.

Basin, D., Apkun, S., Schaller, P., and Schmidt, B. (2009). Let's get physical. Models and methods for real-world security protocols. In *Proceedings of the 22nd International Conference on Theorem Proving in Higher Order Logics*, TPHOLs '09. Springer (USA). Pages 1–22

Baskerville, R. & Pries-Heje, J. (2001). A multiple-theory analysis of a diffusion of information technology case. *Information Systems Journal*, 11(3), 181-212.

Basuki, R., Suhono, H., Jaka, S. and Kridanto, S. (2010). Threat Scenario Dependency-Based Model of Information Security Risk Analysis. *International Journal of Computer Science and Network Security*. August. Vol. 10 No. 8, pages 93-102.

Bayuk, J., Healey, J., Rohmeyer, P., Sachs, M., Schmidt, J., Weiss, J. (2012). *Cyber security policy guidebook*. John Wiley & Sons (USA).

Bazzell, M. and Carroll, J. (2016) *The Complete Privacy & Security Desk Reference*. CreateSpace Independent (USA). ISBN-13: 978-1522778905

Bazzell, M. (2016) Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information 5th Edition. CreateSpace Independent (USA). ISBN-13: 978-1530508907 (Social engineering)

Bazzell, M. (2016). *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information (5th Edition)*. CreateSpace Independent (USA). ISBN-13: 978-1530508907.

Beaver, Kevin (2012). *How to use Metasploit commands for real-world security tests*. TechTarget Inc (USA). Available at :http://searchsecurity.techtarget.com/. Visited on: 7th April 2017.

Becker, M., Russo, A., and Sultana, N. (2012). Foundations of Logic-Based Trust Management. *33rd IEEE Symposium on security and privacy (S&P 2012)*. IEEE computer society (USA). Pages 161–175

Beebe, N. and Clark, J. (2007). A Model for Predicting Hacker Behavior. *Journal of Information System Security*. Washington DC, USA: Information Institute Publishing. Volume 3, Number 3. Pages 3–20.

Bell, D. E. and LaPadula, L. J. (1973). Secure computer systems. mathematical foundations and model. *The MITRE Corp. Technical Report M74-244*. May. Bedford, Mass. USA: MITRE Corporation.

Bell, J. B. and Whaley, B. (1991) *Cheating and Deception*. Transaction Publishers (New Brunswick-USA).

Benjamin, U. and Wong, J. (2008). An agent-based framework for intrusion detection alert verification and event correlation. *International Journal of Security and Networks* (USA). Vol. 3, No.3, pages 193-200.

Benoît, D., Stefan, B., Kieran, M. and Sakir, S. (2010). Analysis of information leakage from encrypted Skype conversation. *International Journal of Information Security*. Volume 9, No. 5, pages 313-325.

Berkant, U. (2011). Integrating identity-based and certificate-based authenticated key exchange protocols. *International Journal of Information Security*. Volume 10, Number 4, pages 201-212.

Bernardeschi, C., Domenici, A. and Palmieri, M. (2020). Formalization and co-simulation of attacks on cyber-physical systems. *J Comput Virol Hack Tech* **16,** 63–77. https://doi.org/10.1007/s11416-019-00344-9

BERR (2012). White Paper: *Information security: How to write an information security policy*. Department for Business, Enterprise & Regulatory Reform (UK). Available at: http://webarchive.nationalarchives.gov.uk/. Visited on: 7th April 2017.

Bhattarai, A. and Dasgupta, D. (2011). A Self-Supervised Approach to Comment Spam Detection Based on Content Analysis. *International Journal of Information Security and Privacy (IJISP)* (USA). Volume 5, Issue 1.

Bishop, M. (2017). *Computer Security*. Addison Wesley (USA). ISBN-13: 978-0321712332.

Bishop, M., Engle, S., Howard, D. and Whalen, S. (2012). A Taxonomy of Buffer Overflow Characteristics. *IEEE Transactions on Dependable and Secure computing*. IEEE (USA). May-June. Vol. 9, no.3, No. 3. Pages 305-317.

Blackmer, M. (2017). *At Industrial Control Security Con: Will hack IoT*. Security Ledger (USA). Available at: https://securityledger.com/2017/01/at-industrial-control-security-con-will-hack-iot. Visited on: 20th October/2017.

Blumstein, A. (1978). *Introduction in deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates*. Washington, DC: National Academy of Sciences.

Bob, M., Mason, B., Alan, P. and Dennis, K. (2011). *CWE/SANS Top 25 Most Dangerous Software Errors*. The MITRE Corporation (USA). June 29. Available at: http://cwe.mitre.org/top25/. Visited on: 25th July 2017.

Boland, R., and Collopy, F. (2004). *Managing as designing*. Stanford University Press.

Bolkan, J. (2017). IT Spending to Hit $3.5 Trillion in 2017. *Campus Technology* (USA). July 2017. Available at: https://campustechnology.com/articles/2017/07/25/research-it-spending-to-hit-3.5-trillion-in-2017.aspx. Visited on: 24 September 2017.

Bonneau, J., Herley, C., Oorschot, P, and Stajano, F. (2012). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. *33rd IEEE Symposium on security and privacy (S&P 2012).* IEEE computer society (USA). 2012. Pages 553-570.

Bonneau, Joseph (2012). The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. *33rd IEEE Symposium on security and privacy (S&P 2012).* IEEE computer society (USA). Pages 538–552.

Botacin, M., de Geus, P.L. and Grégio, A. (2019). "VANILLA" malware: vanishing antiviruses by interleaving layers and layers of attacks. *J Comput Virol Hack Tech* **15,** 233–247. https://doi.org/10.1007/s11416-019-00333-y

Bowles, M. (2012). The Business of Hacking and Birth of an Industry. *Bell Labs Technical Journal, 17*(3): 5-16.

Boyle, R. J. and Panko, R. J. (2021). *Corporate Computer Security*. 5th edition. PEARSON (USA).

Bozman, J., and Chen, G. (2014). White paper: *Best Practice for Cloud Adoption*. June. IBM Corporation (USA). Available at: https://www.ibm.com/cloud-computing/files/77_IDC_Whitepaper_BestPractice_for_Cloud_Adoption.pdf. Visited on 30th Oct 2017.

Brancik, Kenneth C. (2008). *Insider computer Fraud.* Auerbach Publications (USA).

Bratus, S. (2007). What hackers learn that the rest of us don't. *IEEE Security & Privacy*. July/August. Vol 5 No. 4 Pages 72-75.

Brdiczka, O., Liu, J., Price, B., Shen, J., Patil, A., Chow, R., Bart, E., and Lam, N. (2012). Proactive Insider Threat Detection through Graph Learning and Psychological Context. *IEEE CS on Security and Privacy Workshops.* IEEE computer society (USA). Pages 142-149.

Breach (2009). White paper: *Web Hacking Incidents Report 2009*. Breach Security Incorporation (USA).

Breach (2010). White paper: *WEB Defender and OWASP top ten*. Breach Security Incorporation (USA).

Brian, S. and Owen, M. (2011). Creating and enforcing access control policies using description logic techniques. *International Journal of Internet Technology and Secured Transactions* (Ireland). Vol. 3, No.3, pages 253-278.

Brunette, Glenn and Mogull, Rich (2009). White Paper: *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*. Cloud Security Alliance (USA).

Brungs, A. & Jamieson, R. (2005). Identification of legal issues for computer forensics. Information Systems Management, 22(2), 57 - 66.

Buchanan, R. (1992). Wicked problems in design thinking. *Design issues:* 5-21.

Buecker, A., Borrett, M., Lorenz, C. and Powers, C. (2013). *Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security*. Redbooks (USA). ISBN: 0738437891. Available at: http://www.redbooks.ibm.com/redbooks/pdfs/sg248100.pdf. Visited on: 12/August/2017

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523– 548.

Burch, H. and Cheswick, B. (2000). Tracing anonymous packets to their approximate source. In *Proceedings of LISA*. (USA).

Burgess, C., Gallego, P., Gourley, P., Swan, C. (2017). White Paper: *Know Your Enemy: Threat Intelligence Enables Companies to Defend Against Cyber Attacks. IBM SCmagazine (USA).* Available at: https://www.scmagazine.com/. Visited on: 2nd April 2017

Burns, B., Killion, D., Beauchesne, N. and Moret, E. (2007). *Security Power Tools*. 1st edition. O'Reilly Media (USA).

Burns, F.M. (1998). Essential components of schizophrenia care: a Delphi approach. *Acta Psychiatry Scand*, 98, 400-405.

Burr, W., Dodson, D., and Polk, W. (2006). Electronic authentication guideline. *NIST Technical Report*. (USA).

Byers, Bob. and Owen, Harold. (2021), *Automation Support for CVE Retrieval*. National Institute of Standards and Technology. (US). Available at: https://csrc.nist.gov/CSRC/media/Projects/National-Vulnerability-Database/documents/web%20service%20documentation/Automation%20Support%20for%20CVE%20Retrieval.pdf (Accessed September 12, 2021)

Calder, A. (2008). Developing an IT Governance framework. *IT adviser*. Winter. Issue 56.

Caldwell, A. and Curran, K. (2020). A Critique of Active Defense or 'Hack Back'. International Journal for Information Security Research (IJISR), Volume 10, Issue 1. P957-961

Campion, M., PredaMila, M., Giacobazzi, R. (2021). Learning Metamorphic Malware Signatures From Samples. *Journal of Computer Virology and Hacking Techniques (2021) 17:167–183* https://doi.org/10.1007/s11416-021-00377-z.

Cappelli, D.M., Moore, A.P., Trzeciak, R.F. (2020). The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Addison-Wesley. Available online: http://ptgmedia.pearsoncmg.com/images/9780321812575/samplepages/9780321812575.pdf (accessed on 27 May 2020)

Carl, C. (2009). Human Factors in Information Security: The insider threat – Who can you trust these days. *Information Security Technical Report* (UK). November. Volume 14, Issue 4, pages 186-196.

Carminati, B. and Ferrari, E. (2009). Enforcing relationships privacy through collaborative access control in web-based social networks. *In Proceedings of the 5th International Conference on Collaborative Computing. Networking, Applications and Worksharing (CollaborateCom '09)*. November. Washington DC, USA: CollaborateCom.

Carminati, B., Ferrari, E., and Perego, A. (2006). Rule-based access control for social networks. *The OTM 2006 Workshops*. Ser. LNCS, vol. 4278. October. Springer (USA). Pages 1734–1744.

Casey, E. (2011). *Digital evidence and computer crime.* 3rd edition. Elsevier (USA).

Cavusoglu, H., Son, J., & Benbasat, I. (2009). *Information security control resources in organizations: A multidimensional view and their key drivers* (Working Paper). Vancouver: Sauder School of Business, University of British Columbia.

Cha, S., Avgerinos, T., Rebert, A. and Brumley, D. (2012). Unleashing Mayhem on Binary Code. *33rd IEEE Symposium on security and privacy (S&P 2012).* IEEE computer society (USA). Pages 380-394.

Chakraborty, A., Garg, M. K., Majumdar, A. K. and Sural, S. (2008). Attack recovery from malicious transactions in distributed database systems. *International Journal of Information and Computer Security* (India). Vol. 2, No. 2, pages 197–217.

Chandler, A. (1996). The changing definition and image of hackers in popular discourse. *International Journal of the Sociology of Law, 24*(2): 229-251

Chaney, B. H., Eddy, J. M., Dorman, S. M., Glessner, L. L., Green, B. L., & Lara-Alecio, R. (2009). A primer on quality indicators of distance education. *Society for Public Health Education,* 10(2), 222-231.

Chapple, Mike (2012). *Egress filtering*. TechTarget Inc (USA). Available at: http://searchsecurity.techtarget.com/. Visited on: 27th April 2017.

Chen, Jim. Q. (2020). A Framework of Partnership. *The Cyber Defense Review, Volume 5 Number 1.* (USA). 15-28.

Chen, Y., Nyemba S., and Malin, B. (2012). Detecting Anomalous Insiders in Collaborative Information Systems. *IEEE Transactions on Dependable and Secure Computing*. IEEE (USA). May/June**.** Vol. 9, no. 3. Pages 332-344**.**

Cheng, A. and Friedman, E. (2005). Sybil proof reputation mechanisms. *In Proceedings of the 2005 ACM SIGCOMM Workshop on Economics of peer-to-peer systems (P2PEcon'05)*. August. Philadelphia, PA, USA: ACM SIGCOMM. Pages 128–132.

Chenjia, W., Kevin, P. M. and Weisong, Shi. (2009). HACK: A Health-Based Access Control Mechanism for Dynamic Enterprise Environments. *International Conference on Computational Science and Engineering*. Vol. 2, pages 795-801.

Chess, B. and West, J. (2007). *Secure Programming with Static Analysis*. 1st edition. Addison Wesley (USA).

Chesti, I., Humayun, M., Sama, N. and Jhanjhi N. (2020). Evolution, Mitigation, and Prevention of Ransomware. *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*. IEEE. USA.

Chien-Chuan, L. and Ming-Shi, W. (2008). Genetic-clustering algorithm for intrusion detection system. *International Journal of Information and Computer Security* (Taiwan). Vol. 2, No.2, pages 218-234.

Cho and Ben-Asher (2017). Cyber defense in breadth: Modeling and analysis of integrated defense systems. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology (USA)*. ISSN: 1548-5129. 16th March 2017. Available from https://doi.org/10.1177/1548512917699725. Visited on: 20th June/2017.

Cho J.-H., and Ben-Asher, N. (2018). Cyber defense in breadth: Modeling and analysis of integrated defense systems. *The Journal of Defense Modeling and Simulation*, vol. 15, no. 2, pp. 147–160.

Cho, J., Sharma, D., Alavizadeh, H., Yoon, S., Ben-Asher, N., Moore, T., Kim, D., Lim, S. and Nelson, F. (2020). Toward proactive, adaptive defense: A survey on moving target defense. *IEEE Communications Surveys Tutorials*, pp. 1–1, 2020.

Chris, S. (2010). Cryptography in the real world. *Information Security Technical Report* (UK). February. Volume 15, Issue 1, pages 2-7.

Christensen, L. B., Johnson, R. B. and Turner, L. A. (2010). *Research Methods*. 11th edition. Allyn and Bacon (USA).

Christina, T. (2011). *IT organization of the future is a hybrid*. TechTarget Inc (USA). July. Available at: http://itknowledgeexchange.techtarget.com/. Visited on: 27th Jul 2017.

Chua, W.F. (1986). Radical developments in accounting thought. *The Accounting Review*, 61(4), 601-632.

Chunsheng, Liu and Huang, Yu. (2007). Effects of Embedded Decompression and Compaction Architectures on Side-Channel Attack Resistance. *IEEE VLSI Test Symposium (VTS'07)*. Page 461-468.

Churchhouse, R. (2002). *Codes and Ciphers*. 1stedition. Cambridge University Press (USA).

Chwan-Hwa, 'John' Wu, Tong, L., Chun-Ching, 'Andy' Huang and David, J. I. (2009). Modelling and simulations for Identity-Based Privacy-Protected Access Control Filter (IPACF) capability to resist massive denial of service attacks. *International Journal of Information and Computer Security* (USA). Vol. 3, No.2, pages 195–223.

Cicotte, C. (2017). *Defense in Breadth: Securing the Multi-Cloud Hydra*. Dell Incorporation (USA). Available from https://www.cio.com/article/3201959/analytics/Defense-in-Breadth.html. Visited on: 25th June/2017.

CIS. (2017). White Paper: *Security configuration Benchmark*. Center for Internet Security organization (USA). Available at: https://downloads.cisecurity.org/?bypassToken=FRgh8EXgnw9JY2rMUvK0UdedJu3BAkq2#/. Visited on: 27th October 2017.

Cisco. (2017). White paper: *Cisco Security Agent*. Cisco Corporation (USA). Available at: http://www.cisco.com/go/csa. Visited on 13th September 2017.

Cisco. (2021). Cisco Trust Agent 2.1. Available from https://cisco-trust-agent.software.informer.com Visited on: 5th October/2021.

Clarke, Justin (2009). *SQL Injection Attacks and Defense*. Syngress (USA).

Clarke, R. A., & Knake, R. K. (2011). *Cyber war*. HarperCollins. (USA).

Cobb, Michael (2012). *Locking down your Web applications*. TechTarget Inc (USA). Available at: http://searchsecurity.techtarget.com/. Visited on: 27th February 2017.

Cohen, Fred. (2012). Forensic Methods for Detecting Insider Turning Behaviors. *IEEE CS on Security and Privacy Workshops*. IEEE computer society (USA). Pages 150-158.

Collins, K. M. T., Onwuegbuzie, A. J., & Jiao, Q. G. (2007). A mixed methods investigation of mixed methods sampling designs in social and health science research. *Journal of Mixed Methods Research*, 1(3), 267–294.

Collins, S., Osborne, J., Ratcliffe, M., Millar, R., & Duschl, R. (2001). What 'ideasabout-science' should be taught in school science? A Delphi study of the expert community. *Paper presented at the American Educational Research Association (AERA) national conference*. Seattle, WA, April 2001. pp 28.

Constantin, L. (2012). NSA Chief Seeks Help From Hackers. *Computerworld, 46*(14): 4-4.

Cox, Chris. (2012). *Network security checklist*. TechTarget Inc (USA). Available at: http://searchnetworking.techtarget.com/. Visited on: 27th April 2017.

Cox, K. and Greg, C. (2004). *Managing Security with Snort and IDs Tools*. 1st edition. O'Reilly Media (USA).

Cremers, C., Rasmussen, K., Schmidt, B., and Capkun, S. (2012). Distance Hijacking Attacks on Distance Bounding Protocols. *33rd IEEE Symposium on security and privacy (S&P 2012).* IEEE computer society (USA). Pages 113-127.

Creswell, J. W. (2009). *Reseaerch Design: Qualitative, Quantitative and Mixed Methods approaches*. London: Sage.

Creswell, J. W. (2015). *Educational Research: Planning, Conducting and Evaluating Quantitative and Qualitative Research (5th Ed.)*. Boston: Pearson.

Cristofaro, E., Soriente, C., Tsudik, G. and Williams, A. (2012). Hummingbird: Privacy at the Time of Twitter. *33rd IEEE Symposium on security and privacy (S&P 2012).* IEEE computer society (USA). Pages 285–299.

CSIS. (2021). *Strategic Technologies Program: Significant Cyber Incidents*. Center for Strategic and International Studies. (USA). Available at: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. Visited date: 29th September 2021.

CVE Mitre (2021). *CVE list of publicly disclosed cybersecurity vulnerabilities.* MITRE Corporation (USA). Available at: https://cve.mitre.org/cve/. Visited on: 8th Sep 2021.

CWE (2017). *A Community-Developed List of Software Weakness Types.* Common Weakness Enumeration Organization (USA). Available at: https://cwe.mitre.org/data/index.html. Visited on: 8th October 2017.

CWE Mitre. (2021). *2021 CWE Top 25 Most Dangerous Software Weaknesses*. The MITRE Corporation (USA). June 29. Available at: https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html. Visited on: 25th August 2021.

Cyberpro. (2019). Strategies to Mitigate Cyber Security Incidents. Australian Cyber Security Centre. (Australia). Available from https://www.cyberpro.com.au/wp-content/uploads/2019/11/protect-strategies-to-mitigate-cyber-security-incidents-february-2017.pdf.

CynoSure Prime (2017). *320 Million Hashes Exposed*. Available from https://cynosureprime.blogspot.my/2017/08/320-million-hashes-exposed.html. Visited on: 2nd September/2017.

D'Arcy, J., and Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences, 43*(6), 1091–1124.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research, 20*(1), 79–98.

Dahbu, R., Lim, c. and Purnama, J. (2017). Enhancing Honeypot Deception Capability Through Network Service Fingerprinting. *Journal of Physics: Conf Series 801 (2017)*. 12057 doi:10.1088/1742-6596/801/1/012057)

Dai, S., Wei, T., Zhang, C., Wang, T., Ding, Y., Liang, Z. and Zou, W. (2012). A Framework to Eliminate Backdoors from Response-Computable Authentication. *33rd IEEE Symposium on security and privacy (S&P 2012)*. IEEE computer society (USA). Pages 3-17.

Dalit, N. and Moni, N. (2003). Protecting Cryptographic Keys: The Trace-and-Revoke Approach. *Computer*. (USA). July. Vol. 36, no. 7, pages 47-53.

Dalkey, N. C. (1969). The Delphi Method: An Experimental Study of Group Opinion. In N. C. Dalkey, D. L. Roueke, R. Lewis, and D. Snyder (Eds). *Future*. IPC Business Press Limited. (USA). Vol. 1, pp. 408-426

Dalkey, N. C., and Rourke, D. L. (1971). Experimental Assessmen of Delphi Procedures with Group Value Judgement. *Future*. IPC Business Press Limited. (USA)

Damiani, E., Proctor, S., and Singhal, A. (2011). Security and Dependability in SOA and Business Processes. *IEEE Transactions on services computing*. IEEE (USA). October-December. Vol. 4, No. 4. Pages 255 - 256.

Damiani, M. L., Bertino, E. and Perlasca, P. (2007). Data security in location-aware applications. an approach based on RBAC. *International Journal of Information and Computer Security* (Italy). Vol. 1, No.1/2, pages 5–38.

Damien, S. (2009). Multiapplication smart card. Towards an open smart card?. *Information Security Technical Report* (UK). May. Volume 14, Issue 2, pages 70-78.

Dargahi, T., Dehghantanha, A. and Bahrami, P. (2019). A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. *J Comput Virol Hack Tech* 15, 277–305. https://doi.org/10.1007/s11416-019-00338-7

Darke, P., Shanks, G., & Broadbent, M. (1998). Successfully completing case study research: Combining rigor, relevance, and pragmatism. *Information Systems Journal*, 8, 273-289.

Data Loss Database (2015). *Index of Largest Data Base Losses*. Data Loss Database Organization (USA). Available at: http://datalossdb.org/index/largest. Visited on: 12th July 2017

Davis, A. (2014). Safeguard database connection strings and other sensitive settings in your code. *MSDN Magazine*. Available at: http://msdn.microsoft.com/en-us/magazine/cc164054.aspx. Visited on: 25th April 2014.

Davis, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems: theory and results* (PhD dissertation). Massachusetts Institute of Technology, Cambridge, MA

Davis, M., Bodmer, S. and Aaron, (2009). *Hacking Exposed: Malware and Rootkits Secrets & Solutions*. 3rdEdition. McGraw-Hill Osborne Media (USA).

Davod, S. and Khaleghei, H. (2007). On the vulnerability of Simplified AES Algorithm Against Linear Cryptanalysis. *International Journal of Computer Science and Network Security*. Jul. Vol. 7, No. 7, pages 257-263.

Defa, H. and Qiaoliang, L. (2010). Bandwidth efficient asymmetric fingerprinting based on one-out-of-two oblivious transfer. *International Journal of Information and Computer Security* (China). Vol. 4, No.2, pages 152–163.

Delbecq, A. L., Van de Ven, A. H. and Gustafson, D. H. (1975). *Group Techniques for Program Planning: A Guide to Nominal Group and Delphi Processes*. Longman Higher Education.

Dell SecureWorks (2014). *Advanced Threat Protection with Attack model*. Dell Incorporation (USA). Available at: https://www.secureworks.com/resources/sb-advanced-threat-protection. Visited on: 20th October/2017.

Denning, D. E. (2006). *A View of Cyberterrorism Five Years Later, "Readings in Internet Security. Hacking, Counter hacking, and Society (K. Himmaed.)*". Jones and Bartlett Publishers (USA).

Denning, D. E. (2007a). *Assessing the CNO Threat of Foreign Countries, in "Information Strategy and Warfare (J. Arquilla and D. Borer eds.)"*. Routledge (USA).

Denning, D. E. (2007b). *The Ethics of Cyber Conflict, in "Information and Computer Ethics (K. E. Himma and H. T. Tavani eds.)"*. Wiley (USA).

Denning, P. (1976). Fault tolerant operating systems. *ACM Computing Surveys*. Vol. 8, no. 4. Dec. (USA). Pages 359–*389*.

Denning, P. J. and Denning, D. E. (2010). Discussing Cyber Attack. *Comm. of the ACM*, Sept. Vol. 53, No. 9. (USA).

Desmond, L., Watters, P., Xin-Wen, Wu. and Li Sun. (2010). Windows Rootkits: Attacks and Countermeasures. *Cybercrime and Trustworthy Computing Workshop*. Pages 69-78.

Dey, D., Lahiri, A., and Zhang, G. (2015) Optimal Policies for Security Patch Management. *INFORMS Journal on Computing* (USA). Volume 27, Number 3, Summer 2015. 462-477

Dhanjani, N., Rios, B. and Hardin, B. (2009a). *Hacking the Next Generation*. O'Reilly (USA).

Dhanjani, N., Rios, B. and Hardin, B. (2009b). *Hacking: The Next Generation (Animal Guide).* O'Reilly Media (USA).

Dillman, D., Smyth, J., Christian, LM. (2009). Internet, Mail and Mixed-Mode Surveys: The tailored design method. John Wiley and Sons (USA).

Dimitrios, P., Chez, C., and Fred, P. (2010). The status of National PKIs – A European overview. *Information Security Technical Report* (Greece). February. Volume 15, Issue 1, Pages 13-20.

Dingledine, R., Mathewson, N. and Syverson, P. (2004). Tor: the second generationonion router. In *Proceedings of conference on USENIX Security Symposium*. (USA).

Dolan-Gavitt, B., Leeky, T., Zhivichy, M., Giffin, J., and Virtuoso, W. (2011). Narrowing the Semantic Gap in Virtual Machine Introspection. *32nd IEEE Symposium on security and privacy (S&P 2011).* IEEE computer society (USA). Pages 297–312

Douceur, J. (2002). The Sybil attack. *International Workshop on Peer-to-Peer Systems (IPTPS'02)*. Ser. LNCS, vol. 2429. March. Cambridge, MA, USA: IPTPS. Pages 251–260.

Dover, J. (2016). White Paper: *Defense in breadth*. Information Security Magazine (USA) 19th January 2016. Available from https://www.infosecurity-magazine.com/opinions/defence-in-breadth/. Visited on: 25th June/2017.

Drake, Victoria. (2021). *Threat Modeling*. OWASP (USA). Available at: https://owasp.org/www-community/Threat_Modeling Visited on 2nd October 2021.

Duchêne, J., Le Guernic, C. and Alata, E. (2018). State of the art of network protocol reverse engineering tools. *J Comput Virol Hack Tech* **14,** 53–68. https://doi.org/10.1007/s11416-016-0289-8

Dyer, K., Coull, S., Ristenpart, T. and Shrimpton, T. (2012). Peek-a-Boo, I Still See You: Why Efficient Traffic Analysis Countermeasures Fail. *33rd IEEE*

Symposium on security and privacy (S&P 2012). IEEE computer society (USA). Pages 332–346

EC-Council (2016a). *Computer Forensics: Investigating Network Intrusions and Cybercrime (2nd Edition)*. Course Technology (USA). ISBN 13: 9781305883505.

EC-Council (2016b). Ethical Hacking and Countermeasures: Web Applications and Data Servers (2nd Edition). Course Technology (USA). ISBN-13: 978-1305883451.

EC-Council (2016c). Ethical Hacking and Countermeasures-Secure Network Infrastructures (2nd Edition). Course Technology (USA). ISBN-13: 978-1305883468.

EC-Council (2016d). Computer Forensics: Investigating File and Operating Systems, Wireless Networks, and Storage (CHFI) (2nd Edition). Course Technology (USA). ISBN-13: 978-1305883482.

Efendi, A. I. M., Ibrahim, Z., Zawawi, M. N. A., Abdul Rahim, F., Pahri, N. A. M., and Ismail, A. (2019). A survey on deception techniques for securing web application. *IEEE 5th Int'l Conf on Big Data Security on Cloud (BigDataSecurity)*, pp. 328–331.

Eilam, E. (2005). *Reversing: Secrets of Reverse Engineering*. Wiley Publishing (USA).

El-Kosairy A., and Azer, M. A. (2018). A new web deception system framework. *International Conference on Computer Applications & Information Security (ICCAIS)*. IEEE, pp. 1–10.

Ellen, M. (2010). Banks battling crooks who hijack customer PCs. *Network World* (USA). Jun 21. Vol. 27, Iss. 12, pages 1-3.

EMA (2010). *TrendMicro's End-to-End Vulnerability Management: A New Approach to Layered Security*. Enterprise Management Associates (USA). Available at: https://www.mercurymagazines.com/pdf/NCTRENDMICRO3.pdf. Visited on: 12 July 2017.

E-Oman. (2019). Information Security Management Framework. Information Technology Authority (Oman). Available at:

https://oman.om/wps/wcm/connect/18655e32-ea30-4dd9-8b51-4023051aa223/Information+Security+Management+Framework-Final+draft.pdf?MOD=AJPERES&CACHEID=18655e32-ea30-4dd9-8b51-4023051aa223. Visited on: 06th August 2021.

Eric, S. (2011). *Using NFS to support a virtual server environment*. TechTarget Inc (USA). July. Available at: http://searchvirtualstorage.techtarget.com/. Visited on: 12 July 2017.

Eskandari, R., Shajari, M. and Ghahfarokhi, M.M. (2019).. ERES: an extended regular expression signature for polymorphic worm detection. *J Comput Virol Hack Tech* 15, 177–194. Doi.org/10.1007/s11416-019-00330-1

Fadia, A. (2006). *The Unofficial Guide to Ethical Hacking*. 2ndedition. Thomson Course Technology (Canada).

Fazirulhisyam, H. and Abbas, J. (2011). A generic sampling framework for improving anomaly detection in the next generation network. *Security and Communication Networks*. John Wiley & Son Ltd (USA). August. Volume 4. Issue 8, pages 919–936.

Ferguson-Walter, K. J. (2020). *An empirical assessment of the effectiveness of deception for cyber defense*. Ph.D. dissertation, University of Massachusetts Amherst.

Fernando, E., Elena, S. A., Paul, H., Haixia, J. and Stephanie, F. (2007). Protecting data privacy through hard-to-reverse negative databases. *International Journal of Information Security*. July 24. Volume 6, Number 6, pages 403-415.

Fichman, R.G., & Kemerer, C.F. (1999). The illusory diffusion of innovation: An examination of assimilation gaps. *Information Systems Research*, 10(3), 255-275.

Filiol, E., Delong, M. and Nicolas, J. (2020). Statistical and combinatorial analysis of the TOR routing protocol: structural weaknesses identified in the TOR network. *J Comput Virol Hack Tech* 16, 3–18. doi.org/10.1007/s11416-019-00334-x (

Filkins, B. (2017) *White Paper: Sensitive Data at Risk: The SANS 2017 Data Protection Survey. SANS Institute Organization (USA)*. Available at:https://www.sans.org/reading-room/whitepapers/threats/sensitive-data-risk-2017-data-protection-survey-37950. Visited on: 28th September 2017.

Flow, S. (2017). *How to Hack Like a PORNSTAR: A step by step process for breaking into a BANK (Hacking the planet)*. CreateSpace Independent (USA). ISBN-13: 978-1520478517.

Flowerday, S. and Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security*. Volume 61, August 2016, Pages 169-183.

Flynn, H. (2006). *Designing and Building Enterprise DMZs*. Syngress Publishing (USA).

Follis, Luca. and Adam, Fish. (2020a). *Hacking for Profit*. MIT Press. USA

Follis, Luca. and Adam, Fish. (2020b). *Hacking the State Boundary*. MIT Press. USA

Fomichev, V.M., Koreneva, A.M., Miftakhutdinova, A.R., Zadorozhny, D.I.: Evaluation of the maximum performance of block encryption algorithms. Math. Aspects Cryptogr. **10**(2), 7–16 (2019)

Fong, P. (2011a). Preventing Sybil Attacks by Privilege Attenuation: A Design Principle for Social Network Systems. *32nd IEEE Symposium on security and privacy (S&P 2011)*. IEEE computer society (USA). Pages 263–278

Fong, P. W. L. (2011b). Relationship-based access control: protection model and policy language. *In Proceedings of the First ACM Conference on Data and Application Security and Privacy (CODASPY'11)*. February. San Antonio, TX, USA: CODASPY. Pages 191–202.

Fong, P. W. L. and Siahaan, I. (2011). Relationship-based access control policies and their policy languages. *In Proceedings of the 16th ACM Symposium on Access Control Models and Technologies (SACMAT'11)*. June. Innsbruck, Austria: SACMAT.

Fonyi, S. (2020). Overview of 5G Security and Vulnerabilities. *The Cyber Defense Review, Vol 5 No 1*. (USA). 117-134.

Forni, A. and Vandermeulen, R. (2017). World IT Spending Forcast. *Gartner* (USA). September 2017. Available at: http://www.gartner.com/newsroom/id/3568917. Visited on: 24 September 2017.

Foster, J. C. (2006). *Writing Security Tools and Exploits*. 1st edition. Andrew Williams (Canada).

Fowler, A. (2011). *Do Not Track Adoption in Firefox Mobile is 3x higher than desktop*. Mozilla Inc (USA). November.

Francis Hsu, Hao Chen, Thomas Ristenpart, Jason Li and Zhendong Su. (2006). Back to the Future: A Framework for Automatic Malware Removal and System Repair. *Annual Computer Security Applications Conference (ACSAC'06)*. Pages 257-268.

Fredrikson, M. And Livshits, B. (2011). REPRIV: Re-Imagining Content Personalization and In-Browser Privacy. *32nd IEEE Symposium on security and privacy (S&P 2011).* IEEE computer society (USA). Pages 131-146.

Friedman, Sara. (2018). White paper: *A new model for cyber risk management*. Defense Systems (USA).. Available at: https://defensesystems.com/articles/2018/07/20/prism-risk-management-model.aspx. Visited on: 12th Nov 2021.

Friend, J. G. (2001). A Delphi study to identify the essential tasks and functions for ADA coordinators in public higher education. Digital Abstracts International, 62 (04), 1339. (UMI No. 3012967).

Fu, Y. and Lin, Z. (2012). Space Traveling across VM: Automatically Bridging the Semantic Gap in Virtual Machine Introspection via Online Kernel Data Redirection. *33rd IEEE Symposium on security and privacy (S&P 2012).* IEEE computer society (USA). Pages 586-600.

Gallardo, F., and Yuste, A. P. (2020). SCER spoofing attacks on the galileo open service and machine learning techniques for end-user protection. *IEEE Access*, vol. 8, pp. 85515–85532. doi: 10.1109/ACCESS.2020.2992119.

García, T., Díaz, V., Maciá, F., and Vázquez, E. (2009). Anomaly-based network intrusion detection. Techniques, systems and challenges. *Computers and Security*. February. Volume 28, Issue 1-2, pages 18-28.

Garfinkel, T. (2003). Traps and pitfalls: Practical problems in system call interposition based security tools. In *Network and Distributed Systems Security Symposium (NDSS)*. (USA).

Gartzke, Erik and Lindsay Jon R. (2015) Weaving Tangled Webs: Offense, Defense, and Deception. *Cyberspace Security Studies*. Taylor & Francis Group, LLC (October 2015). Available at: http://dx.doi.org/10.1080/09636412.2015.1038188. Visited on: 12th Jun 2017.

Gary, H. (2011). The State of IT Auditing in 2007. *Edpacs the EDP audit, control and security newsletter*. August. London: Taylor & Francis.

Gavel, P., Prasad, R., Rathore, N. and Yadav, D. (2020). Ethical Hacking and Cyber Security against Cyber Attacks. *Int. J. Tech, Vol: 10, Issue: 1*. Pp83-87. DOI: 10.5958/2231-3915.2020.00016.4.

Geer, David. (2006). Hackers Get to the Root of the Problem. *Computer*. IEEE Computer Society (USA). May. Vol. 39, No. 5, pages 17-19.

Gellman, D. (2011). *Computer Security.* 3rd edition. Wiley (USA).

George, A. and Sokratis, K. (2010). Disaster Recovery Plan Activities into the System Development Life Cycle. *Journal of Information System Security*. Washington DC, USA: Information Institute Publishing. Volume 6, Number 1, pages 20–35.

George, F. and Mike, B. (2010). Caveat venditor: *Information Security Technical Report* (UK). February. Volume 15, Issue 1, pages 28-32.

Georges, A. (2010). Review PCI DSS audit and compliance. *Information Security Technical Report* (UK). November. Volume 15, Issue 4, pages 138-144.

Gërvalla, M., Preniqi, N. and Kopacek, P. (2018). IT Infrastructure Library (ITIL) framework approach to IT Governance. *IFAC-PapersOnLine. Volume 51, Issue 30*. Elsevier. (USA)..Pp 181-185. https://doi.org/10.1016/j.ifacol.2018.11.283

Gibbert, M., Ruigrok, W., & Wicki, B. (2008). What passes as a rigorous case study? *Strategic Management Journal*, 29, 1465-1474.

Gibbs, J. P. (1975). *Crime, Punishment, and Deterrence*. New York: Elsevier Ltd.

Gibbs, J. P. (1986). Deterrence Theory and Research. In G.B. Melton (Ed.) *Nebraska Symposium on Motivation, 1985* (pp.87- 130). Lincoln: University of Nebraska Press.

Gilmore, G. D., and Campbell, M. D. (1996). *Needs Assessment Strategies for Health Education and Health Promotion* (3rd). Sudbury, MA Jones and Bartlett Publishers. pp. 65-72

Girish, M., Manjunath, K., Juslin, F. and Harshitha, N. (2018). Double Stegging Design To Hide Message In Video Using AES And DWT Methods. *2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. IEEE. USA.

Goebel, M., Dameff, C. and Tully, J. (2019). Hacking 9-1-1: Infrastructure Vulnerabilities and Attack Vectors. *Journal of Medical Internet Research, Vol 21, Issue 7*. doi: 10.2196/14383.

Goel, R., Kumar, A. and Haddow, J. (2020). *PRISM: A Strategic Decision Framework For Cybersecurity Risk Assessment*. Research Gate. (USA). Available at: https://www.researchgate.net/publication/342315184_PRISM_a_strategic_decision_framework_for_cybersecurity_risk_assessment. Visited on: 12th Nov 2021. DOI: 10.1108/ICS-11-2018-0131

Goodhue, D. L. and Straub, D. W. Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security Measures. *Information & Management* (USA). (20:1, January), 1991, pp.13-27.

Goodin, D. (2011). Anonymous hacks US gov contractor, airs dirty laundry. *The Register (UK)*. July 30th.

Gotha, A., Fredrikson, M., Livshits, B. and Swamy, N. (2011). Verified Security for Browser Extensions. *32nd IEEE Symposium on security and privacy (S&P 2011)*. IEEE computer society (USA). Pages 115-130.

Graham, B. (2013). *Innovation and Organisation: Towards an Art of Social System Design*. Monash University.

Green, P. J. (1982). *The Contents of a College-Level Outdour Leadership Course*. Paper Presented at the Conference of the North West District Association for the American. (USA)

Gregg, M. (2008). *Build Your Own Security Lab*. 1st edition. Wiley Publishing (USA).

Gregor, S. and Hevner, A. (2013) positioning and presenting design science research for maximum impact. *MIS Quarterly*, Vol. 37 No. 2, pp. 337-355.

Gregory, B. (2007). The Community Cyber Security Maturity Model. *40th Hawaii International Conference on System Sciences*. IEEE computer society (USA). Pages 1-8.

Gregory, C., Thomas, B. and John, N. (2011). Hacking Competitions and Their Untapped Potential for Security Education. *IEEE Security and Privacy*. IEEE Computer Society (USA). Vol. 9, no. 3, pages 56-59.

Grimes, R. A. (2017). *Hacking the Hacker: Learn From the Experts Who Take Down Hackers*. Wiley (USA). ISBN-13: 978-1119396215.

Guba, E. G., and Lincoln, Y. S. 2005. "Paradigmatic Controversies, Contradictions, and Emerging Confluences," *in The Sage Handbook of Qualitative Research (3rd ed.)*, N. K. Denzin and Y. S. Lincoln (eds.), Thousand Oaks, CA: Sage Publications, 2005, pp. 191-215.

Guido, S., Engin, K., Paolo, M., Stefano, Z., Clemens, K. and Christopher, K. (2010). Identifying Dormant Functionality in Malware Programs. *IEEE Symposium on Security and Privacy*. May. Pages 61-76.

Guido, Schryen (2007). *Anti – Spam Measures*. Springer (USA).

Guillaume, H., Valerie, V. T. T., Ludovic, M. and Benjamin, M. (2009). Policy-based intrusion detection in web applications by monitoring Java information flows. *International Journal of Information and Computer Security* (France). Vol. 3, No.3/4, pages 265–279.

Gullasch, D., Bangerter, E. and Krenn, S. (2011). Cache Games – Bringing Access-Based Cache Attacks on AES to Practice. *32nd IEEE Symposium on security and privacy (S&P 2011).* IEEE computer society (USA). Pages 490–505.

Guojun, W., Qin, L., Jie, W. and Minyi, G. (2011). Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers. *Computer security*. July. Volume 30, Issue 5, Pages 320-331.

Gustafson, D. H., Shukla, R. K., Delbecq, A., & Walster, G. W. (1973). A comparison study of differences in subjective likelihood estimates made by individuals, interacting groups, Delphi groups and nominal groups. Organizational Behavior and Human Performance, 9(2), 280 - 291.

Hadnagy, C., Kelly, F. and Ekman, P. (2014). *Unmasking the Social Engineer: The Human Element of Security*. Wiley (USA). ISBN-13: 978-1118608579.

Hadnagy, C. and Wilson, P. (2011). *Social Engineering: The Art of Human Hacking*. Wiley (USA). ISBN-13: 978-0470639535.

Haining, W., Danlu, Z. and Kang, G. S. (2004). Change-Point Monitoring for the Detection of DOS Attacks. *IEEE Transactions on Dependable and Secure Computing*. (USA). October-December. Vol. 1, no. 4, pages 193-208.

Hamadouche, S., Lanet, J. and Mezghiche, M. (2020). Hiding a fault enabled virus through code construction. *J Comput Virol Hack Tech* **16,** 103–124 https://doi.org/10.1007/s11416-019-00340-z

Handcock, M. S. and K. J. Gile (2011). Comment on the Concept of Snowball Sampling. *Sociological Methodology* (USA). 41(1): 367-371

Hannemyr, G. (1997). *Hacking considered constructive*. Paper presented at the Position paper for the 1997 Oksnoen Symposium on Pleasure and Technology (USA).

Hao Yang, Eric, O., Dan, M., Songwu, L. and Lixia, Z. (2011). Deploying Cryptography in Internet-Scale Systems: A Case Study on DNSSEC. *IEEE Transactions on Dependable and Secure Computing*. September/October. Vol. 8, no. 5, pages 656-669.

Haque M. S., and Chowdhury, M. U. (2018). A new cyber security framework towards secure data communication for unmanned aerial vehicle (UAV). *Security and*

Privacy in Communication Networks. Cham, Switzerland: Springer, pp. 113–122, doi: 10.1007/978-3-319-78816-6_9.

Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. and Williams, T. (2011). *Gray Hat Hacking*. 3rd edition. McGraw Hill (USA).

Harris, S. (2010-2016). *CISSP Practice Exams 7th Edithion*. McGraw-Hill (USA). ISBN-13: 978-0071849272.

Harrison, Keith and White, Gregory (2010). An Empirical Study on the Effectiveness of Common Security Measures. *43rd Hawaii International Conference on System Sciences (hicss)*. IEEE computer society (USA). Pages 1-7.

Hartmann, K. and Steup, C. (2020). Hacking the AI - the Next Generation of Hijacked Systems. *12th International Conference on Cyber Conflict (CyCon)*. IEEE. USA. Hacking-resistant IoT- Park, Yj. and Lee, Kh. (2018). Constructing a secure hacking-resistant IoT U-healthcare environment. *J Comput Virol Hack Tech* **14,** 99–106. https://doi.org/10.1007/s11416-017-0313-7

Harvey, B. (1985). *What is a Hacker?* Available from http://www.cs.berkeley.edu/~bh/hacker.html. Visited on: 07th October 2017

Harvey, S. and Evans D. (2016). Defending Against Cyber Espionage: The US Office of Personnel Management Hack as a Case Study in Information Assurance. *Intelligence and National Security*. Coastal Carolina University-April 7th, 2016. (USA) Available at: http://ncurproceedings.org/ojs/index.php/NCUR2016/article/viewFile/1764/982. Visited on: 12th Jun 2017.

Hasson F., Keeney S. and Mckenna H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing* 32(4), 1008-1015

Healy, J. (2017). Who's in Control: Balance in Cyber's Public-Private Sector Partnerships. *Georgetown Journal of International Affairs,* 18 (3), 120-130.

Hedieh, S. and Mansour, J. (2011). HYSA: Hybrid steganographic approach using multiple steganography methods. *Security and Communication Networks*. John Wiley & Son Ltd (USA). October. Volume 4. Issue 10, pages 1173–1184.

Henderson, Lance. (2017). *Tor and the Deep Web: Bitcoin, DarkNet & Cryptocurrency*. John Wiley (USA). ISBN: 9781-549727627.

Henry, R. and Goldberg, I. (2011). Formalizing Anonymous Blacklisting Systems. *32nd IEEE Symposium on security and privacy (S&P 2011).* IEEE computer society (USA). Pages 81-95.

Hesse-Biber, S. (2010). *Mixed Methods Research: Merging Theory With Practice*. The Guilford Press (USA). ISBN: 978-1-60623-505-8

Heubl, Ben. (2019). How to hack into the IOT: An E&T investigation carried out with leading cyber-threat experts reveals how simple it is to hack web-connected Internet of Things (IoT) devices and explores the implications for consumers and critical infrastructure in the UK. *Engineering & Technology*. Volume: 14, Issue: 7/8. IET (USA).

Hevner, A., March, S., Park, J. and Ram, S. (2004) Design Science in Information Systems Research. *MIS Quarterly*, Vol. 28, No. 1, pp. 75-105. Available at: http://www.jstor.org/stable/25148625 . Accessed on: 26th Jul 2017

Heyvaert, M., Maes, B., and Onghena, P. (2013). Mixed Methods Research Synthesis: Definition, Frameworks, and Potential. *Quality & Quantity*, 1-18.

Hicks, M., Finnicum, M., King, S., Martin, M. and Smith, J. (2010). Overcoming an untrusted computing base: Detecting and removing malicious hardware automatically. *IEEE Symposium on Security and Privacy.* IEEE computer society (USA). Pages 159–172.

Hill, Michael. and Swinhoe, Dan. (2021). The 15 biggest data breaches of the 21st century. IDG Communications. (USA). Available at: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html. Visited date: 29th September 2021.

Hinson, Gary (2011). Social Engineering Techniques, Risks, and Controls. *The EDP Audit, Control, and Security News Letter.* Taylor & Francis Group (UK). April-May. Volume. XXXVII, Iss. 4-5, pages 32-46.

Hoath, P. and Mulhall, T. (1998) Hacking: motivation and deterrence, part I. *Computer Fraud & Security*, 1998(4), 16-19.

Hoesung, K. and Seongjin, A. (2007). Study on developing a security violation response checklist for the improvement of internet security management systems. *International Conference on Multimedia and Ubiquitous Engineering (MUE'07)*. Pages 1199-1204

Holmes, W. (2017). *White Paper: VMware NSX Micro-segmentation*. VMware Press (USA). Available from: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-microsegmentation.pdf. Visited on: 20th October 2017.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y. and Ochoa, M. (2019). Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Comput. Surv. (USA). Vol* 52.

Hongxin, H, Gail-Joon, A. and Kulkarni, K. (2012). Detecting and Resolving Firewall Policy Anomalies. *IEEE Transactions on Dependable and Secure Computing*. IEEE (USA). May/June. Vol. 9, no. 3. Pages 318-331.

Hoon, W. L. and Kenneth, G. P. (2010). Identity-based cryptography for grid security. *International Journal of Information Security*. Volume 10, Number 1, pages 15-32.

Hossain, M., Inoue, H., Ochiai, H., Fall, D. and Kadobayashi, Y. (2020). LSTM-Based Intrusion Detection System for In-Vehicle Can Bus Communication. *IEEE Access, vol. 8*, pp. 185489-185502, doi: 10.1109/ACCESS.2020.3029307.

Howe, A., Ray, I., Roberts M., Urbanska, M. and Byrne, Z. (2012). The Psychology of Security for the Home Computer User. *33rd IEEE Symposium on security and privacy (S&P 2012)*. IEEE computer society (USA). Pages 209– 223

HP (2021). White Paper: *HP Printing Security Best Practices for HP FutureSmart Products*. Version 2.6. Hewlett-Packard Development Company (USA).

Hsiao, H., Kim, T., Perrig, A., Yamada, A., Nelson, S., Gruteser, M. and Meng, W. (2012). LAP. Lightweight Anonymity and Privacy. *33rd IEEE Symposium on security and privacy (S&P 2012)*. IEEE computer society (USA). Pages 506-522.

Hsu, C. C. & Sandford, B. A. (2007). Minimizing non-response in the Delphi process: How to respond to non-response. *Practical Assessment Research & Evaluation, 12(17)*

Hu, J., Hoang, X. D. and Khalil, I. (2011). An embedded DSP hardware encryption module for secure e-commerce transactions. *Security and Communication Networks*. John Wiley & Son Ltd (USA). August. Volume 4. Issue 8, pages 902–909.

Huajun, H., Junshan, T. and Lingxi, L. (2009). Countermeasure Techniques for Deceptive Phishing Attack. *International Conference on New Trends in Information and Service Science*. Pages 636-641.

Huajun, H., Shaohong, Z. and Junshan, T. (2009). Browser-Side Countermeasures for Deceptive Phishing Attack. *International Conference on Information Assurance and Security*. Vol. 1, pages 352-355

Huang L., and Zhu, Q. (2019). Dynamic Bayesian games for adversarial and defensive cyber deception. *Autonomous Cyber Deception*. Springer, pp. 75–97.

Huang, Y., Katz, J., and Evans, D. (2012). Quid-Pro-Quo-tocols: Strengthening Semi-honest Protocols with Dual Execution. *33rd IEEE Symposium on security and privacy (S&P 2012)*. IEEE computer society (USA). Pages 272–284.

Huaqiang, W., Alves-Foss, J., Terrence, S., Hugh, P., Zhang, D. and Deborah, F. (2008). A Layered Decision Model for cost-effective system security. *International Journal of Information and Computer Security* (USA). Vol. 2, No. 3, pages 297–324.

Huei-Ru, T., Rong-Hong, J. and Wuu, Y. (2011). A robust user authentication scheme with self-certificates for wireless sensor networks. *Security and Communication Networks*. John Wiley & Son Ltd (USA). August. Volume 4. Issue 8, pages 815–824.

Hwasu, S., Jong-sub, M. and Manhyun, C. (2011). A Distributed and Dynamic System for Detecting Malware. *IEEE International Conference on Advanced Information Networking and Applications Workshops (USA)*. Page 783-788

Hyun-Soo, C., Jea-Tek, R., Byeong-hee, R., Jeong-Wook, K. and Hyun-Cheol, J. (2008). Detection of SIP De-Registration and Call-Disruption Attacks Using a Retransmission Mechanism and a Countermeasure Scheme. *IEEE International Conference on Signal Image Technology and Internet Based Systems* (USA). Pages 650-656.

IBM (2021). White paper: *Cost of Data Breach Report 2021*. IBM Security (USA).. Available at: https://www.ibm.com/security/data-breach. Visited on: 12th Nov 2021.

IC3 (2021). White paper: *the Internet Crime Complaint Center's (IC3) 2020 report*. Internet Crime Complaint Centre (USA). Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf. Visited on: 24th Nov 2021.

Igbe, D. (2017). White Paper: *Defense in Breadth or Defense in Depth?*. Cloud Technology (USA). Available from https://www.cloudtechnologyexperts.com/Defense-in-Breadth-or-Defense-in-Depth/. Visited on: 25th June/2017

Igor, K. (2009). Framework for Integrated Proactive Network Worm Detection and Response. *Euromicro Conference on Parallel, Distributed and Network-based Processing*. Pages 379-386.

Igor, M., and Chris, B. (2009). Cloud security technologies**.** *Information Security Technical Report* (UK). February. Volume 14, Issue 1, Pages 1-6**.**

Ileana, B., Bas, B., Jeroen, D., Pieter, H. Hartel and Raymond, N.J. V. (2009). Secure pairing with biometrics. *International Journal of Security and Networks* (USA). Vol. 4, No.1/2, pages 27–42.

Imperva (2017a). White paper: *Cyberthreat Defense Report*. Imperva (USA). Available at: https://www.imperva.com/docs/gated/CyberEdge_2017_CDR_Report.pdf. Visited on 9th Jun 2017.

Imperva (2021a). White paper: *Cyberthreat Defense Report*. Imperva (USA). Available at: https://www.imperva.com/resources/resource-library/reports/2021-cyberthreat-defense-report/#:~:text=The%20Cyberthreat%20Defense%20Report%20provides,in%20your%20industry%20and%20region.. Visited on 29th Jun 2021.

Imperva (2021b). White paper: *Web Attack Survival Guide*. Imperva (USA). Available at: https://www.imperva.com/resources/resource-library/ebooks/web-attack-survival-guide-ebook-ty?lang=EN&asset_id=220. Visited on 12th Jun 2021.

Imperva (2021c). White paper: *2021 Global DDoS Threat Landscape Report hreat Landscape Report*. Imperva (USA). Available at: https://www.imperva.com/resources/resource-library/reports/ddos-threat-landscape-report-report-ty?lang=EN&asset_id=4828. Visited on 12th Nov 2021.

Imperva. (2021d). *Cyber Security Statistics & Trends*. Imperva. USA. Available at: https://www.imperva.com/cyber-threat-index. Visited date: 29th September 2021.

INNOVA (2012). *Infosec Management Framework*. INNOVA (USA). Available at: https://innova-sa.ed/security/information-security-information-management-ISMS.hlms. Visited on: 1st October/2017.

Insurance Information Institute. (2017). Facts and Statistics: Identity Theft and Cybercrime. *Insurance Information Institute* (USA). September 2017. Available at: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime. Visited on: 24 September 2017.

Invernizzi, L. and Comparetti, P. (2012). EvilSeed: A Guided Approach to Finding Malicious Web Pages. *33rd IEEE Symposium on security and privacy (S&P 2012).* IEEE computer society (USA). Pages 428-442.

Ioannis, M., Andreas, M., Ioannis, P., Isabella, K. and Christos, I. (2008). Supporting dynamic administration of RBAC in web-based collaborative applications during run-time. *International Journal of Information and Computer Security* (Greece) Vol. 2, No.4, pages 328-352.

IOT (2021). *Indiana Office of Technology - Information Security Framework*. State of Indiana (USA) Available at: https://www.in.gov/iot/policies-procedures-and-standards/. Visited on: 9th June 2021.

Irwin, L. (2021). *List of data breaches and cyber attacks in August 2021 – 61 million records breached. IT Governance*. (USA). Available at: https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-august-2021-61-million-records-breached. Visited date: 29th September 2021

Ismahani, I., Muhammad, N. M. and Sulaiman, M. N. (2010). Detecting Worms Using Data Mining Techniques. Learning in the Presence of Class Noise. *IEEE International Conference on Signal-Image Technology and Internet Based Systems*. pages 187-194.

ISO/IEC. (2021a). *SC27 STANDING DOCUMENT SD11: 2021 (2).* Geneva, Switzerland: ISO Organization. Available at: https://www.din.de/resource/blob/78920/053414214d97cf9b7a9276ff5c56a1e8/sc27-sd11-work-programme-data.pdf. Visited on 9th October 2021.

ISO/IEC. (2021b). *ISO/IEC 27002:2013 Information technology — Security techniques — Code of Practice for Information Security Controls (Second Edition).* Geneva, Switzerland: ISO Organization. Available at: https://www.iso27001security.com/html/27002.html. Visited on 19th October 2021.

ISO/IEC. (2021c). *ISO/IEC 27000 family - Information security management systems.* ISO/IEC (USA). Available at: https://www.iso27001security.com/html/27002.html. Visited on 22nd October 2021.

ISO/IEC. (2021d). *ISO 31000 - Risk management.* ISO/IEC (USA). Available at: https://www.iso.org/iso-31000-risk-management.html. Visited on 02nd October 2021.

IspartNersllc. (2021). *Updates from the PCI SSC* (USA). Available at: https://www.ispartnersllc.com/blog/pci-dss-version-4-0-launching-2020//. Visited on: 02/August/2021.

ITG (2021). *ISO 27000 Series of Standards.* IT Governance Corporation (UK). Available at: https://www.itgovernance.co.uk/iso27000-family. Visited on: 29th October 2021.

ITIL (2011). ITIL standard: ITiL. *ITIL* (USA). Available at: http://www.itil-officialsite.com/. Visited on: 26th May 2017.

Jacobs, David (2012). How to perform a network security audit for customers. TechTarget Inc (USA). Available at: http://searchsecuritychannel.techtarget.com/. Visited on: 27th April 2017.

Jahangir, H. S. and Hussein, T. M. (2011). A self-stabilized random access protocol against denial of service attack in wireless networks. *Security and Communication Networks*. John Wiley & Son Ltd (USA). September.Volume 4. Issue 9. Pages1075–1087.

Jahangiri, A. (2009). *Practical hacking and countermeasures*. Ali Jahangiri Org (USA).

Jakobsson, M. and Ramazan, Z. (2008). *Crimeware*. Symantec Press (USA).

Jana, S., Porter, D. and Shmatikov, V. (2011). TxBox: Building Secure, Efficient Sandboxes with System Transactions. *32nd IEEE Symposium on security and privacy (S&P 2011).* IEEE computer society (USA). Pages 329–344

Jang, J., Agrawal, A., and Brumley, D. (2012). ReDeBug: Finding Unpatched Code Clones in Entire OS Distributions. *33rd IEEE Symposium on security and privacy (S&P 2012).* IEEE computer society (USA). Pages 48–64

Jangbok, K., Kihyun, C. and Kyunghee, C. (2007). Spam Filtering With Dynamically Updated URL Statistics. *IEEE Security and Privacy*. July/August. Vol. 5, no. 4, pages 33-39.

Java, S., Basheer, F., Riaz, S., Kaur, M. and Mushtaq, A. (2019). Detection of Online Manipulation to Prevent Users Victimization. *Amity International Conference on Artificial Intelligence (AICAI)*. IEEE. USA.

Jeff, T. (2010). Matchmaking between PCI-DSS and Security. *Information Security Technical Report*. Elsevier Ltd. Volume 15, Issue 4, pages 137-166.

Jeffrey, A., Dan, S., Nancy, R. and Antonio, D. (2009). Threat Modeling the Enterprise. *Journal of Information System Security*. Washington DC, USA: Information Institute Publishing. Volume 5, pages 42–57.

Jeffrey, R. J. (2007). Estimating Software Vulnerabilities. *IEEE Security and Privacy*. July/August. Vol. 5, no. 4, pages 28-32.

Jenkins, C. C. (2009). A quality agricultural education program: A national Delphi study (unpublished doctoral dissertation). *University of Kentucky, Lexington KY*.

Jin, L., Takabi, H., and Joshi, J. (2011). Towards active detection of identity clone attacks on online social networks. *In Proceedings of the First ACM Conference on Data and Application Security and Privacy (CODASPY'11)*. February. San Antonio, TX, USA: IEEE. Pages 27–38.

Jinzhu, Kong. (2010). Protecting the Confidentiality of Virtual Machines Against Untrusted Host. *International Symposium on Intelligence Information Processing and Trusted Computing* (USA). Pages 364-368.

Jiutao, T. and Guoyuan, L. (2010). Research of Software Protection. *International Conf on Educational and network Technology (ICENT)*. Pages 410-413

Jo, B., and Mathias, K. (2009). Disclosure of personal information and online privacy. Control, choice and consequences. *Information Security Technical Report* (UK). August. Volume 14, Issue 3, pages 160-166.

John, C. G., Andrew, F. T. and James, M. (2011). Token-based graphical password authentication. *International Journal of Information Security* (USA). October.

Johnson, Jerry. (2008). Network Defense Requires Layers of Strategic Thinking. *Information Week* (USA). Feb 25. Iss. 1174, pp. 43 - 49.

Johnston, A.C. and Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly*, 34(3), 549-566.

Jonathan, V., Nathaniel B., and Salvatore, J. S. (2012). Lost in Translation: Improving Decoy Documents via Automated Translation. *IEEE CS on Security and Privacy Workshops*. IEEE computer society (USA). Pages 129-133.

Jones, Don (2009). White Paper: *Reaching the Tipping Point for Two-Factor Authentication*. Quest Software Inc (USA).

Joo, J. and Hovav, A. (2015). The influence of information security on the adoption of web-based integrated information systems: an e-government study in Peru, *Journal of Information Technology for Development*. Republic of Korea. Available at: http://dx.doi.org/10.1080/02681102.2014.979393. Visited on 28th March 2017.

Joon, S. P., Gaeil, A. and Ivy, Y. L. (2011). Active access control (AAC) with fine-granularity and scalability. *Security and Communication Networks*. John Wiley & Son Ltd (USA). October. Volume 4. Issue 10, pages 1114–1129.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *Sociological Review, 46*(4), 757– 780.

Joseph, L. H. (2011). *Email Attachments Best Practices*. University of California (USA). January.

Joshua, O. N. (2011). Understanding the decision rules for partitioning logs of intrusion detection systems (IDS).*International Journal of Internet Technology and Secured Transactions* (UK). Vol. 3, No.3, pages 293–309.

Judith, E., Scott, C. and Paul, S (2007). eTVRA, a Threat, Vulnerability and Risk Assessment Method and Tool for eEurope. *International Conference on Availability, Reliability and Security*. Pages 925-933

Julio, C. H., José, M. S., Arturo, R. and Benjamín, R. (2001). Search Engines as a Security Threat. *Computer* (USA). October. Vol. 34, no. 10, pages 25-30.

Jung-Shian, L., Che-Jen, H., Chih-Ying, C. and Naveen, C. (2011). Improved IPsec performance utilizing transport-layer-aware compression architecture. *Security and Communication Networks*. John Wiley & Son Ltd (USA). September. Volume 4. Issue 9, pages 1063–1074.

Kankanhalli, A., Teo, H., Tan, B., & Wei, K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23,* 139–154.

Kanneganti, R. and Chodavarapu, P. (2008). *SOA Security*. 1st edition. Manning Publications CO (USA).

Karen, L. Ö. (2010). The art of alchemy. *Information Security Technical Report* (UK). May. Volume 15, Issue 2, pages 47-50.

Keeney, S., Hasson, F., & McKenna, H. (2011a). The Delphi Technique. *The Delphi Technique in Nursing and Health Research,* 1-17. John Wiley & Sons.

Keeney, S., Hasson, F., & McKenna, H. (2011b). Conducting Research Using the Delphi Technique. *The Delphi Technique in Nursing and Health Research*, 69-83. John Wiley & Sons

Keeney, S., McKenna, H., & Hasson, F. (2010). *The Delphi technique in nursing and health research*. John Wiley & Sons.

Kefei, C., Meng, G., Ruijie, G. (2010). Analysis and Research on HTTPS Hijacking Attacks. *International Conference on Networks Security, Wireless Communications and Trusted Computing*. Vol. 2, pages 223-226.

Keil, M., Tiwana, A. & Bush, A. (2002). Reconciling user and project manager perceptions of IT project risk: A Delphi study. Information Systems Journal, 12(2), 103 - 119.

Kelemen, Z. D., Kusters, R., and Trienekens, J. (2012). Idetifying Criteria for Multimodel Software Process Improvement Solutions: Based on a Review of Current Problems and Investigations. *Journal of Software Maintanance and Evolution: Research and Practice*, 24(8), 895-909.

Kelley, P., Komanduri, S., Mazurek, M., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L. and Lopez, J. (2012). Guess Again (and Again and Again). Measuring Password Strength by Simulating Password-Cracking Algorithms. *33rd IEEE Symposium on security and privacy (S&P 2012).* IEEE computer society (USA). Pages 523-537.

Kewley, D. and Lowry, J. (2015) Observations on the effects of defense in depth on adversary behavior in cyber warfare. *Research Gate (USA)*. Available at: https://www.researchgate.net/publication/242601537_Observations_on_the_effects_of_defense_in_depth_on_adversary_behavior_in_cyber_warfare). Visited on: 10th September 2017.

Khodadadi, Touraj and A. K. M., Muzahidul Islam and Baharun, Sabariah and Komaki, Shozo (2016) Evaluation of recognition-based graphical password schemes in terms of usability and security attributes. *International Journal of Electrical and Computer Engineering (IJECE)*, 6 (6). (USA).

Kim, K. and Raymond, C. (2010). High tech criminal threats to the national information infrastructure. *Information Security Technical Report* (Australia). August. Volume 15, Issue 3, pages 104-111.

Kim, P. (2014). *The Hacker Playbook: Practical Guide To Penetration Testing*. CreateSpace Independent. (USA). ISBN-13: 978-1494932633.

Kimbell, L. (2011). Rethinking design thinking: Part I. *Design and Culture, 3*(3): 285-306.

Kindervag, John (2012). *Ease credit card risks: POS encryption and data tokenization for PCI.* TechTarget Inc (USA). Available at: http://searchsecurity. techtarget.com/. Visited on 28th March 2017.

King, C. M., Dalton, C. E. and Osmanoglu, T. E. (2001). *Security architecture.* ASA Press (USA).

Kjell, J. H., Erlend, D. and Thorsheim, Per. (2005). Securing Wi-Fi Networks. *Computer*. July. Vol. 38, no. 7, pages 28-34.

Klein, H. K., and Myers, M. D. (1999). “A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS Quarterly* (23:1), pp. 67-93.

Klein, H.K. & Myers, M.D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly, 23(1),* 67-88.

Kohno, T. and Broido, A. (2005). A Distributed Vulnerability Detection System for WLANs. *International Conference on Wireless Internet (WICON'05).* Los Alamitos, CA, USA: IEEE Computer Society. Pagses 86-93.

Kohno, T., Broido, A. and Claffy, K. (2005). Remote physical device fingerprinting. *IEEE Transactions on. Dependable Secure Computing* Vol. 2. (USA). April. Pages 93–108.

Kolbitsch, C., Livshits, B., Zorn, B. and Rozzle, C. (2012). De-cloaking Internet Malware. *33rd IEEE Symposium on security and privacy (S&P 2012).* IEEE computer society (USA). Pages 443-460.

Komanduri, S., Shay, R., Kelley, P., Mazurek, M., Bauer, L., Christin, N., Cranor, L., and Egelman, S. (2011). Of passwords and people. Measuring the effect of password-composition policies. In *Proceedings CHI (USA).*

Konstantinos, M., Keith, M., Damien, S. and Ioannis, G. A. (2008). Overview of Security Threats for Smart Cards in the Public Transport Industry. *IEEE International Conference on e-Business Engineering* (USA). Pages 506-513.

Konstantinos, M., Michael, T., Gerhard, H., Ioannis, A., and Keith, M. (2009). Attacking smart card systems: Theory and practice. *Information Security Technical Report*. May. Volume 14, Issue 2, pages 46-56.

Kontaxis, G., Polakis, I., Ioannidis, S. and Markatos, E. (2011). Detecting social network profile cloning. *In Proceedings of the 3rd IEEE International Workshop on Security and Social Networking (SESOC'11)*. March. Seattle, WA, USA: IEEE.

Kovah, X., Kallenberg, C., Weathers, C., Herzog, A., Albin, M. and Butterworth, J. (2012). New Results for Timing-Based Attestation. *33rd IEEE Symposium on security and privacy (S&P 2012).* IEEE computer society (USA). Pages 239-256.

Kozachok, A.V., Kopylov, S.A. and Shelupanov, A.A. (2019). Text marking approach for data leakage prevention. *J Comput Virol Hack Tech 15, 219–232*. https://doi.org/10.1007/s11416-019-00336-9.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers and Security, 27*, 224–231.

Kuheli, R. S (2010). Assessing insider threats to information security using technical, behavioral and organizational measures. *Information Security Technical Report* (UK) August. Volume 15, Issue 3, pages 112-133.

Kulkarni, A. N., Luo, H., Leslie, N. O., Kamhoua, C. A., and Fu, J. (2021). Deceptive labeling: Hypergames on graphs for stealthy deception. *IEEE Control Systems Letters*, 28 July, 2021.

Kvale, S. (1996). Interviews: An introduction to qualitative research interviewing. Thousand Oaks, CA: Sage

Kyungroul, L. and Kangbin, Y. (2011). Keyboard Security: A Technological Review. *International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*. Pages 9-15.

Kyungroul, L., Wansoo, K., Kwangjin, B. and Kangbin, Y. (2010). A Solution to Protecting USB Keyboard Data. *International Conference on Broadband, Wireless Computing, Communication and Applications*. Pages 108-111.

Lachapelle, E., Bislimi, M. (2016). White Paper: *ISO/IEC 27002:2013: Information Technology – Security Techniques Code of Practice for Information Security Controls*. Professional Evaluation and Certification Board (PECB) . Available at: www.pecb.com. Visited on 19th October 2017.

Lam, S. S. Y., Petri, K. L., & Smith, A. E. (2000). Prediction and optimization of a ceramic casting process using a hierarchical hybrid system of neural networks and fuzzy logic. IIE Transactions, 32(1), 83 - 92.

Lamar University (2021). *Privacy & Security*. Lamar University (USA). Available on: https://lamar.bncollege.com/shop/lamar/page/privacy-security. Visited on: 12 September 2021.

Lance, Adrian. (2010). Database Auditing Tools. *Information Security Magazine* (USA). October. Vol. 12. Number 8, pages 40-45.

Lanier, W., Raheem, B. and Cherita, C. (2009). Using link RTT to passively detect unapproved wireless nodes. *International Journal of Security and Networks* (USA). Vol. 4, No.3, pages 153-163.

Lanzi, A., Sharif, M. I., and Lee, W. (2009). K-tracer. A system for extracting kernel malware behavior. *Network and Distributed Systems Security Symposium (NDSS)*. San Diego, CA,USA: NDSS.

Lark, J. (2015). *ISO 31000 - Risk Management - A practical guide for SMEs.* ISO/IEC (Switzerland). ISBN 978-92-67-10645-8.

Laura, Didio. (2009). *White-Paper: Security Considerations for a Windows Server Integration.* Information Technology Intelligence Corporation (USA).

Lazarte, M. (2016). *Are we safe in the Internet of Things?*. ISO/IEC (USA). Available at: https://www.iso.org/news/2016/09/Ref2113.html. Visited on 22nd October 2017.

Lee, A. S., and Hubona, G. S. (2009). A Scientific Basis for Rigor in Information Systems Research. *MIS Quarterly* (33:2), pp. 237-262

Lee, A.S. (1989). A scientific methodology for MIS case studies. *MIS Quarterly*, 13(1), 33-50.

Lee, D., Park, W. and Kim, K. (2011). A Study on Analysis of Malicious Codes Similarity Using N-Gram and Vector Space Model. *International Conference on Information Science and Applications*. Pages 1-4.

Lee, J. & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management and Computer Security*, 10(2), 57-63.

Lee, Y., Woo, S., Song, Y., Lee, J., and Hoon Lee, D. (2020). Practical Vulnerability-Information-Sharing Architecture for Automotive Security-Risk Analysis. *IEEE Access, Volume 8, 2020.* (USA).

Lee, Y., Woo, S., Song, Y., Lee, J., and Hoon Lee, D. (2020). Practical Vulnerability-Information-Sharing Architecture for Automotive Security-Risk Analysis. IEEE Access, Volume 8, 2020. (USA).

Leedy, P. D. and Ormrod, J. E. (2019). *Practical Research Planning and Design*. 12th edition. Pearson (USA).

Lehman, D. W. & Ramanujam, R. (2009). Selectivity in organizational rule violations. *Academy of Management Review, 34*(4), 643-657.

Lennon, M. (2011). Anonymous hacks mantech, FBI cyber security contractor. *Security Week (USA)*. July 29th.

Leon, A. T. D., and Huertas, J. M. (2012). The Balance Score Card for the Design and Validation Instruments to Measure the Academic Teachers. *Achievement and Performance. Education*. Scientific & Academic Publishing. 2(7), 220-226

Levchenko, K., Pitsillidis, A., Chachra, N., Enright, B., F´elegyh´azi, M., Grier, C., Halvorson, T., Kanich, C., Kreibich, C., Liu, H., McCoy, D., Weaver, N., Paxson, V., Voelker, G. and Savage, S. (2011). Click Trajectories: End-to-End Analysis of the Spam Value Chain. *32nd IEEE Symposium on security and privacy (S&P 2011).* IEEE computer society (USA). Pages 431–446.

Levy, I., (2018). Active Cyber Defense – One Year On. https://www.ncsc.gov.uk/information/active-cyberdefense-one-year. Visited Date: 02 January 2021

Levy, I., (2019). Active Cyber Defense – The Second Year. https://www.ncsc.gov.uk/blog-post/active-cyber-defense-acd-the-secon-year. Visited Date: 02 January 2021

Levy, S. (2010). Hackers: Heroes of the Computer Revolution - 25th Anniversary Edition. O'Reilly (USA). ISBN: 1449388396.

Lewis, Nick (2012a). *Email, website and IP spoofing: How to prevent a spoofing attack*. TechTarget Inc (USA). Available at: http://searchsecurity.techtarget.com/. Visited on: 27th April 2017.

Lewis, Nick (2012b). *Why attackers exploit multiple zero-day attacks and how to respond*. TechTarget Inc (USA). Available at: http://searchsecurity.com/. Visited on: 27th April 2017.

Lewis, Nick. (2011). *Secure tokens: Preventing two-factor token authentication exploits*. TechTarget Inc (USA). Available at: http://searchsecurity.techtarget.com/. Visited on: 15th August 2017.

Li, N. and Tripunitara, M. V. (2005). On safety in discretionary access control. *In Proceedings of the 2005 IEEE Symposium on Security and Privacy (S&P '05)*. May. Oakland, California, USA: IEEE. Pages 96–109.

Lieven, D., Pierre, V., Wouter, J. and Frank, P. (2008). Provable Protection against Web Application Vulnerabilities Related to Session Data Dependencies. *IEEE Transactions on Software Engineering (USA)*. January. Vol. 34, no. 1, pages 50-64.

Lili, Y. and S.H. Y. (2007). framework of security and safety checking for internet-based control systems. *International Journal of Information and Computer Security* (UK). Vol. 1, No.1/2, pages 185-200.

Lilja Josefine L., Annika Frodi-Lundgren, Jan Johansson Hanse, Torbjörn Josefsson, Lars-Gunnar Lundh, Camilla Sköld, Erling Hansen & Anders G. Broberg (2011). Five Facets Mindfulness Questionnaire—Reliability and Factor Structure: A Swedish Version. *Journal of Cognitive Behaviour Therapy.*

Volume 40/ 2011. Issue 4. Pages: 291-303. (Sweden). DOI:10.1080/16506073.2011.580367.

Lincoln, D. S. and Stewart, J. N. (2017a). General Questions. *W3C-The World Wide Web Security FAQ*. W3C Organization (USA). Available at: https://www.w3.org/Security/faq/wwwsf1.html. Visited on: 7th April, 2017.

Lincoln, D. S. and Stewart, J. N. (2017b). *Protecting Confidential Documents at Your Site*. W3C Organization (USA). Available at: https://www.w3.org/ Security/faq/wwwsf5.html. Visited on: 7th April, 2017.

Lincoln, D. S. and Stewart, J. N. (2017c). *Securing against Denial of Service attacks*. W3C Organization (USA). Available at: https://www.w3.org /Security/faq/wwwsf6.html. Visited on: 7th April, 2017.

Lincoln, D. S. and Stewart, J. N. (2017d). *Server Side Security*. W3C Organization (USA). Available at: https://www.w3.org/Security/faq/wwwsf3.html. Visited on: 7th April, 2017.

Lincoln, Y. S., and Guba, E. G. 2000. "Paradigmatic Controversies, Contradictions, and Emerging Confluences," *in Handbook of Qualitative Research*, N. K. Denzin and Y. S. Lincoln (eds.), Thousand Oaks, CA: Sage Publications, pp. 163-188.

Lingfeng, Yu (2004). *Multidimensional data encryption with virtual optics*. University of Science and Technology (Hong Kong).

LingYun, Z. (2009). VMM-Based Framework for P2P Botnets Tracking and Detection. *International Conference on Information Technology and Computer Science*. July. Pages 172-175.

Liu, Alexander Y. and Lam, Dung N. (2012). Using Consensus Clustering for Multi-view Anomaly Detection. *IEEE CS on Security and Privacy Workshops*. IEEE computer society (USA). Pages 117–124.

Liu, L., de Vel, O., Han, Q., Zhang, J. and Xiang, Y. (2018). Detecting and preventing cyber insider threats: A survey. *IEEE Commun. Surv. Tutor*. Vol, 20, Pp1397–1417.

Liu, V., Han, S., Krishnamurthy, A., and Anderson, T. (2011). Tor instead of IP. In *Proceedings of ACM Hotnets (USA).*

Loch, K., Carr, H.., & Warkentin, M. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly, 16*(2), 173–186.

Lockhart, A. (2006). *Network Security Hacks*. 2nd edition. O'REILLY (USA).

Lohrmann, Dan. (2021). Research: Data breach numbers, costs and impacts all rise in 2021. Government Technology. USA. Available at https://www.securityinfowatch.com/cybersecurity/news/21241763/research-data-breach-numbers-costs-and-impacts-all-rise-in-2021. Visited date: 29th September 2021.

Long, David. T. (2020). Wargaming and the Education Gap: Why CyberWar: 2025 Was Created. *The Cyber Defense Review, Vol 5 No 1.* (USA). 185-198.

Ludwig, B. G. (1994). Internationalizing Extension: An Exploration of the characteristics Evident In *A State University Extention System That Achieves Internationalzation*. Ohio State University. (USA).

Ludwig, B. G. (1997). Predicting the Future: Have you Considered Using the Delphi Methodology?. *Journal of Extension*. (USA). 35(5) pp1-4

Lumension (2011). White Paper: *Minimizing your insider risk by controlling USB devices and encrypting data*. July. Lumension Endpoint Security (USA).

Luttgens, T., Pepe, M., Mandia, K.(2014). *Incident Response & Computer Forensics (3rd Edition).* McGraw-Hill. ISBN-13: 978-0071798686.

Madden, J. (2015). Leveraging Design: How the Design Process and a Design Framework Strengthen Nonprofit Management Pedagogy. Journal of Nonprofit Education and Leadership, 5(1): 6-11.

Madden, T. j., Ellen, P. S., & Ajzen, I. (1992). A Comparison of the Theory of Planned Behavior and the Theory of Reasoned Action. *PSBP1, 18*(1), 3 – 9.

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., and Raghu, T. S. (2010). Moving toward black hat research in information systems security : An editorial introduction to the special issue. *MIS Quarterly, 34*(3), 431–433

Malkin, G., and Parker, T. L. (1993). *RFC 1392 - Internet Users Glossary*. Available from http://tools.ietf.org/html/rfc1392. Visited on: 07th October 2017

Malliga, S. and Tamilarasi, A. (2010). A backpressure technique for filtering spoofedtraffic at upstream routers. *International Journal of Security and Networks*. Vol. 5, No. 1, pages 3–14.

Malwarebytes. (2021). *Hacking definition: What is hacking?*. Malwarebytes. (USA). Available at: https://www.malwarebytes.com/hacker. Visited Date: 02 January 2021.

Marin, Ericsson., Almukaynizi, Mohammed., Nunes, Eric., Shakarian, Jana. and Shakarian, Paulo. (2018). Predicting Hacker Adoption on Darkweb Forums Using Sequential Rule Mining. IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications. IEEE. (USA).

Marin, Ericsson., Almukaynizi, Mohammed. and Shakarian, Paulo. (2020). Inductive and Deductive Reasoning to Assist in Cyber-Attack Prediction. *10th Annual Computing and Communication Workshop and Conference (CCWC). IEEE. USA*. Pp. 0262-0268, doi: 10.1109/CCWC47524.2020.9031154.

Mario K., Marin G. and Stjepan G. (2009). A method for identifying Web applications. *International Journal of Information Security*. Volume 8, Number 6, pages 455-467.

Masters, G. (2015) Shifu trojan now targeting U.K. banks. *IBM SCmagazine (USA). Issue: 30th Sep 2015*. Available at: https://www.scmagazine.com/shifu-trojan-now-targeting-uk-banks/article/533692/. Visited on: 2nd April 2017

Masters, G. (2017). Shifu banking trojan evolves and expands. *IBM SCmagazine (USA). Issue: 9th Jan 2017*. Available at: https://www.scmagazine.com/shifu-banking-trojan-evolves-and-expands/article/630349/. Visited on: 2th April 2017

Mathew, N., Hussein, F. and Charles, H. (2011) An Integrated Security Governance Framework for Effective PCI DSS Implementation. *International Journal of Information Security and Privacy (IJISP)*. Volume 5, Issue 3.

Martinelli, F., Mercaldo, F., Nardone, V., Santone, A., Sangaiah, A.K., Cimitile, A. (2018). Evaluating model checking for cyber threats code obfuscation identification. *J. Parallel Distrib. Comput. 119, 203–218.* (USA)

Mauro, C., Roberto, Di P., Luigi, V. M. and Alessandro, M. (2011). Distributed Detection of Clone Attacks in Wireless Sensor Networks. *IEEE Transactions on Dependable and Secure Computing* (USA). September/October. Vol. 8, no. 5, pages 685-698.

Maxwell, J. A. (1992). Understanding and validity in qualitative research. *Harvard Eduational Review*, 62(3), 279–300.

May, C., Hammerstein, J., Mattson, J. and Rush, K. (2012). White Paper: *Defense-in-Depth. Foundations for Secure and Resilient IT Enterprises (*CMU/SEI-2006-HB-003*).* Carnegie Mellon University (USA). September. Available at: http://www.sei.cmu.edu/publications/pubweb.html. Visited on: 28th March 2017.

Mayer, J. (2011a). *Tracking the trackers: Selfhelp tools*. Stanford University (USA). September.

Mayer, J. (2011b). *Tracking the trackers: Early results*. Stanford University (USA). July.

Mayer, J. and Mitchell, J. (2012). Third-Party Web Tracking. Policy and Technology. *33rd IEEE Symposium on security and privacy (S&P 2012).* IEEE computer society (USA). Pages 413-427.

McClure, S., Scambray, J. and Kurtz, G. (2012). *Hacking Exposed Network Security Secrets and Solutions*. 7th edition. McGraw-Hill/ Osborne (USA).

McGraw, G., Migues, S. and West, J. (2017). *Building Security In Maturity Model BSIMM8.* BSIMM (USA). Available at: https://www.bsimm.com/content/dam/bsimm/reports/bsimm8.pdf. Visited on: 10th April/2017.

McLoughlin, Ian (2008). Secure Embedded Systems: The Threat of Reverse Engineering. *IEEE International Conference on Parallel and Distributed Systems*. Pages 729-736.

McNab, C. (2017). *Network Security Assessment.* 2nd edition. O'REILLY (USA). ISBN-13: 978-1491910955.

Melone, M. (2017). *Think Like a Hacker: A Sysadmin's Guide to Cybersecurity.* Bitlatch Books (USA).

Menn, J. (2010). *Fatal System Error: The Hunt for the crime Lords who are bringing down the internet.* Public Affairs (USA).

Mercaldo, F. and Santone, A. (2020). Deep learning for image-based mobile malware detection. *J Comput Virol Hack Tech* **16,** 157–171. Doi.org/10.1007/s11416-019-00346-7.

Mete, E., Erdem, U. and Saban, E (2009). The positive outcomes of information security awareness training in companies – A case study. November. *Human Factors in Information Security.* Vol. 14, issue 4, pages 175-230

Meyers, M. and Harris, S. (2009). *Certified Information Systems Security Professional.* Mitp-Verlag (USA).

Michael, G. (2015). *The Network Security Test Lab: A Step-by-Step Guide.* Wiley (USA) ISBN-13: 978-1118987056

Michael, S. (2012). *Hacking back puts security on the offensive.* TechTarget Inc (USA). Available at: http://searchsecurity.techtarget.com/. Visited on: 27th March 2017.

Michael, S. M. (2010). Do You Have a Disaster Recovery Plan?.*Information Security Journal. A Global Perspective.* Taylor & Francis (UK). Mar. Vol. 19, Iss.1, pages 1-3.

Michel, C. (2011). The client side – Patch Management. *Information Security* (USA). March. Pages 37- 42.

Michelle, Kincaid. (2010). Cyber Attacks Can Be Prevented. *Business Wire (USA).* July. Pages: 202–207.

Microsoft. (2020). *Threat Modeling Tool update release 7.3.00714.2 - 07/14/2020.* Available from https://docs.microsoft.com/bs-latn-ba/azure/security/develop/threat-modeling-tool-releases-73007142. Visited on: 20th September/2021.

MicrosoftCo. (2009). *Getting Started with MOF 4.0*. Microsoft Corporation

Miles, M. B., and Huberman, A. M. (1994). *Qualitative Data Analysis: An Expanded Sourcebook*. Beverly Hills: SAGE Publications. 2(1)

Miller, L. E. (2006). Determining what could/should be: The Delphi technique and its application. *Paper presented at the 2006 annual meeting of the Mid-Western Educational Research Association*, Columbus, OH.

Ming, Yu. (2009). A Probabilistic Drop Scheme for Mitigating SYN Flooding Attacks. *International Conference on Networks Security, Wireless Communications and Trusted Computing*. Vol. 1, pages 732-734.

Ming-Yang S. and Sheng-Cheng Y. (2011). A study on the prevention of sniffing nodes in mobile ad hoc networks. *Security and Communication Networks*. August. Volume 4. Issue 8. John Wiley & Son Ltd (USA). Pages 910–918.

Mirtsch, M., Kinne, J. and Blind, K. (2020). Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis. *IEEE Transactions on Engineering Management* Pp(99):1-14 (USA). DOI: 10.1109/TEM.2020.2977815

MITRE Corporation. (2021). CVE reference map for source ISS. U.S. Department of Commerce. Available at: https://cve.mitre.org/data/refs/refmap/source-ISS.html. Accessed September 12, 2021

Mo, L., Xiaoye, J., and Leonidas, G. (2011). Fingerprinting Mobile User Positions in Sensor Networks: Attacks and Countermeasures. *IEEE Transactions on Parallel and Distributed Systems*. IEEE Computer Society (USA). Vol. 99, no. 1.

Mohassel, P. and Franklin, M. (2006). Efficiency tradeoffs for malicious two-party computation. *International Conference on Theory and Practice of Public Key Cryptography (PKC 2006)*. Volume 3958 of LNCS. Springer (USA). Pages 458–473.

Monarchi, D. and Puhr, G. (1992). A Research Topology for Object Oriented Analysis and Design. *Communications of the ACM*. Vol. 33, No, 9, Pages 35-47

Monecke, A., & Leisch, F. (2012). semPLS : Structural Equation Modeling Using Partial Least Squares. *Journal of Statistical Software*, 48(3), 1–32.

Monia, L., Mohamed, J. and Mohamed, M. (2009). Dynamic security framework for mobile agent systems. specification, verification and enforcement. *International Journal of Information and Computer Security* (France). Vol. 3, No.3/4, pages 321-336.

More, S., Matthews, M., Joshi, A., and Finin, T. (2012). A Knowledge-Based Approach to Intrusion Detection Modeling. *IEEE CS on Security and Privacy Workshops*. IEEE computer society (USA). Pages 76-81.

Morgan, S. (2016). Cyber Crime Costs Projected To Reach $2 Trillion by 2019. *Forbes* (USA). Jan 2016. Available at: https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#39361f743a91. Visited on: 24 September 2017.

Moskowitz, J. (2008). *Group Policy Fundamentals, Security, and Troubleshooting*. 1st edition. Wiley Publishing (Canada).

Mouza Ahmad, B. S., Chan Yeob, Y. and Mohamed, Jamal Z. (2010). Lightweight mutual authentication protocol for securing RFID applications. *International Journal of Internet Technology and Secured Transactions*. Vol. 2, No.3/4, pages 205–221.

Muir, J. and Oorschot, P. (2009). Internet geolocation: Evasion and counterevasion. *ACM Comput. Surv*. Vol. 42. (USA). December. Pages 4.1–4.23

Murat, K. and Onur, K. (2008). Privacy-preserving data mining in the malicious model. *International Journal of Information and Computer Security* (USA). Vol. 2, No.4, pages 353 – 375.

Murphy, J., Berk, V., and Gregorio-de Souza, I. (2012). Decision Support Procedure in the Insider Threat Domain. *IEEE CS on Security and Privacy Workshops*. IEEE computer society (USA). Pages 159-163.

Murray, J. (2014). The logic of consensus on the foundations of science education in Canada – A Delphi study. (PhD Dissertation), University of Manitoba Winnipeg. Canada.

Mustonen-Ollila, E., & Lyytinen, K. (2003). Why organizations adopt information system process innovations: a longitudinal study using Diffusion of Innovation theory. *Information Systems Journal*, 13(3), 275-297.

Naik, N., Shang, C., Jenkins, P., and Shen, Q. (2020). D-FRI-Honeypot: A Secure Sting Operation for Hacking the Hackers Using Dynamic Fuzzy Rule Interpolation. *IEEE Transactions on Emerging Topics in Computational Intelligence*. IEEE. USA

Nakasone, P. (2019). A Cyber Force for Persistent Operations. *Joint Force Quarterly, Vol 92, 1st Quarter 2019*. National Defense University Press. (USA). Pp10-14. Available at: Library: www.dtic.mil/doctrine/jfq/jfq.htm. Visited Date: 02 January 2021.

Nambisan, S., Agarwal, R., & Tanniru, M. (1999). Organisational mechanisms for enhancing user innovation in information technology. MIS Quarterly, 23(8), 365 - 395.

Nambisan, S., Agarwal, R., & Tanniru, M. (1999). Organisational mechanisms for enhancing user innovation in information technology. MIS Quarterly, 23(8), 365 - 395.

Nance, W. D. and Straub, D.W. (1988). An Investigation into the Use and Usefulness of Security Software in Detecting Computer Abuse. *Proceedings of the 9th International Conference on Information Systems (ICIS)*, Minneapolis, MN, (USA). pp. 283-294.

Nanevski, A., Banerjee, A. and Garg, D. (2011). Verification of Information Flow and Access Control Policies with Dependent Types. *32nd IEEE Symposium on security and privacy (S&P 2011).* IEEE computer society (USA). Pages 165–179.

Natan, R. B. (2011). *Implementing Database Security and Auditing*. Elsevier digital press (USA). Available at: www.guardium.com. Visited on: 12th August 2017.

National Intelligence (2019). *Improving Cybersecurity for the Intelligence Community Information Environment Implementation Plan.* National Intelligence (USA). Available at: https://www.dni.gov/files/documents/CIO/Improving_Cybersecurity-IC_IE_ImpPlan-August_2019_reduced_web.pdf. Visited on: 1st October/2020.

Nayot, P., Rinku, D. and Indrajit, R. (2011). Dynamic Security Risk Management Using Bayesian Attack Graphs. *IEEE Transactions on Dependable and Secure Computing*. Vol. 99, no. 1.

Nelson, P., Philips, A. and Stuart, C. (2010). *Guide to computer forensics and investigations*. Course technology (USA).

Neville, H. (2005). In Defense of Spam. *Computer* (USA). April. Vol. 38, no. 4, pages 86-87.

Nichols, R., Ryan, D., and Ryan, J. (2000). *Defending Your Digital Assets*. (USA).

Nikitina, S. (2012). Hackers as Tricksters of the Digital Age: Creativity in Hacker Culture. *The Journal of Popular Culture, 45*(1): 133-152

NIST (2021). Al Risk Management Framework FAQs. National Institute of Standards and Technology (USA). Available at: https://www.nist.gov/itl/ai-risk-management-framework/ai-risk-management-framework-workshops-events. Visited on: 31st July 2021.

Nitesh, S. and Jonathan, V. (2011). Data remanence effects on memory-based entropy collection for RFID systems. *International Journal of Information Security*. Volume 10, Number 4, pages 213-222.

Nolan, L. N. (1994). Forward to the future: A Delphi study of the future of education. Digital Abstracts International, 55 (07), 1747. (UMI No. 9430911).

Nora, C., Frederic, C., Fabien, A. and Herve, D. (2009). An ontology-based approach to react to network attacks. *International Journal of Information and Computer Security* (France). Vol. 3, No.3/4, pages 280-305.

Norman, P. and Mark, R. (2009). A Simulation of Various Variable Hacker Populations. *International Conference on Computational Science and Engineering.* Vol. 3, pages 504-510.

Norman, S. (2010). Metrics for Mitigating Cyber security Threats to Networks. *IEEE Internet Computing.* IEEE (USA). January/February. Vol. 14, Iss. no. 1, pages. 64-71.

Nunamaker, J., Chen, J. and Purdin, T. (1991). Systems Development in Information Systems Research. *Journal of Management Information Systems*, Winter 1990-91, Vol. 7, No. 3, pp. 89-106

Nunna, K. C. and Marapareddy, R. (2020). Secure Data Transfer Through Internet Using Cryptography and Image Steganography. *SoutheastCon. IEEE. USA*. Pp. 1-5, doi: 10.1109/SoutheastCon44009.2020.9368301.

Nunna, K. C. and Marapareddy, R. (2020). Secure Data Transfer Through Internet Using Cryptography and Image Steganography. *SoutheastCon. IEEE. USA*. Pp. 1-5, doi: 10.1109/SoutheastCon44009.2020.9368301.

Nunna, K. C. and Marapareddy, R. (2020). Secure Data Transfer Through Internet Using Cryptography and Image Steganography. SoutheastCon 2020, pp. 1-5, doi: 10.1109/SoutheastCon44009.2020.9368301.

OCERT. (2021). Oman National CERT. OCERT (Oman). Available at: https://www.ita.gov.om/ITAPortal/Pages/Page.aspx?NID=2038&PID=200075. Visited on: 06th August 2021.

OIT-VA (2019). Cisco Security Agent VA Technical Reference Model v 21.11. US Department of Veterans Affairs. (USA). Available from https://www.oit.va.gov/Services/TRM/ToolPage.aspx?tid=13529. Visited on: 25th January/2021.

Okoli, C. and Powlowski, S. D. (2004). The Delphi Method as a Research Tool: An Example, Design Considerations and Applications. *Information & Management.* 42(1). pp15-29.

Olakanmi, O. Oladayo. (2011). RC42's innovative way for data security in wireless data communication. *International Journal of Information and Computer Security*. Vol. 4, No.3, pages 264–275.

Olenick, D. (2015) Shifu Trojan now striking 14 Japanese banks: IBM. *IBM SCmagazine (USA). Issue: 30th Sep 2015*. Available at: https://www.scmagazine.com/shifu-trojan-now-striking-14-japanese-banks-ibm/article/532465/. Visited on: 2th April 2017

Ollam, Deviant (2010). *Practical Lock Picking: A Physical Penetration Tester's Training Guide*. Syngress (USA).

Oltsik, J. (2010). White Paper: *Information Security Virtualization and the Journey to the Cloud*. Enterprise Strategy Group Inc (USA).

Olzak, T. (2017). *Incident Management and Response Guide: Tools, Techniques, Planning, and Templates*. Erudio Security, LLC (USA).

Oman Royal Palace (2010). *Program in Information Security*. Oman Royal Pabace. Muscat. Oman.

Oracle (2020). Oracle and KPMG cloud Threat Report 2020. https://www.oracle.com/ie/cloud-threat-report/. Visited: 03 January 2021

Oreku G., Jianzhong, L. and Fredrick, J. (2009). A framework towards enhancing trust and authorisation for e-commerce service. *International Journal of Internet Technology and Secured Transactions* (Ireland). Vol. 1, No.3/4, pages 173–202.

Osborne, J., Collins, S., Ratcliffe, M., Millar, R., & Duschl, R. (2003). What "ideasabout-science" should be taught in school science? A Delphi study of the expert community. *Journal of Research in Science Teaching*, 40(7), 692-720.

OSU (2016). *Ohio Supercomputer Center - Information Security Framework*. Ohio State University (USA). Available at: http://cybersecurity.osu.edu/sites/default/files/itsecurity.pdf.Visited on: 12th August 2017..

OSU (2021). *Ohio Supercomputer Center - Information Security Framework*. Ohio State University (USA). Available at: https://cybersecurity.osu.edu/cybersecurity-ohio-state/internal-policies-compliance/security-framework.Visited on: 10th August 2021.

OWASP (2017). White paper: *OWASP Top 10 2017*. OWASP (USA). Available at: https://www.owasp.org/images/b/b0/OWASP_Top_10_2017_RC2_Final.pdf.

Visited on 22nd October 2017.

OWASP (2020). White paper: *OWASP Top 10: Vulnerabilities 2020*. OWASP (USA). Available at: https://owasp.org/www-project-top-ten/. Visited on 2nd September 2020.

OWASP (2021a). *Session Management Cheat Sheet*. OWASP Organization (USA). Available at: https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html. Visited on: 22nd August 2021.

OWASP (2021b). White paper: *OWASP Web Applications Security Project*. OWASP (USA). Available at: https://www.castsoftware.com/glossary/owasp. Visited on 22nd October 2021.

OWASP (2021c). TLS Cipher String Cheat Sheet Organization (USA). Available at: https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html. Visited on: 22nd August 2021 .

OWASP (2021d). SSL Config Generator (USA). Available at: https://ssl-config.mozilla.org/#server=apache&version=2.4.41&config=intermediate&openssl=1.1.1k&guideline=5.6. Visited on: 22nd August 2021.

Owen, C., Grove, D., Newby, T., Murray, A., North, C. and Pope, M. (2011). PRISM: Program Replication and Integration for Seamless MILS. *32nd IEEE Symposium on security and privacy (S&P 2011)*. IEEE computer society (USA). Pages 281–296

Owen, K. (2016). *Motivation And Demotivation Of Hackers In The Selection Of A hacking Task – A Contextual Approach*. PhD (Information Systems), McMaster University. USA.

Owen, K. (2016). *Motivation And Demotivation Of Hackers In The Selection Of A hacking Task – A Contextual Approach*. PhD (Information Systems), McMaster University. USA.

Padmashri. R, Senduru, S., Jeberson. R., Jabez, j. and Gowri, S. (2021). Perceptual Image Hashing Using Surffor Feature Extraction and Ensemble Classifier. *3rd International Conference on Signal Processing and Communication (ICPSC)*. IEEE.USA

Padmashri. R, Senduru, S., Jeberson. R., Jabez, j. and Gowri, S. (2021). Perceptual Image Hashing Using Surffor Feature Extraction and Ensemble Classifier. *3rd International Conference on Signal Processing and Communication (ICPSC)*. IEEE.USA

Panko, R. J. (2011). *Corporate Computer and Network Security*. 2ndedition. PEARSON (USA).

Paolo, F., Riccardo, S. and Mario, B. (2006). Remote Trust with Aspect-Oriented Programming. *International Conference on Advanced Information Networking and Applications (AINA'06)*. Volume 1, pages 451-458.

Par, G. (2004). Investigating Information Systems with Positivist Case Study Research. *Communications of the Association for Information Systems*. 13(1). pp233-264.

Park, Yj. and Lee, Kh. (2018). Constructing a secure hacking-resistant IoT U-healthcare environment. *J Comput Virol Hack Tech* **14,** 99–106. https://doi.org/10.1007/s11416-017-0313-7

Patrick, K. (2010). Staying one step ahead of the hackers. *NZ Business* (New Zealand). Jul. Vol. 24, Iss. 6, pages 50.

Pavel, C., Radek, K., Jan, V., Martin, D. (2010). Embedded Malware - An Analysis of the Chuck Norris Botnet. *European Conference on Computer Network Defense*. pages 3-10.

Payer, M., Hartmann, T., and Thomas R. (2012). Gross Safe Loading - A Foundation for Secure Execution of Untrusted Programs. *33rd IEEE Symposium on security and privacy (S&P 2012).* IEEE computer society (USA). Pages 18-32.

Payne, B. D., Carbone, M., Sharif, M. and Lares, W. (2008). An architecture for secure active monitoring using virtualization. In *IEEE Symposium on Security and Privacy*. Oakland, CA, USA: IEEE.

PCI-DSS (2020). *PCI DSS Penetration Test Requirements*. PCI Security Standards Council LLC (USA). Available at: https://www.pcidssguide.com/pci-penetration-test-requirements/. Visited on: 02/August/2021.

PCI-DSS (2021a). *PCI Security Standard Version 4.0*. PCI Security Standards Council LLC (USA).

PCI-DSS (2021b). *PCI Compliance Guide*. PCI Security Standards Council LLC (USA). https://www.pcicomplianceguide.org/faq/

PCI-DSS (2021c). *Verify PCI Compliance*. PCI Security Standards Council (USA). Available at: https://www.pcisecuritystandards.org/. Visited on: 02/August/2021.

Peter, O. and Thomas, J. (2007). On the Anatomy of Human Hacking. *Information Systems Security*. Taylor & Francis Group (UK). Nov/Dec. Vol. 16, Iss. 6, pages 302-314.

Pham,L. H., Albanese, M., Chadha, R., Chiang, C.-Y. J., Venkatesan, S., Kamhoua, C., and Leslie, N. (2020). A quantitative framework to model reconnaissance by stealthy attackers and support deception-based defences. *IEEE Conference on Communications and Network Security (CNS)*. IEEE, pp. 1–9.

Phil, Cox. (2011). *White-Paper: Cloud Computing Security Up Close*. TechTarget (USA). July. Available at: http://docs.media.bitpipe.com. Visited on: 12th July 2017.

Picoto, W., Bélanger, F., and Palma-dos-Reis, A. (2014). *An organizational perspective on m-business: usage factors and value determination*. European Journal of Information Systems, 23(5), 571–592.

Ponemon (2017). White paper: *State of Web Application Security*. Ponemon Institute LLC (USA). Available at: https://securityintelligence.com. Visited on: 12th July 2017.

Ponemon (2019). White paper: *Ponemon Report: Cost of Web Application & Denial of Service*. Ponemon Institute LLC (USA).. Available at: https://securityintelligence.com. Visited on: 12th Aug 2019.

Ponemon (2021). White paper: *Reducing Enterprise Application Security Risks: More Work Needs to Be Done*. Ponemon Institute LLC (USA).. Available at: https://www.ponemon.org/research/ponemon-library/security/reducing-enterprise-application-security-risks-more-work-needs-to-be-done.html. Visited on: 25th April 2021.

Ponemon. (2018). State of Endpoint Security Risk (2018)

Powell, C. (2003). The Delphi Technique: Myths and Realities. *Journal of Advanced Nursing 41(4), 376–382.*

Prashant, D., Partha, D. and Amiya, B. (2009). Mitigating routing vulnerabilities in ad hoc networks using reputations. *International Journal of Information and Computer Security* (USA). Vol. 3, No.2, pages 150-172.

Prescott, E. (2011). *An Impractical Strategy for a Cyber World.* CreatSpace Independent (USA). ISBN: 9781-4657918994.

Prescott, E. (2012). White Paper: *Defense in Depth: An Impractical Strategy for a Cyber World.* SANS Institute (USA).

Prestamo, A. M. (2000). A comprehensive inventory of technology and computer skills for academic reference librarians. Digital Abstracts International, 61 (09), 3401. (UMI No. 9987367).

Privacyrights (2017) *Data-Breaches*. Privacy Rights Organization (USA). Available at: www.privacyrights.org/data-breaches. Visited on: 15th October 2017

Purple Security (2021). 2021 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends. Purple Security. USA. Available at https://purplesec.us/resources/cyber-security-statistics/. Visited date: 29th September 2021.

Purple Security. (2021). 2021 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends. *Purple Security.* (USA). Available at https://purplesec.us/resources/cyber-security-statistics/. Visited date: 29th September 2021.

PWC (2009). White paper: *BERR Survey on Security Breaches.* UK Government (UK).

Qian, Z. and Mao, Z. (2012). Off-path TCP Sequence Number Inference Attack - How Firewall Middleboxes Reduce Security. *33rd IEEE Symposium on security and privacy (S&P 2012).* IEEE computer society (USA). Pages 337–364.

QSI (2008). White paper: *Defender 5: The Right Way to Prove Identify and Establish Trust.* Quest Software Incorporation (USA).

Rachana, D. (2010). What the hack. *Tribune Business News* (USA). July.

Raghavan, B., Kohno, T., Snoeren, A., and Wetherall, D. (2009). Enlisting ISPs to improve online privacy: IP address mixing by default. In *Proceedings of PETS (USA).*

Raja, K. S., Syed, I. H., Niklas, L. (2010). Detection of Spyware by Mining Executable Files. *International Conference on Availability, Reliability and Security*. Pages 295-302.

Rajesh, K. T. and Sahoo, G. (2011). A novel steganographic methodology for high capacity data hiding in executable files. *International Journal of Internet Technology and Secured Transactions* (India). Vol. 3, No.2, pages 210–222.

Rakhra, T., Kaushal, A., Tanwar, S., Datta, P. and Rana, A. (2020). De Authentication Attack: A Review. 2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC). IEEE. USA.

Ramesh, K., Jeyavijayan, R., Kurt, R. and Mohammad, T. (2010). Trustworthy Hardware. Identifying and Classifying Hardware Trojans. *Computer*. October. Vol. 43, no. 10, pages 39-46.

Ramsey, J. W. & Edwards, M. C. (2011). Entry-level technical skills that agricultural industry experts expected students to learn through their supervised agricultural experiences: A modified Delphi study. *Journal of Agricultural Education, 52(2)*, 82-94. doi: 10.5032/jae.2011.02082

Randall, Gamby. (2011). *SMS two-factor authentication for electronic identity verification*. TechTarget Inc (USA). Available at: http://searchsecurity.techtarget.com/. Visited on: 15th August 2017.

Ransbotham, S. & Mitra, S. (2009). Choice and chance: a conceptual model of paths to information security compromise. *Information Systems Research*, 20(1), 121-139.

Rath, G., and Stoyanoff, K. (1983). The Delphi technique. In F. L. Ulschak (Ed.), *Human resource development: The theory and practice of need assessment* (pp. 111-131). Reston, VA: Reston.

Raval, V. and Fichadia, A. (2007). *Risks, Controls, and Security: Concepts and Applications*. Wiley (USA).

Ray, I. and Kumar, M. (2006). Towards a location-based mandatory access control model. *Computers and Security*. February. Volume 25, Issue 1, pages 36-44.

Reddy, V., Kolli, N. & Balakrishnan, N. (2021). Malware detection and classification using community detection and social network analysis. *J Comput Virol Hack Tech* (USA). doi.org/10.1007/s11416-021-00387-x.

Ridenour, C. S., and Newman, I. (2008). *Mixed Methods Research: Exploring the Interactive Continuum, Carbondale*, IL. Southern Illinois University Press. (USA).

Risen, T. (2014). Study: Hackers Cost More Than $445 billion Annually. *US News and World Report* (USA). July 2014. Available at: https://www.usnews.com/news/articles/2014/06/09/study-hackers-cost-more-than-445-billion-annually. Visited on: 24 September 2017.

Robert, E. and France, B. (2009). The Effects of Security Education Training and Awareness Programs and Individual Characteristics on End User Security Tool Usage. *Journal of Information System Security*. Washington DC, USA: Information Institute Publishing. Volume 5, No. 3, pages 3–22.

Robert, K., Frederick, T. and Ali, M. (2011). Validating Cyber Security Requirements. A Case Study. *44th Hawaii International Conference on System Sciences*. Pages 1-10.

Robert, W. (2011a). *Attackers zero in on Web application vulnerabilities*. TechTarget Inc (USA). Available at: http://searchsecurity.techtarget.com/. Visited on 10th August 2017.

Robert, W. (2011b). *Software code analysis firm gives security vendors poor marks*. TechTarget Inc (USA). Apr, 20. Available at: http://searchsecurity.techtarget.com/. Visited on 10th August 2017.

Roberta, Bragg (2012a). *Checklist: Lock down PCs, workgroups and AD domains*. TechTarget Inc (USA). Available at: http://searchwindowsserver.techtarget.com/. Visited on: 27th April 2017.

Roberta, Bragg (2012b). *Checklist: Secure domain controller settings*. TechTarget Inc (USA). Available at: http://searchwindowsserver.techtarget.com/. Visited on: 27 April 2017.

Robin, S. and Nikita, B. (2011). Improving Security and Performance in the Tor Network through Tunable Path Selection. *IEEE Transactions on Dependable and Secure Computing* (USA). September/October. Vol. 8, no. 5, pages 728-741.

Robinson, B. (2015). Cyberattack platforms call for defense in depth and breadth. *CyberEye (USA).* Available from https://gcn.com/Blogs/CyberEye/2014/12/Backdoor-Regin-APT.aspx?p=1. Visited on: 20th June/2017.

Roesner, F., Kohno, T., Moshchuk, A., Parno, B., Wang, H. and Cowan, C. (2012). User-Driven Access Control. Rethinking Permission Granting in Modern Operating Systems. *33rd IEEE Symposium on security and privacy (S&P 2012).* IEEE computer society (USA). Pages 224-238.

Rohit, S. and Nish B (2009). *Vulnerability test methods for application security assessments*. TechTarget Inc (USA). Available at: http://searchsecurity. techtarget.com/. Visited on 25th March 2017.

Role based access control - Saxena, U. and Alam, T. (2021). Role based access control using identity and broadcast based encryption for securing cloud data. *J Comput Virol Hack. Tech* https://doi.org/10.1007/s11416-021-00402-1

Rostami, M., Bashah, I. and Zuraini, I. (2016) A holistic botnet detection framework independent of botnet protocols and architecture. In: *International Conference on Advanced Information and Communication Technology,* 16 May, 2016, Chittagong, Bangladesh

Rowley, J. (2014). Designing and using research questionnaires. *Management Research Review*. Vol. 37, No. 3, pages 308-330

RSA (2011). White Paper: *Making Sense of Man-in-the-browser Attacks: Threat Analysis and Mitigation for Financial Institutions*. RSA security LLC. (USA). Available at: https://www.rsa.com/content/dam/rsa/PDF/Making_Sense_of_Man_in_the_browser_attacks.pdf. Visited on 25th March 2017.

Runesin, P. and M. Host (2009). Guidelines for conducting and Reeporting Case Study research in Software Engineering. *Empirical Sofware Engineering* (USA) 14(2): 131-164.

Runeson, P., & Höst, M. (2009). Guidelines for conducting and reporting case study research in software engineering. *Empirical Software Engineering*, 14(2), 131-164.

Russinovich, M. and Schmidt, H. (2011). *Zero Day: A Novel.* Thomas Dunne Books (USA).

Rutvij, H. J., Ashish, D. P., Jatin, D. P. and Bhavin, I. S. (2010). MANET Routing Protocols and Wormhole Attack against AODV. *International Journal of Computer Science and Network Security.* April. Vol. 10, No. 4, pages 12-18.

Sachowski, J. (2018). *Digital Forensics and Investigations.* Taylor & Francis (USA). ISBN-13: 978-1-138-72093-0.

Sackman, H. (1974a). *Delphi assessment: Expert opinion, forecasting, and group process* (No. RAND-R-1283-PR). RAND Corporation. Santa Monica, CA. Available at: http://www.rand.org/pubs/reports/R1283.html. Visited on: 10th October 2017.

Sackman, H. (1974b). *Delphi critique; expert opinion, forecasting, and group process* (RAND Report No. R-1283-PR). Lexington, Mass.,: Lexington Books.

Saha T., Aaraj, N., Ajjarapu N. and Jha, T. K. (2021). SHARKS: Smart Hacking Approaches for Risk Scanning in Internet-of-Things and Cyber-Physical Systems based on Machine learning. *IEEE Transactions on Emerging Topics in Computing*. IEEE. USA

Saha, T., Aaraj, N., Ajjarapu, N., and Jha, N. K. (2021). SHARKS: Smart Hacking Approaches for RisK Scanning in Internet-of-Things and Cyber-Physical Systems based on Machine learning. IEEE Transactions on Emerging Topics in Computing. IEEE. USA.

Salvatore, J. S., Malek Ben Salem, and Keromytis, Angelos D. (2012). Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud. *IEEE CS on Security and Privacy Workshops.* IEEE computer society (USA). Pages 125–128.

Sami, R. (2009). A look at Portable Document Format vulnerabilities. *Information Security Technical Report* (Stonesoft Corporation, Finland). February. Volume 14, Issue 1, pages 30-33.

Sanchez, F., Lin, W. and Korunka, .K. (2019). Applying Irregular Warfare Principles to Cyber Warfare. *Joint Force Quarterly, Vol 92, 1st Quarter 2019*. National Defense University Press. (USA). Pp15-22. Available at: Library: www.dtic.mil/doctrine/jfq/jfq.htm. Visited Date: 02 January 2021.

Sanjay, G., Salvatore, B. and Laura, I. (2004). A Resilient Network that Can Operate Under Duress to Support Communication between Government Agencies during Crisis Situations. *37th Annual Hawaii International Conference on System Sciences (HICSS'04)*. vol. 5, Pages 50123a.

SANS Institute (2015) WhitePaper: *2015 Analytics and Intelligence Survey*. SANS Institute Organization (USA). Available at: https://www.sans.org/reading-room/whitepapers/analyst/2015-analytics-intelligence-survey-36432. Visited on: 28th September 2017

SanthiJeslet, D., Sivaraman, G., Uma, M., Thangadurai, K. and Punithavalli, M. (2010). Survey on Awareness and Security Issues in Password Management Strategies. *International Journal of Computer Science and Network Security*. April. Vol. 10, No. 4, pages 19-23.

Saravanan, K. (2010). An effective defence mechanism for Distributed Denial-of-Service (DDOS) attacks using router-based techniques. *International Journal of Critical Infrastructures.* (Department of CSE, Erode Sengunthar Engineering College, ERODE-57, India). Vol. 6, No.1, pages 73–80.

Sarker, S. & Lee, A.S. (2002). Using a positivist case research methodology to test three competing theories-in-use of business process redesign. *Journal of the Association for Information Systems, 2(7).*

Sarker, S. & Lee, A.S. (2003). Using a case study to test the role of three key social enablers in ERP implementation. *Information & Management*, 40, 813-829

Satish, N. S., Matthias, J. and Wolfgang, P. (2007). Security analysis of mobile web service provisioning. *International Journal of Internet Technology and Secured Transactions* (Germany). Vol. 1, No.1/2, pages. 151-171.

Sattarova Feruza, Y. and Tao-hoon, K. (2007). IT Security Review. Privacy, Protection, Access Control, Assurance and System Security. *International Journal of Multimedia and Ubiquitous Engineering*. Vol. 2, No. 2. Pages 17-31.

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo K. and Burnap, P. (2020). Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. *Electronics*. Vol 9, 1460; doi:10.3390/electronics9091460. Visited Date: 02 January 2021.

Saxena, U.R. and Alam. (2021), T. Role based access control using identity and broadcast based encryption for securing cloud data. *J Comput Virol Hack Tech*.doi.org/10.1007/s11416-021-00402-1

Scambray, J., Shema, M. and Sima, C. (2010). *Hacking Exposed: Web Application.* 3rd Edition. McGraw-Hill Osborne Media (USA).

Scheibe, M., Skutch, M. & Schofer, J. (1975). Experiments in Delphi Methodology. In H. A. Linstone, & M. Turoff (Eds.) *The Delphi Method: Techniques and Applications*. Reading, MA: Addison-Wesley Publishing Company. (USA). pp 262-287.

Schell, B. H., & Dodge, J. L. (2002). *The hacking of America: Who's doing it, why, and how*. Greenwood Publishing Group Inc. (USA).

Schifreen, R. (2006). *Defeating the Hackers*. Wiley (UK).

Schmidt, R., Lyytinen, K., Keil, M., & Cule, P. (2001). Identifying software project risks: An international Delphi study. Journal of Management Information Systems, 17(4), 5 - 36.

Schneier, B. (2015). *Applied Cryptography*. WILEY (USA). ISBN-13: 978-1119096726.

Schuessler, J. 2009. *General deterrence theory: Assessing information systems security effectiveness in large versus small businesses*. Ph.D. dissertation, University of North Texas (USA). (Publication No. AAT 3377466).

Schuessler, J. H. (2009). *General deterrence theory: Assessing information systems security effectiveness in large versus small businesses.* Unpublished manuscript, University of North Texas.

Schwab, W., and Poujol, M. (2018). The State Of Industrial Cybersecurity. *Trend Study Kaspersky Reports*, p. 33.

Scott, D. (2014). White Paper: *Defense in depth and breadth: Securing the Internet of Things*. CSG Invotas International (USA). Available from https://inform.tmforum.org/sponsored-feature/2014/09/defense-depth-breadth-securing-internet-things/. Visited on: 25th June/2017.

Seacord, R. C. (2013). *Secure Coding in C and C++*. 2nd edition. Addison Wesley (USA). ISBN-13: 978-0321822130.

Seokhee, L., Antonio, S., Sangjin, L. and Jongin, L. (2007). Password Recovery Using an Evidence Collection Tool and Countermeasures. *International Conference on Information Hiding and Multimedia Signal Processing* (USA). Vol. 2, pages 97-102.

Serror, M., Hack, S., Henze, M., Schuba, M., and Wehrle, K. (2021). Challenges and Opportunities in Securing the Industrial Internet of Things. IEEE Transactions on Industrial Informatics, vol. 17, no. 5, pp. 2985-2996, May 2021, doi: 10.1109/TII.2020.3023507

Shackleford, D. (2016) *Using Analytics to Predict Future Attacks and Breaches*. SANS Institute Organization (USA). Available at: https://www.sans.org/reading-room/whitepapers/analyst/analytics-predict-future-attacks-breaches-36720. Visited on: 12th July 2017

Shackleford, Dave (2012). *Penetration testing tutorial: Guidance for effective pen tests*. TechTarget Inc (USA). Available at: *http://searchsecuritychannel. techtarget.com/*. Visited on 28th March 2017.

Shapland, Rob (2010). *Session fixation protection: How to stop session fixation attacks*. TechTarget Inc (UK). June. Available at: http://searchsecurity. techtarget.co.uk/. Visited on 20th April 2017.

Shearman and Sterling (2014). Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm. *Writing Prize inComparative and International Law*, Outstanding Note Award. Available at: http://jtl.columbia.edu/wp-content/uploads/sites/4/2014/05/MesserschmidtNoteHackback.pdf. Visited on: 10th September 2017.

Shema, M., Davis, C. and Cowen, D. (2006). *Anti-Hacker Tool Kit*. 3rd edition. McGraw-Hill/ Osborne (USA).

Shimonski, R., Schmied, W., Chang, V. and Shinder, T. (2003). *DMZs for Enterprise Networks*. SYNGRESS (USA).

Shokri, R., Theodorakopoulos, G., Boudec, J. and Hubaux, J. (2011). Quantifying Location Privacy. *32nd IEEE Symposium on security and privacy (S&P 2011).* IEEE computer society (USA). Pages 247–262

Shuman, D. (2000). Implementation theory and determinants for success: A case study of televised distance learning implementation in an urban university. Digital Abstracts International, 61 (04), 1371. (UMI No. 9970453).

Singaravel, G., Palanisamy, V. and Krishnan, A. (2010). Adaptive Reusability Risk Analysis Model (ARRA). *International Journal of Computer Science and Network Security.* Feb. Vol. 10 No. 2, pages 97-101.

Singleton, T. W. and Singleton, A. J. (2010). *Fraud Auditing and Forensic Accounting.* 4th Edition. Wiley (USA).

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management and Computer Security, 8*(1), 31–41.

Skoudis, Ed. (2012). *How can hackers bypass proxy servers*. TechTarget Inc (USA). Available at: http://searchsecurity.techtarget.com/.Visited on: 27th March 2017.

Skulmoski, Gregory J., Hartman, Francis T. and Krahn, J. (2007). The Delphi Method for Graduate Research. *Journal of Information Technology Education*. Volume 6, 2007.

Slim, K., Anis, C., Mira, M., Mohamed, J. and Andreas, S. (2009). A holistic approach for access control policies: From formal specification to aspect-based enforcement. *International Journal of Information and Computer Security.* (Germany). Vol. 3, No.3/4, pages 337–354.

Slim, R., Jihene, K. and Noureddine, B. (2008). Cognitive-Maps Based Investigation of Digital Security Incidents. *IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*. Pages 25-40.

Smith, P. D. (2009). *Developing & Implementing an Information Security Policy and Standard Framework.* SANS Institute (USA).

Solanki, K., Sullivan, K. and Madhow, U. (2008). *Information Hiding*. 10^{th} edition. Springer (USA).

Spivey, M. D. (2007). *Practical Hacking Techniques and Countermeasures.* Auerbach Publications (USA).

Sriramkrishnan, S. (2010). Identity based encryption. Progress and challenges. *Information Security Technical Report* (UK). February. Volume 15, Issue 1, pages 33-40.

SSC, Search Security Channel (2010). *Snort Tutorial: How to use Snort intrusion detection resources*. TechTarget Inc (USA). Available at: http://searchsecuritychannel. techtarget.com. Visited on 27^{th} Jul 2017.

Statista (2020). https://www.statista.com/statistics/617136/digital-population-worldwide/ Visited Date: 22 February 2021.

Stefano, Z. (2010). Observing the Tidal Waves of Malware: Experiences from the WOMBAT Project. *International Conference on Information Technology for Real World Problems*. December. Pages 30-35.

Steganography based Information Hiding - Jayakokela, S. and Avila, J. (2021). Steganography based Information Hiding and Transmission via SC-FDMA *Transceiver. 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*. IEEE. USA

Sterling, B. (1992). *The Hacker Crackdown, law and disorder on the electronic frontier*. New York: Bantam.

Stewart, J. M., Chapple, M., Gibson, D. and Seidl, D. (2016) *CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide and Official ISC2 Practice Tests 7^{th} Edition*. Sybex (USA). ISBN-13: 978-1119314011.

Stewart, J. M., Chapple, M., Gibson, D. and Seidl, D. (2016). *CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide and Official ISC2 Practice Tests 7th Edition*. Sybex (USA). ISBN-13: 978-1119314011.

Stiennon, Richard. (2015) *There Will Be Cyberwar: How The Move To Network-Centric Warfighting Has Set The Stage For Cyberwar*. IT-Harvest Press (USA). ISBN:0985460784

Stiennon, Richard. (2015). *There Will Be Cyberwar: How The Move To Network-Centric Warfighting Has Set The Stage For Cyberwar*. IT-Harvest Press (USA). ISBN:0985460784.

Storm, D. (2011). Epsilon breach: hack of the century. *Computer World (USA).* April 04th.

Straub, D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research* (1:3), 255-276

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *Management Information Systems Quarterly*, 22(4), 441.

Straub, D., & Weike, R. J. (2008). Coping With Systems Risk : Security Planning Models for Management Decision Making. *MIS Quarterly, 22*(4), 441–469

Stuart, I., McCutcheon, D., Handfield, R., McLachlin, R., & Samson, D. (2002). Effective case research in operations management: a process perspective. *Journal of Operations Management*, 20, 419-433

Sturton, C., Hicks, M., Wagner, D. and King, S. (2011). Defeating UCI: Building Stealthy and Malicious Hardware. *32nd IEEE Symposium on security and privacy (S&P 2011).* IEEE computer society (USA). Pages 64-77.

Stuttard, D. and Pinto, M. (2011). *The Web Applications Hacker's: Discovering and Exploring Security Flaws*. Wiley (USA).

Stytz, M. and Whitaker, J. (2003). Software Protection Security's Last Stand. *IEEE Security & Privacy* (USA). *Vol 1, Issue 1*. Pages 95-98.

Subramanian, R., Avula, R., Surya, P. and Pranay, B. (2021). Modeling and Predicting Cyber Hacking Breaches. *5th International Conference on Intelligent Computing and Control Systems (ICICCS).* IEEE. USA

Summers, T. (2015). *How Hackers Think: A Mixed Method Study Of Mental Modelsand Cognitive Patterns Of High-Tech Wizards*. PhD (Management), Case Western Reserve University. USA.

Summers, T. C., Lyytinen, K. J., and Gaskin, J. (2014). How Hackers Think: Understanding the Mental Models and Cognitive Patterns of High-Tech Wizards: Case Western Reserve University.

Sun Tzu, and Cleary, T. (2005). *The Art of War*. Shambhala Publications Inc. (USA).

Swenson, C. (2008). *Modern Cryptanalysis Techniques for Advanced Code Breaking*. 1st edition. Wiley Publishing (USA).

Syngress, S. (2006). *IT Security Project Management*. 1st edition. Andrew Williams (Canada).

Tammy, L. Clark, and Stiko, T. D. (2008). White paper: *Information Security Governance - Standardizing the Practice of Information Security*. Educause-Center for Applied Research. August. Vol, issue 17.

Tashakkori, A., and Teddlie, C. (2003). The Past and the Future of Mixed Methods Research: From 'Methodological Triangulation' to 'Mixed Methods Designs', *in Handbook of Mixed Methods in Social and Behavioral Research*, A. Tashakkori and C. Teddlie (eds.), Thousand Oaks, CA: Sage Publications, pp. 671-701.

Tasmanian (2021a). White Paper: *Information Security Framework*. Tasmanian Government (Australia). Available at: https://www.informationstrategy.tas.gov.au/Government-Information-Strategy. Visited on: 6th Nov 2021.

Tasmanian (2021b). White paper: *Information Security Guidelines*. Tasmanian Government (Australia). Available at: https://www.6clicks.com/content/tas-information-security-framework-isf/. Visited on: 06th Nov 2021.

Taylor, P. A. (1999). *Hackers: crime in the digital sublime*. Psychology Press. (USA)

Taylor, S. E., Pham, L. B., Rivkin, I. D., & Armor, D. A. (1998). Harnessing the imagination: Mental simulation, self-regulation, and coping. *American psychologist, 53(*4): 429.

Taylor-Powell E. and Renner M. (2009). Collecting Evaluation Data: end-of-Session Questionnaire. UW-Extension (USA). Available at https://learningstore.uwex.edu/Assets/pdfs/G3658-11.pdf. Visited on: 20 September 2017

Taylor-Powell Ellen (1998). Program Development and Evaluation-Questionnaire Design: Asking questions with a purpose. UW-Extension (USA). Available at https://learningstore.uwex.edu/Assets/pdfs/G3658-02.pdf. Visited on: 20 September 2017

Teddlie, C., and Tashakkori, A. (2009). *Foundations of Mixed Methods Research*. Thousand Oaks, CA: Sage Publications.

Tejay, G.P.S. & Zadig, S.M. (2012). Investigating the effectiveness of IS security countermeasures towards cyber attacker deterrence. *Proceedings of the 45th Annual Hawaii International Conference on Systems Sciences*, Maui, Hawaii.

Telstra (2017) *Telstra Cyber Security Report 2017*. Telstra Corporation (USA). Available at: https://www.telstraglobal.com/images/assets/insights/resources/Telstra_Cyber_Security_Report_2017_-_Whitepaper.pdf. Visited on 30th Oct 2017

Thaier, H., Razvi, D., Prashant, K. and David, T. (2011). Source—destination obfuscation in wireless adhoc networks. *Security and Communication Networks*. John Wiley & Son Ltd (USA). August. Volume 4. Issue 8. Pages 888–901.

Thawatchai, C. (2007). HTTPS Hacking Protection: *International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)*. Vol. 1, pp. 590-594.

The Economic Times Security. (2021). Definition of 'Hacking' Definition. *The Economic Times English Edition, IST, E-Paper*. Available at: https://economictimes.indiatimes.com/definition/hacking. Visited Date: 02 January 2021.

The Irrawaddy. (2021). Myanmar Hackers Take Down Military-Run Websites. *The Irrawaddy*. (Myanmar). Available at:

https://www.irrawaddy.com/news/burma/myanmar-hackers-take-military-run-websites.html. Visited on: 2nd Sep 2021.

The Mentor. (1986). Hacker's Manifesto. *Phrack Inc., 1(7), 3 of 10*. Available at: http://phrack.org/issues/7/3.html. Visited on: 20 September 2017.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers and Security, 24, 472–484.*

Thomas, D. (2002). *Hacker culture*: U of Minnesota Press. (USA).

Thomas, K., Grier, C., Ma, J., Paxson, V. and Song, D. (2011). Design and Evaluation of a Real-Time URL Spam Filtering Service. *32nd IEEE Symposium on security and privacy (S&P 2011).* IEEE computer society (USA). Pages 447–462.

Tieyan, Li and Guilin, Wang. (2011). Analyzing a Family of Key Protection Schemes against Modification Attacks. *IEEE Transactions on Dependable and Secure Computing* (USA). September/October. Vol. 8, no. 5, pages 770-776.

Tipton, H. and Krause, M. (2007). *Information Security Management Handbook.* 6th Edition. Auerbach Publication (USA).

Toapanta, S. M., Caicedo, H. A., Sanchez, B. A. and Gallegos, L. E. (2020). Analysis of Security Mechanisms to Mitigate Hacker Attacks to Improve e-Commerce Management in Ecuador. International Conference on Information and Computer Technologies (ICICT). IEEE. USA.

Toapanta, S., Caicedo, H., Sanchez, B. and Gallegos, L.. (2020). Analysis of Security Mechanisms to Mitigate Hacker Attacks to Improve e-Commerce Management in Ecuador. *3rd International Conference on Information and Computer Technologies (ICICT)*. IEEE. USA.

Trabelsi, Z., & McCoey, M. (2016). Ethical hacking in Information Security curricula. *International Journal of Information and Communication Technology Education*, 12(1), 1- 10. (USA)

Tripathy, S. and Nandi, S. (2008). Secure user-identification and key distribution scheme preserving anonymity. *International Journal of Security and Networks*. Vol. 3, No.3, pages 201–205.

Trostle, J., Way, B., Matsuoka, H., Tariq, M., Kempf, J. and Jain, R. (2004). Cryptographically protected prexes for location privacy in IPv6. In *Proceedings of PETS (USA).*

Trump, D. (2018), National Cyber Strategy of the United States of America. *Washington DC*. The White House.

Trustwave (2015). White paper: *Web-Application-Firewall*. Trustwave Incorporation (USA). Available at: https://www.trustwave.com/Products/Application-Security/Web-Application-Firewall/. Visited on: 12/August/2017.

Tsai, J. (2008). Efficient multi-server authentication scheme based on one-way hash function without verification table. *Computers and Security***.** May. Volume 27, Issue 3-4, pages 115-121**.**

Tsai, K.Y., Hsu, C.L. and Wu, T.C. (2010). Mutual anonymity protocol with integrity protection for mobile peer-to-peer networks. *International Journal of Security and Networks*. Vol. 5, No. 1, pages 45–52.

Turkle, S. (1984). The Second Self (Twentieth). *Cambridge, MA*: MIT Press.

Tutton, J. (2010). Incident response and compliance. A case study of the recent attacks. *Information Security Technical Report Elsevier Ltd*. November. Volume 15, Issue 4, pages 145-149.

Uhr, C. (2017), Leadership ideals as barriers for efficient collaboration during emergencies and disasters. *Journal of Contingencies and Crisis Management* 25 (4), 301-312.

Ulschak, F. L. (1983). *Human Resouces Developments. The Theory and Practice of Need Assessments.* Reston, V A: Reston Publishing Company, Inc. (USA).

Urbach, N., Ahlemann, F. (2010). Structural Equation Modelling in Information Systems Research Using Partial Least Squares. Journal Of Information Technology Theory And Application. Vol 11, issue 2, 98, 400-405.

US-CERT (2021a). *PGP Public Key Block Version: Encryption Desktop 10.3.2 (Build 15413).* U.S. Department of Homeland Security (USA). Available at:

https://us-cert.cisa.gov/sites/default/files/documents/ICS-CERT_PGP_Pub_Key.asc. Visited on: 28th August 2021.

US-CERT (2021b). White Paper: *Recommended Practice: Improving Industrial Control Systems Cyber security with Defense-in-Depth Strategies.* U.S. Department of Homeland Security (USA). Available at: https://us-cert.cisa.gov/ics/Recommended-Practices. Visited on: 28th August 2021.

Vaughan, J. and Chong, S. (2011). Inference of expressive declassification policies. *32nd IEEE Symposium on security and privacy (S&P 2011).* IEEE computer society (USA). Pages 180–194.

Vazquez-Ramos, R. A. (2003). A Delphi study to assess a potential set of items to evaluate participatory ethics in rehabilitation counseling. Digital Abstracts International, 64 (04), 1231. (UMI No. 3087663).

Venkataram, P., Jeremy, P., Sathish, B. and Mamdani E. (2008) . An intelligent proactive security system for cyber centres using Cognitive Agents. *International Journal of Information and Computer Security* (UK). Vol. 2, No.3, pages 235-249.

Venkatesh, B., Brown, S. and Bala, H. (2013) Bridging the Qualitative–Quantitative Divide. *MIS Quarterly.* Vol. 37 No. 1/March 2013.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: toward a unified view. *MIS Quarterly*, 27(3), 425–478

Verizon (2010). Verizon RISK Team - *Data Breach Investigations Report*. July. Verizon Business (USA). Pages 26.

Verizon (2014) *Reports on Database Incident Response*. Verizon Enterprise (USA). Available at: www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf. Visited on: 12th July 2017

Verizon (2017a) *2017 Data Breach Investigations Report (10th Edition).* Verizon Enterprise (USA). https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf. Available at: Visited on: 12th July 2017

Verizon (2017b) *Data Breach Digest- Perspective is Reality.* Verizon Enterprise

(USA). http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-perspective-is-reality_xg_en.pdf. Available at: Visited on: 12th July 2017.

Verizon (2017c) *Insider Threat.* Verizon Enterprise (USA). http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-insider-threat_xg_en.pdf. Available at: Visited on: 12th July 2017.

Vernon, W. (2009). The Delphi technique: A review. *International Journal of Therapy & Rehabilitation*, 16(2), 69-76.

Vijayalakshmi, A. and Soon, Ae C. (2007). A geotemporal role-based authorization system. *International Journal of Information and Computer Security* (USA). Vol. 1, No.1/2, pages 143-168.

Vijayalakshmi, A., Guo, Q., Heechang, S. and Jaideep, V. (2010). A unified index structure for efficient enforcement of spatiotemporal authorizations. *International Journal of Information and Computer Security* (USA). Vol. 4, No.2, pages 118.

Vijayan, J. (2009). *Hackers crack secure authentication*. CIO Corporation (UK).

Vural, Ü. and Thomas, H. (2005). The Access-Usage-Control-Matrix: A Heuristic Tool for Implementing a Selected Level of Technical Content Protection. *IEEE International Conference on E-Commerce Technology (CEC'05)*. Pages 512-517.

Wael, K., Nora, C. B., Frédéric, C. and Samuel, D. (2010). Risk-Aware Framework for Activating and Deactivating Policy-Based Response.*International Conference on Network and System Security* (USA). Page 207-215.

Wael, K., Nora, C. B., Frédéric, C., Samuel, D. and Antony, M. (2009). Success Likelihood of Ongoing Attacks for Intrusion Detection and Response Systems. *International Conference on Computational Science and Engineering*. Vol. 3, pages 83-91.

Wahsheh, Luay. A., and Mekonnen, Biruk. (2019). Practical Cyber Security Training Exercises. *International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE. USA

Waksman, A. and Sethumadhavan, S. (2011). Silencing Hardware Backdoor. *32nd IEEE Symposium on security and privacy (S&P 2011).* IEEE computer society (USA). 2011. Pages 49-63.

Wall, J., Lowry, P., and Barlow, J. (2016). Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems (JAIS).* (USA). Vol. 17(1) Available at: http://aisel.aisnet.org/jais/vol17/iss1/ . Visited on: 12th October 2017.

Wall, Jeffrey D., Lowry, Paul B. and Barlow, J. (2016). Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems. vol. 17*(1), pp. 39–76 ISSN: 1536-9323

Walonick, D. (2010). Survey and questionnaire design. Statpac, Inc (USA). ISBN 0-918733-11-1. Available at: http://www.statpac.com/surveys/ . Visited on: 22 September 2017

Wang Y., Wing-kei, Y., Shuo, W., Malysa, G., Suh, G. and Kan E. (2012). Flash Memory for Ubiquitous Hardware Security Functions. True Random Number Generation and Device Fingerprints. *33rd IEEE Symposium on security and privacy (S&P 2012).* IEEE computer society (USA). Pages 33-47

Wang, J. and Smith, G. L. (2010). A cross-layer authentication design for secure video transportation in wireless sensor, network. *International Journal of Security and Networks*. Vol. 5, No. 1, pages 63–76.

Wang, N., Liang, H., Zhong, W., Xue, Y. and Xiao, J. (2012). Resource structuring or capacity building? An empirical study of the business value of information technology. *Journal of Management Information Systems*, 29(2), 325-367.

Wang, P., Wu, L., Cunningham, R. and Zou, C. (2010). Honeypot detection in advanced botnet attacks. *Int. J. Information and Computer Security*. Vol. 4, No. 1, pages 30–51.

Wang-R., Chen, S. and Wang, X. (2012). Signing Me onto Your Accounts through Facebook and Google: A Traffic-Guided Security Study of Commercially

Deployed Single-Sign-On Web Services. *33rd IEEE Symposium on security and privacy (S&P 2012).* IEEE computer society (USA). Pages 365-379.

Watson, R. (2007). Exploiting concurrency vulnerabilities in system call wrappers. *WOOT* (USA).

Wawryn, K. and Widuliński, P. (2021). Detection of anomalies in compiled computer program files inspired by immune mechanisms using a template method. *J Comput Virol Hack Tech* **17,** 47–59 (2021). https://doi.org/10.1007/s11416-020-00364-w

Wayne, A. Jansen. (2011). Cloud Hooks: Security and Privacy Issues in Cloud Computing. *44th Hawaii International Conference on System Sciences* (USA). Pages 1-10.

Weber, R. (1988). *EDP auditing: Conceptual foundations and practice*. McGraw Hill. New York, USA.

Wei, L. and Issa, T. (2008). Unsupervised anomaly detection using an evolutionary extension of k-means algorithm. *International Journal of Information and Computer Security* (Canada). Vol. 2, No.2, pages 107–139.

Wei, Y., Nan, Z., Xinwen, F., Riccardo, B. and Wei, Z. (2010a). Localization Attacks to Internet Threat Monitors: Modeling and Countermeasures. *IEEE Transactions on Computers* (USA). December. Vol. 59, no. 12, pages 1655-1668.

Wei, Y., Nan, Z., Xinwen, F. and Wei, Z. (2010b). Self-Disciplinary Worms and Countermeasures: Modeling and Analysis. *IEEE Transactions on Parallel and Distributed Systems*. October. Vol. 21, no. 10, pages 1501-1514.

Wei, Y., Xun, W., Xinwen, F., Dong, X. and Wei, Z. (2009). An Invisible Localization Attack to Internet Threat Monitors. *IEEE Transactions on Parallel and Distributed Systems* (USA). November. Vol. 20, no. 11, pages 1611-1625.

Weinberg, Z., Chen, E., Jayaraman, P. and Jackson, C. (2011). I Still Know What You Visited Last Summer. *32nd IEEE Symposium on security and privacy (S&P 2011).* IEEE computer society (USA). Pages 147-161.

Weir, M., Aggarwal, S., Collins, M., and Stern, H. (2010). Testing metrics for password creation policies by attacking large sets of revealed passwords. In *Proceedings CCS (USA).*

Wells, J. T. (2008). *Principles of Fraud Examination.* 2ndEdition. Wiley (USA).

Wes, A. (2004). Understanding Spyware: Risk and Response. *IT Professional.* September/October. Vol. 6, No. 5, pages 25-29.

WesterVelt, Robert. (2010). Security Response Grapple With Cloud Computing. *Information security magazine* (USA). July/August. Vol. 12. Number 6, pages 13-14.

Whitman, M. E. (2004). In defense of the realm: Understanding the threats to information security. *International Journal of Information Management, 24*(1), 43–57.

Wiles, W. (2010). Insight: Design Hacks, Vol. 2015: *ICON Magazine*

William, W. (2010). Mobile telephony security compromises. *Information Security Technical Report* (UK). August. Volume 15, Issue 3, pages 134-136.

Williams, G. (2006). *Case Study. Crisis Management. When Disaster Strikes, Have a Plan. Then Change It As Needed.* New York, USA: NYC & Co. Nov 13. Vol. 62, Iss. 44.

Willison, R. & Warkentin, M. (2013). Beyond deterrence: an expanded view of employee computer abuse. *MIS Quarterly*, 37(1), 1-20.

Willison, R. (2000). Understanding and addressing criminal opportunity: the application of situational crime prevention to IS security. *Journal of Financial Crime, 7*(3), 201- 210.

Wisniewski, R., Benysek, G., Gomes, L., Kania, D., Simos, T. and Zhou, M. (2019). Cyber-physical systems. IEEE access. Vol. 7, pp. 157688–157692. doi: 10.1109/ACCESS. 2019. 2949898.

Witjes, N. and Wentland, A. (2021). Hacking Humans? Social Engineering and the Construction of the “Deficient User” in Cybersecurity Discourses. *Journal of Science, Technology, & Human Values*, Vol. 46(6) Pp1316-1339. Sage Publications. DOI: 10.1177/0162243921992844.

Wren, K. (2010). White Paper: *Fast and Effective Endpoint Security for Business – Comparative Analysis*. PassMark Software (Australia). June.

Wright, J. and Cache, J. (2015) *Hacking Exposed Wireless*. McGraw Hill (USA). ISBN-13: 978-0071827638

Wu, A. (2014). Project development for ethical hacking practice in a website security course. *Proceedings of the Western Canadian Conference on Computing Education* – WCCCE '14. (Canada)

Wynekoop, J. L. & Walz, D. B. (2000). Investigating traits of top performing software developers. Information Technology & People, 13(3), 186 - 197.

Xiao J., Yanming, W. and Zhiyu, H. (2010). A Malware Sample Capturing and Tracking System. *World Congress on Software Engineering*. December. Pages 69-72.

Xiao, F. W. and Michael, K. R. (2010). Using Web-Referral Architectures to Mitigate Denial-of-Service Threats. *IEEE Transactions on Dependable and Secure Computing* (USA). April-June. Vol. 7, no. 2, pages 203-216.

Xiaoli, L., Pavol, Z., Ron, R. and Dale, L. (2009). Threat Modeling for CSRF Attacks. *International Conference on Computational Science and Engineering*. Vol. 3, pages 486-491.

Xiaoxun, S., Hua, W., Jiuyong, L. and Yanchun, Z. (2011). Injecting purpose and trust into data anonymisation. *Science Direct (Australia).* June 7.

Xie, L., Yong-jun, Xu., Pan, Y., Yue-fei, Zhu. (2009). A Polynomial-Based Countermeasure to Selective Forwarding Attacks in Sensor Networks. *WRI International Conference on Communications and Mobile Computing*. Vol. 3, pages 455-459.

Xu, Z., Hu, Q., & Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM, 56*(4): 64-74.

Yanjun, Z. (2008). Prompt damage identification for system survivability. *International Journal of Information and Computer Security* (USA). Vol. 2, No.4, pages 411-433.

Yeh, Q., & Chang, A. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information and Management, 44*(5), 480–491.

Yihong, Z., Dapeng, W. and Scott, M. N. (2006). On MAC-layer denial of service attacks in IEEE 802.11 ad hoc networks. analysis and counter measures. *International Journal of Wireless and Mobile Computing* (USA). Vol. 1, No.3/4, pages 268–275.

Yin, R. K. (2003). Case Study Research: Design and Methods. *Thousand Oaks*. CA: SAGE Publications, 5.

Yin, R. K. (2009). Case Study Research: Design and Methods. *Singapore*. SAGE Publications.

Yinan, J., Zheng, X., Xueping, W. and Gendu, Z. (2006). O2-DN: An Overlay-based Distributed Rate Limit Framework to Defeat DDOS Attacks. *International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06)* (USA). Pages 79.

Yinghua, G. and Sylvie, P. (2010). Detect DDOS flooding attacks in mobile ad hoc networks. *International Journal of Security and Networks* (South Australia). Vol. 5, No.4, pages 259–269.

Yonemura, K., Kobayashi, H., Sato, J., Taketani, H., Oyama, S., Yamada, S., Izumi, S., Okamoto, H., Fujimoto, Y., Sakamoto, Y., Noguchi, and Kishimoto, S. (2021). Cybersecurity Teaching Expert Development Project by KOSEN Security Educational Community. IEEE Global Engineering Education Conference (EDUCON). IEEE. (USA).

Yoo, Y., Boland Jr, R. J., and Lyytinen, K. (2006). From organization design to organization designing. *Organization Science, 17*(2): 215-229

Young, R., & Zhang, L. (2007). Illegal computer hacking : An assessment of factors that encourage and deter the behavior. *Journal of Information Privacy & Security, 3, 33– 52.*

Youngho, C., Gang, Q., and Yuanming, W. (2012). Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor

Networks. *IEEE CS on Security and Privacy Workshops.* IEEE computer society (USA). Pages 134-141.

Yu, H., Gibbons, P., Kaminsky, M., and Xiao, F. (2008a). Sybil Limit: A nearoptimal social network defense *against Sybil attacks.* In Proceedings of the 2008 IEEE Symposium on Security and Privacy (S&P'08). May. Oakland, CA, USA: IEEE. Pages 3–17.

Yu, H., Kaminsky, M., Gibbons, P. and Flaxman, A. (2008b). SybilGuard: Defending against Sybil attacks via social networks. *IEEE/ACM Transactions on Networking*. Vol. 16, no. 3. IEEE (USA). June. Pages 576–589.

Yu, H., Shi, C., Kaminsky, M., Gibbons, P., and Xiao, F. (2009). DSybil: Optimal Sybil-resistance for recommendation systems. *In Proceedings of the IEEE Symposium on Security and Privacy (S&P'09).* May. Berkeley, CA, USA: IEEE. Pages 283–298.

Yuill, J., Denning, D., and Feer, F. (2006). Using Deception to Hide Things from Hackers. *Journal of Information Warfare*. Vol. 5, No. 3, pages 26-40.

Zadig, T. (2016). *Understanding the Impact of Hacker Innovation upon IS Security Countermeasures*. PhD (Information Systems), Nova Southeastern University. USA

Zadig, T. (2016). *Understanding the Impact of Hacker Innovation upon IS Security Countermeasures*. PhD (Information Systems), Nova Southeastern University. USA.

Zager, R., Zager, J. (2015). Deploying Deception Countermeasures. *Spearphishing Defense*. Iconix, Inc. Available at: file:///C:/Users/user/Downloads/Spearphishing_Defense_Using_Deception_Countermeasures.pdf. Visited on: 12th Jun 2017.

Zesheng, C., Chao, C. and Yubin, L. (2009). Deriving a closed-form expression for worm-scanning strategies. *International Journal of Security and Networks* (USA). Vol. 4, No.3, pages 135 – 144.

Zhang X., Hsiao, H., Hasker, G., Chan, H., Perrig, A. and Andersen, D. (2011). SCION: Scalability, Control, and Isolation On Next-Generation Networks.

32nd IEEE Symposium on security and privacy (S&P 2011). IEEE computer society (USA). Pages 212–227

Zhang Y., Juels, A., Oprea, A. and Reiter, M. (2011). HomeAlone: Co-Residency Detection in the Cloud via Side-Channel Analysis. *32nd IEEE Symposium on security and privacy (S&P 2011).* IEEE computer society (USA). Pages 313–328

Zhang, H., Banick, W., Yao, D., and Ramakrishnan, N. (2012). User Intention-Based Traffic Dependence Analysis for Anomaly Detection. *IEEE CS on Security and Privacy Workshops.* IEEE computer society (USA). Pages 104-112.

Zhanshan, S. (2011). Frailty modelling for risk analysis in network security and survivability. *International Journal of Information and Computer Security.* Vol. 4, No.3, pages 276 - 294.

Zhenyun, Z., Ying, Li and Zesheng, C. (2010). *Enhancing Intrusion Detection System with proximity information. International Journal of Security and Networks* (USA). Vol. 5, No.4, pages 207–219.

Zhou, Z., Gligor, V., Newsome, J., and McCune, J. (2012). Building Verifiable Trusted Path on Commodity x86 Computers. *33rd IEEE Symposium on security and privacy (S&P 2012).* IEEE computer society (USA). Pages 616-630.