

PENGOPTIMUMAN ALGORITMA PENGESANAN BATU LONCATAN
DALAM SISTEM PENGESANAN PENCEROBOHAN

MOHD NIZAM BIN OMAR

Tesis ini dikemukakan
sebagai memenuhi syarat penganugerahan
ijazah Sarjana Sains (Sains Komputer)

Fakulti Sains Komputer dan Sistem Maklumat
Universiti Teknologi Malaysia

MAY 2005

Buat ayah dan ibu yang tercinta.....

Omar Bin Ahmad
Seliah Binti Mat Sap

Juga sumber insiperasiku...
Zurianawati Ibrahim

Serta ...
Keluarga tersayang

PENGHARGAAN

Alhamdulillah, syukur ke hadrat Allah SWT kerana dengan limpah dan kurniaNya, penulis dapat menyiapkan tesis untuk penyelidikan dengan tajuk Pengoptimuman Algoritma Pengesanan Batu Loncatan Dalam Sistem Pengesanan Pencerobohan. Setinggi-tinggi penghargaan buat PM Dr. Mohd Aizaini Maarof yang telah membimbing serta memberi tunjuk ajar sepanjang tempoh penyelidikan ini dijalankan Bantuan dan teguran membina yang diberikan sudah pasti memberi banyak manfaat kepada penulis. Penghargaan turut diberikan kepada Pn. Anazida Zainal yang turut banyak membimbing. Kepada Pn. Subariah Ibrahim juga ucapan terima kasih diucapkan.

Terima kasih juga turut diucapkan kead Kementrian Sains, Teknologi dan Inovasi Malaysia yang memberikan sumbangan di dalam bentuk biasiswa sepanjang tempoh penyelidikan dilakukan.

Juga penghargaan tidak terhingga untuk pensyarah-pensyarah yang turut membantu dalam usaha memantapkan lagi penyelidikan yang dijalankan. Buat keluarga juga yang memberi sokongan dalam usaha penulis menghadapi penyelidikan ini. Juga tidak ketinggalan pemberi sumber inspirasi, Zurianawati Ibrahim. Tidak ketinggalan rakan-rakan seperjuangan yang membantu, juga individu yang terlibat secara langsung dan juga tidak langsung. Terima kasih diucapkan.

ABSTRAK

Pengesanan pencerobohan rangkaian dan penindakbalasan manual tanpa tindakan selanjutnya mendatangkan masalah yang dikenali sebagai jurang masa. Jurang masa adalah tempoh masa di antara pengesanan dan penindakbalasan. Penyelidikan terdahulu menggunakan pendekatan seperti agen pintar dan adaptasi Sistem Pengesanan Pencerobohan (IDS) untuk menyelesaikan masalah jurang masa. Walaubagaimanapun, penyelidikan terdahulu tidak mengambil perhatian aspek mekanisma penindakbalasan pencerobohan. Tujuan kajian ini adalah untuk mengoptimumkan algoritma batu loncatan, yang mana ianya sebahagian daripada mekanisma penindakbalasan pencerobohan. Di dalam penyelidikan ini, metodologi khas Atas-Bawah digunakan untuk mengoptimumkan algoritma batu loncatan. Ini dicapai dengan menganalisa lima algoritma batu loncatan, di mana setiap algoritma dibahagikan kepada tiga bahagian utama. Bahagian-bahagian tersebut adalah penawaran paket, pengenpastian dan perbandingan. Di antara algoritma-algoritma ini, pendekatan terbaik yang menghasilkan masa pemprosesan minimum untuk setiap bahagian dibangunkan dan diuji sebagai algoritma batu loncatan yang lengkap. Keputusan daripada kedua-dua pendekatan yang dioptimumkan dan algoritma sedia ada dibandingkan. Hasil daripada perbandingan, algoritma dioptimumkan memberikan keputusan yang terbaik. Penemuan daripada penyelidikan ini mencadangkan jurang masa boleh dikurangkan melalui pengoptimuman algoritma batu loncatan.

ABSTRACT

Detection of a network intrusion and manual response without any further action does create a problem known as time gap. Time gap is duration between detection and response. Previous researches have used some approaches like intelligent agent and IDS adoption to solve time gap problem. However, they do not consider the aspect of intrusion response mechanism. The purpose of this study is to optimize the stepping stone algorithm, which is part of intrusion response mechanism. In this research, special Top-Down methodology has been used to optimize the stepping stone algorithm. It is achieved by analyzing five stepping stone algorithms, in which each algorithm is divided into three main parts. The parts are packet capture, identification and comparison. Among these algorithms, the best approach which produces minimum processing time from each main part has been deployed and tested as a complete stepping stone algorithm. The results from both the optimized approach and existing algorithm are compared. From this comparison, the optimized algorithm gives the best result. The finding of this research suggests that time gap can be reduced through the optimization of the stepping stone algorithm.

KANDUNGAN

BAB	PERKARA	MUKA SURAT
1	PENGENALAN	
	1.1 Pengenalan	1
	1.2 Latar Belakang	3
	1.3 Pernyataan Masalah	4
	1.4 Tujuan	5
	1.5 Objektif	6
	1.6 Skop	6
	1.7 Andaian	7
	1.8 Kepentingan Kajian	7
	1.9 Hasil Jangkaan	8
	1.10 Organisasi Tesis	8
2	KAJIAN LATAR BELAKANG	
	2.1 Pengenalan	10
	2.2 Sistem Pengesanan Pencerobohan (IDS)	13
	2.3 Simulasi Serangan Siber, Pertahanan dan Akibat	16
	2.4 Jurang Masa	17
	2.4.1 Pencepatan Sebagai Penyelesaian Masalah Jurang Masa	19
	2.4.2 Sistem Penindakbalasan Pencerobohan (IRS) Sebagai Penyelesaian Kepada Masalah Jurang Masa	19
	2.5 Pendekatan Penindakbalasan Pencerobohan	21

2.5.1	Notifikasi	22
2.5.2	Penindakbalasan Manual	22
2.5.3	Penindakbalasan Aktif	23
2.5.4	Perbandingan Pendekatan	24
2.6	Jenis-jenis IRS	24
2.7	Teknik Penindakbalasan Pencerobohan	25
2.8	Penjejakan Pencerobohan	27
2.9	Teknologi Penjejakan Pencerobohan	29
2.9.1	Penjejakan Paket IP	29
2.9.1.1	Penjejakan Aktif	30
2.9.1.2	Penjejakan Pasif	31
2.9.1.3	Perbincangan	32
2.9.2	Penjejakan Sambungan	32
2.9.2.1	Sistem Penjejakan Berasaskan-hos	33
2.9.2.2	Sistem Penjejakan Berasaskan-rangkaian	34
2.9.2.3	Sistem Penjejakan Rangkaian Aktif	34
2.9.2.4	Perbincangan	35
2.10	Terminologi dan Notifikasi	37
2.10.1	Rantaian Sambungan	37
2.10.2	Batu Loncatan	38
2.10.3	Sambungan	38
2.10.4	Sambungan Aliran Ke Atas dan Aliran Ke Bawah	38
2.10.5	Aliran Paket	38
2.11	Pendekatan Penjejakan Berasaskan-rangkaian (<i>Thumbprint</i>)	39
2.12	Pendekatan Penjejakan Berasaskan-rangkaian (<i>ONOFF</i>)	40
2.13	Pendekatan Penjejakan Berasaskan-rangkaian (<i>Deviation</i>)	41
2.14	Perbincangan Pendekatan	42

2.15	Algoritma Pengesanan Batu Loncatan	43
	2.15.1 Algoritma <i>Brute-Force</i>	44
	2.15.2 Algoritma <i>Simple 1</i>	44
	2.15.3 Algoritma <i>Thumbprint</i>	45
	2.15.4 Algoritma <i>ONOFF</i>	45
	2.15.5 Algoritma <i>Deviation</i>	45
	2.15.6 Perbincangan	46
2.16	Pengoptimuman Algoritma	46
2.17	Pemecahan Sebagai Langkah Permulaan	
	Pengoptimuman	48
	2.17.1 Penawanan Paket	49
	2.17.1.1 Penggunaan Kemudahan	
	Penapisan Paket	50
	2.17.1.2 Penggunaan Penapisan Di Dalam	
	Kemudahan Penawanan Paket	51
	2.17.1.3 Penggunaan Kaedah Statistik Di	
	Dalam WinPcap	52
	2.17.1.4 Peranan Penimbal Kemudahan	
	Penawanan Paket	52
	2.17.1.5 Perbincangan	53
	2.17.2 Pengenalpastian Identiti Unik	53
	2.17.2.1 Kaedah Pengambilan Maklumat	
	Paket Rangkaian	54
	2.17.2.2 Bilangan Maklumat Paket	
	Rangkaian	55
	2.17.2.3 Penggunaan Pendekatan	
	Penghasilan Identiti Unik	55
	2.17.2.4 Perbincangan	56
	2.17.3 Perbandingan Identiti Unik	56
	2.17.3.1 Penggunaan Formula	57
	2.17.3.2 Penggunaan Saiz Tetingkap	57
	2.17.3.3 Perbincangan	58
2.18	Peranan Penimbal Di dalam Mengoptimumkan	

Bahagian Penawanan Paket	58
2.18.1 Pengenalan Kepada Penawanan Paket WinPcap	58
2.18.2 Proses Penawanan Paket	59
2.19.3 Penimbal Kernel dan Penimbal Pengguna	59
2.19 Kaedah Pengambilan Maklumat Paket dan Bilangan Maklumat Paket Di dalam Mengoptimumkan Bahagian Pengenalpastian Identiti Unik	60
2.19.1 Paket Rangkaian	61
2.19.2 Pengambilan Maklumat Paket	61
2.19.3 Bilangan Maklumat Paket	62
2.20 Peranan Formula Di dalam Mengoptimumkan Bahagian Perbandingan Identiti Unik	63
2.20.1 Formula Mengikut Teknik Utama	63
2.21.1.1 <i>Thumbprint</i>	63
2.21.1.2 <i>OnOff</i>	63
2.21.1.3 <i>Deviation</i>	64
2.21.1.4 Min/Max Sum Ratio (MMS)	64
2.21.1.5 Normalized Dot Product 1 (NDP1)	64
2.21.1.6 Normalized Dot Product 2 (NDP2)	65
2.21.1.7 Statistical Correlation (STAT)	65
2.21.1.8 Perbincangan	66
2.20.2 Penggunaan Saiz Tetingkap Yang Kecil	66
2.21 Pengiraan Masa Pemprosesan Sebagai Penentu-ukur Pengoptimuman	66
2.22 Pengawalan Nilai Pengoptimuman	67
2.22.1 Peratus Kejayaan Pembacaan Data	67
2.23.2 Ketepatan	68
2.23.3 Keberkesanan	68
2.23.4 Perbincangan	69
2.23 LAN Terasing dan Terancang Sebagai Medium Pengujian	69

2.24	Set Data Terancang dan Berbeza Sumber Input Pengujian	70
2.25	Kesimpulan	71
3	KERANGKA KERJA PENYELIDIKAN	
3.1	Pengenalan	73
3.2	Kerangka kerja Penyelidikan	73
3.3	Metodologi Penyelidikan	78
	3.3.1 Metodologi Atas-Bawah	78
3.4	Kesimpulan	80
4	REKABENTUK	
4.1	Pengenalan	81
4.2	Pemecahan Unit Algoritma Pengesanan Batu Loncatan	81
4.3	Rekabentuk Keseluruhan Penyelidikan	82
	4.3.1 Rekabentuk Algoritma mengikut Pecahan	84
	4.3.2 Rekabentuk Data Input Pengujian mengikut Pecahan	84
	4.3.3 Rekabentuk Persekitaran Pengujian mengikut Pecahan	86
	4.3.4 Rekabentuk Output Pengujian Mengikut Pecahan	87
	4.3.5 Rekabentuk Penggabungan Keseluruhan Pecahan	88
	4.3.6 Rekabentuk Data Input Penggabungan Keseluruhan Pecahan	89
	4.3.7 Rekabentuk Persekitaran Penggabungan	

	Keseluruhan Pecahan	90
4.3.8	Rekabentuk Output Penggabungan	
	Keseluruhan Pecahan	90
4.4	Kesimpulan	91

5 IMPLEMENTASI

5.1	Pengenalan	92
5.2	Rekabentuk Kepada Implementasi	92
5.3	Implementasi Keseluruhan Penyelidikan	93
5.3.1	Implementasi Algoritma Mengikut Pecahan	94
5.3.2	Implementasi Data Input Pengujian Mengikut Pecahan	96
5.3.3	Implementasi Persekitaran Pengujian Mengikut Pecahan	97
5.3.3.1	Implementasi Persekitaran Sumber Pengujian	97
5.3.3.2	Implementasi Persekitaran Bahan Pengujian	98
5.3.4	Implementasi Output Pengujian Mengikut Pecahan	99
5.3.5	Implementasi Hasil Mengikut Pecahan	100
5.3.6	Implementasi Penggabungan Keseluruhan Pecahan	101
5.3.7	Implementasi Data Input Penggabungan Keseluruhan Pecahan	101
5.3.7.1	Implementasi Data Input Sumber Penggabungan Keseluruhan Pecahan	102

5.3.7.1	Implementasi Data Input Bahan	
	Pengujian Penggabungan Keseluruhan	
	Pecahan	103
5.3.8	Implementasi Persekitaran Penggabungan	
	Keseluruhan Pecahan	103
	5.3.8.1 Implementasi Persekitaran	
	Sumber Penggabungan	104
	5.3.8.2 Implementasi Persekitaran	
	Bahan Penggabungan	104
5.3.9	Implementasi Output Penggabungan	
	Keseluruhan Pecahan	104
5.3.10	Implementasi Hasil Pengujian	
	Keseluruhan Pecahan	105
5.4	Kesimpulan	105

6

PENGUJIAN

6.1	Pengenalan	107
6.2	Implementasi Kepada Pengujian	108
6.3	Pengujian Keseluruhan Penyelidikan	108
6.4	Pengujian Mengikut Pecahan	109
	6.4.1 Penawanan Paket	110
	6.4.1.1 Input	110
	6.4.1.2 Persekitaran	111
	6.4.1.3 Output	111
	6.4.1.4 Hasil	112
	6.4.2 Pengenalpastian Identiti	112
	6.4.2.1 Input	112
	6.4.2.2 Persekitaran	113
	6.4.2.3 Output	113
	6.4.2.4 Hasil	113
	6.4.3 Perbandingan Identiti	114

	6.4.3.1 Input	114
	6.4.3.2 Persekitaran	115
	6.4.3.3 Output	115
	6.4.3.4 Hasil	115
6.5	Pengujian Penggabungan Pecahan	116
	6.5.1 Input	116
	6.5.2 Persekitaran	117
	6.5.3 Output	117
	6.5.4 Hasil	118
6.6	Kesimpulan	118
7	HASIL, ANALISA DAN KEPUTUSAN	
7.1	Pengenalan	119
7.2	Hasil, Analisa dan Keputusan Keseluruhan Penyelidikan	120
7.3	Hasil, Analisa dan Keputusan Mengikut Pecahan	122
	7.3.1 Penawanan Paket	122
	7.3.1.1 Analisa dan Keputusan	123
	7.3.2 Pengenalpastian Identiti	125
	7.3.2.1 Analisa dan Keputusan	125
	7.3.3 Perbandingan Identiti	127
	7.3.3.1 Analisa dan Keputusan	128
7.4	Hasil, Analisa dan Keputusan Penggabungan Pecahan	129
	7.4.1 Penawanan Paket	129
	7.4.1.1 Analisa dan Keputusan	130
	7.4.2 Pengenalpastian Identiti	132
	7.4.2.1 Analisa dan Keputusan	133
	7.4.3 Perbandingan Identiti	136
	7.4.3.1 Analisa dan Keputusan	136

7.5	Kesimpulan	138
8	KESIMPULAN	
8.1	Pengenalan	140
8.2	Objektif Penyelidikan dan Kesimpulan	140
8.3	Sumbangan Penyelidikan	144
8.4	Limitasi Penyelidikan	145
8.5	Cadangan Masa Hadapan	146
8.6	Kesimpulan	147
	RUJUKAN	150
	BIBLIOGRAFI	156
	Lampiran B1 – G1	226
	PENERBITAN	227

SENARAI JADUAL

NO. JADUAL	TAJUK	MUKA SURAT
2.1	Klasifikasi pendekatan penjejakan	35
2.2	Pemecahan algoritma berdasarkan kepada bahagian-bahagian utama algoritma	49
3.1	Penerangan kerangka kerja penyelidikan	76
5.1	Rekabentuk dan kaedah implementasi	93
7.1	Analisa masa pemprosesan penawanan paket menggunakan penimbal kernel bersaiz 4, 64 dan 1024 MB dan penimbal pengguna 4, 64 dan 1024 MB	123
7.2	Analisa masa pemprosesan penawanan paket menggunakan penimbal kernel bersaiz 4, 64 dan 1024 MB dan penimbal pengguna 4, 64 dan 1024 MB	124
7.3	Masa minimum, maksimum dan purata masa pelaksanaan pendekatan bahagian pengenalpastian identiti	126
7.4	Masa purata, peratus perbandingan dan masa maksimum bahagian perbandingan	128
7.5	Analisa pengujian penawanan paket bagi penggabungan pecahan menggunakan data kecil	131
7.6	Analisa pengujian penawanan paket bagi penggabungan pecahan menggunakan data besar	131
7.7	Analisa pengujian pengenalpastian identiti bagi penggabungan pecahan menggunakan data kecil	134
7.8	Analisa pengujian pengenalpastian identiti bagi penggabungan pecahan menggunakan data besar	134

7.9	Analisa sebahagian perbandingan identiti	137
-----	--	-----

SENARAI RAJAH

NO. RAJAH	TAJUK	MUKA SURAT
21	Masalah jurang masa <i>a</i>)sebelum pengoptimuman dan <i>b</i>)selepas pengoptimuman	18
22	Klasifikasi pendekatan IRS	25
23	Keseluruhan teknologi penjeakan	28
24	Teknologi penjeakan pencerobohan	29
25	Penandaan paket	0
26	<i>Hop-by-hop</i>	3
27	Komponen penjeakan sambungan	3
28	Penjeakan berasaskan-rangkaian	4
29	Terminologi dan notifikasi	3
210	Pendekatan penjeakan pencerobohan berasaskan rangkaian (<i>Thumbprint</i>)	9
211	Pendekatan penjeakan pencerobohan berasaskan rangkaian (<i>ONOFF</i>)	0
212	Pendekatan penjeakan pencerobohan berasaskan rangkaian (<i>Deviation</i>)	4
213	Bagian kepala dan data paket rangkaian	4
3	Kerangka kerja penyelidikan	5
3	Metodologi Atas-Bawah	9
4	Rekabentuk keseluruhan penyelidikan	8
5	Implementasi keseluruhan penyelidikan	9

6	Pengujian keseluruhan penyelidikan	10
7	Hasil, analisa dan keputusan keseluruhan Penyelidikan	121

SENARAI SIMBOL

C	-	Identiti Unik Sambungan
j	-	Nilai Awalan
k	-	Penambahan Nilai Awalan
kbps	-	Kilo Bait Per Saat
<i>log</i>	-	Logaritma
ms	-	Milisaat
mak	-	Maksimum
Mhz	-	Megahertz
MB	-	Mega Bait
Min	-	Minimum
OFF ₁	-	Tempoh OFF Paket
t	-	Masa
<i>T_g</i>	-	Jurang Masa
<i>T_d</i>	-	Masa Mula Pengesanan
<i>T_r</i>	-	Jumlah Masa Untuk Penindakbalasan
<i>p</i>	-	Fungsi
s	-	Saat
s	-	Saiz Tetingkap
X	-	Nilai Identiti Unik Pertama
y	-	Parameter Kawalan

Y	-	Nilai Identiti Unik Kedua
Π	-	Pai
δ_t	-	Perbezaan
T_k	-	<i>Thumbprint</i>
Σ	-	Jumlah

SENARAI SINGKATAN

API	Application Programming Interface
CERT	Computer Emergency Response Team
CIS	Caller Identification System
CITRA	Cooperative Intrusion Trace back and Response Architecture
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DOS	Denial of Service
DIDS	Distributed Intrusion Detection System
IDS	Intrusion Detection System
IRS	Intrusion Response System
IPD	Inter-Packet Delay
IPSec	IP Security
IDIP	Intrusion Identification and Isolating Protocol
LAN	Local Area Network
MMS	Min/Max Sum Ratio
NIT	National Institute of Technology
NDP 1	Normalized Dot Product 1
NDP 2	Normalized Dot Product 2

NIDS	Network Intrusion Detection System
NIC	Network Interface Card
NLANR	National Laboratory for Applied Network Research
PC	Personal Computer
SSD	Stepping Stone Detection
SA	Security Association
SWT	Sleepy Watermark Tracing
STAT	Statistical Correlation
TCP	Transmission Control Protocol
WAN	Wide Area Network

SENARAI ISTILAH

<i>Adapter</i>	Adapter
<i>Adaptive</i>	Adaptasi
<i>Anomaly</i>	Kejanggalkan
<i>Attack</i>	Serangan
<i>Attacker Filtering</i>	Penapisan Pencerobohan
<i>Audit log</i>	Log audit
<i>Automatic response</i>	Penindakbalasan automatik
<i>Backbone Internet</i>	Tulang belakang Internet
<i>Bidirectional</i>	Dua arah
<i>Brute-force</i>	Cuba-jaya
<i>Circular</i>	Berputar
<i>Connection</i>	Sambungan
<i>Connection Chain</i>	Rangkaian Sambungan
<i>Dot product</i>	Produk Dot
<i>Downstream</i>	Aliran Ke Bawah
<i>Encryption</i>	Penyulitan
<i>Enhanced Notification</i>	Peningkatan Notifikasi
<i>False positive</i>	Salah positif
<i>False negative</i>	Salah negatif
<i>Filter</i>	Penapis
<i>Firewall</i>	Dinding Api

<i>Flood</i>	Limpahan
<i>Header</i>	Kepala
<i>Heterogeneous</i>	Pelbagai
<i>High-level</i>	Aras-tinggi
<i>Host-based</i>	Berasaskan-hos
<i>Network-based</i>	Berasaskan-rangkaian
<i>Hop</i>	Hop
<i>Hop-by-hop</i>	Hop demi hop
<i>Inbound</i>	Sempadan dalam
<i>Intrusion Response</i>	Penindakbalasan Pencerobohan
<i>Kernel Buffer</i>	Penimbal Kernel
<i>Kernel-managed</i>	Selenggaraan-kernel
<i>Manual response</i>	Penindakbalasan manual
<i>Misuse</i>	Penyalahgunaan
<i>Network Analyzer</i>	Penganalisa Rangkaian
<i>Network Tap</i>	Tap rangkaian
<i>Multivariate Statistics</i>	Statistik Perlbagaivariati
<i>Notification</i>	Notifikasi
<i>Only-seen-twice</i>	Hanya dilihat-dua-kali
<i>Optimize</i>	Optimum
<i>Outbound</i>	Sempadan luar
<i>Overlay network</i>	Rangkaian
<i>Packet</i>	Paket
<i>Packet Marking</i>	Penandaan Paket
<i>Packet Stream</i>	Aliran paket

<i>Payload</i>	Muatan
<i>Port</i>	Pot
<i>Principal component analysis</i>	Analisis Komponen Asas
<i>Tracing</i>	Penjejakan
<i>Real-time</i>	Masa nyata
<i>Remote Login</i>	Login jauh
<i>Router</i>	Penghala
<i>Scalable</i>	Mudah alih
<i>Stepping stone</i>	Batu loncatan
<i>Signature</i>	Tandatangan
<i>Specification-based</i>	Berasaskan-spesifikasi
<i>System Administrator</i>	Pentadbir Sistem
<i>System call</i>	Panggilan sytem
<i>Taxonomy</i>	Taxonomi
<i>Tails</i>	Ekor
<i>Time gap</i>	Jurang Masa
<i>Timing-based</i>	Berasaskan-masa
<i>Trust model</i>	Model kepercayaan
<i>Unidirectional</i>	Satu arah
<i>Upstream</i>	Aliran Ke Atas
<i>User-level</i>	Aras-pengguna
<i>User Buffer</i>	Penimbal Pengguna
<i>Window</i>	Tetingkap

SENARAI LAMPIRAN

LAMPIRAN	TAJUK	MUKA SURAT
B1	Senibina WinPcap	158
D1	Rekabentuk Algoritma Pengesanan Batu Loncatan Mengikut Pecahan	159
D2	Rekabentuk Persekitaran	166
D3	Rekabentuk Persekitaran Penggabungan Keseluruhan	167
E1	Implementasi Algoritma Bahagian Penawanan Paket	168
E2	Implementasi Algoritma Bahagian Pengenalpastian Identiti	169
E3	Implementasi Algoritma Bahagian Perbandingan Identiti	170
E4	Implementasi Data Input Pengujian - Penawanan Paket	172
E5	Implementasi Data Input Pengujian - Pengenalpastian Identiti	173
E6	Implementasi Data Input Pengujian - Perbandingan Identiti	174
E7	Implementasi Persekitaran Sumber Pengujian - Bahagian Penawanan Paket	175
E8	Implementasi Persekitaran Sumber Pengujian - Bahagian Pengenalpastian Identiti	176
E9	Implementasi Persekitaran Sumber Pengujian - Bahagian Perbandingan Identiti	177
E10	Implementasi Persekitaran Bahan Pengujian - Bahagian Penawanan Paket	178

E11	Implementasi Persekitaran Bahan Pengujian - Bagian Pengenalpastian Identiti	179
E12	Implementasi Persekitaran Bahan Pengujian - Bagian Perbandingan Identiti	180
E13	Implementasi Output Pengujian - Bagian Penawanan Paket	181
E14	Implementasi Output Pengujian - Bagian Pengenalpastian Identiti	183
E15	Implementasi Output Pengujian - Bagian Perbandingan Identiti	184
E16	Implementasi Hasil Pengujian - Bagian Penawanan Paket	185
E17	Implementasi Hasil Pengujian - Bagian Pengenalpastian Identiti	185
E18	Implementasi Hasil Pengujian - Bagian Perbandingan Identiti	185
E19	Implementasi Algoritma Pengesanan Batu Loncatan	186
E20	Penggabungan Keseluruhan Pecahan	187
E21	Implementasi Data Input	188
E22	Implementasi Persekitaran Sumber Pengujian Penggabungan	189
E23	Implementasi Persekitaran Bahan Pengujian Penggabungan	190
E24	Implementasi Output Penggabungan	191
F1	Input Penawanan Paket	194
F2	Contoh Input Penawanan Paket	195
F3	Output Contoh Oleh Aplikasi Penawanan Paket Rangkaian Testapp	196
F4	Input Pengenalpastian Identiti	197
F5	Contoh Input Bahagian Pengenalpastian Identiti	198
F6	Contoh Output Bahagian Pengenalpastian Identiti	199

F7	Output Analisa Pengujian Penggabungan - Pengenalpastian Identiti	201
F9	Output Analisa Pengujian Penggabungan - Perbandingan Identiti	202
F10	Output Terakhir Algoritma Pengesanan Batu Loncatan	203
G1	Hasil Pengujian Pecahan Penawanan Paket Menggunakan Data Input 10kbps	204
G2	Hasil Pengujian Pecahan Penawanan Paket Menggunakan Data Input 10000kbps	205
G3	Hasil Pengujian Pecahan Pengenalpastian Identiti	206
G4	Hasil Pengujian Bahagian Perbandingan Identiti Menggunakan Data Rawak Kecil	207
G5	Hasil Pengujian Bahagian Perbandingan Identiti Menggunakan Data Rawak Besar	208
G6	Hasil Penawanan Paket Penggabungan Menggunakan Data Input Kecil	209
G7	Hasil Penawanan Paket Penggabungan Menggunakan Data Input Besar	210
G8	Hasil Pengenalpastian Identiti Penggabungan Menggunakan Data Input Kecil	211
G9	Hasil Pengujian Pengenalpastian Identiti Penggabungan Pecahan (Data Besar)	214
G10	Analisa Pengenalpastian Identiti Penggabungan Pecahan Menggunakan Data Input Kecil	217
G11	Analisa Pengenalpastian Identiti Penggabungan Pecahan Menggunakan Data Input Besar	218
G12	Sebahagian Hasil Perbandingan Identiti Penggabungan Pecahan 219	
G13	Analisa Perbandingan Identiti Penggabungan Pecahan	221

BAB 1

PENGENALAN

1.1 Pengenalan

Kini, serangan siber menjadi semakin rumit. Laporan tahunan daripada Computer Emergency Response Team (CERT) menerangkan pertambahan bilangan insiden keselamatan komputer setiap tahun (CERT, 2002). Sistem Pengesanan Pencerobohan (IDS) disenaraikan sebagai salah satu daripada teknologi untuk menghalang serangan terhadap rangkaian selain daripada dinding api (*firewall*) dan Identifikasi sumber pencerobohan (*intrusion source identification*) (Ferguson *et al.*, 1998). IDS boleh ditakrifkan sebagai sistem yang mencuba untuk mengidentifikasikan penggunaan yang tidak dibenarkan, keganjilan dan penyalahgunaan sistem komputer (Puketza *et al.*, 1996). Sistem Penindakbalasan Pencerobohan (IRS) pula menyediakan mekanisme penindakbalasan kepada IDS. Namun demikian, kebanyakan IRS bertindak balas terhadap serangan dengan hanya melalui penjanaan laporan atau amaran (Carver, 2001). Penyelidikan oleh (Cohen, 1999) mendapati bahawa kejayaan satu-satu serangan itu adalah bergantung kepada jurang masa (*time gap*) di antara pengesanan dan penindakbalasan. Secara ringkasnya, sekiranya penceroboh diberi masa tiga puluh jam, penceroboh telah berjaya sepenuhnya mencerooboh.

Masalah jurang masa wujud di antara IDS dan IRS. Ini bermakna masalah jurang masa boleh diselesaikan sama ada menerusi IDS dan IRS. Untuk menyelesaikan masalah jurang masa ini, penyelidikan yang telah dilaksanakan oleh (Carver, 2000) yang memfokuskan kepada adaptasi (*adaptive*) IDS telah menumpukan ke arah usaha untuk menghasilkan IDS yang boleh diadaptasikan.

Melalui penyelidikan ini, sekiranya IDS berada di dalam keadaan sentiasa terkemas kini dan dapat pengesanan segala jenis pencerobohan, ini seterusnya akan dapat memastikan pengesanan dapat dilakukan dengan cepat. Sekiranya pengesanan dapat dilakukan dengan cepat, maka masalah jurang masa dapat diselesaikan. Walau bagaimanapun, pengesanan semata-mata tanpa tindak balas sewajarnya adalah tidak berfaedah. Apa yang diperlukan di sini adalah unsur tindak balas yang diakui oleh (Carver, 2001) adalah lebih penting dari IDS. Oleh yang demikian, untuk penyelidikan ini, pengurangan jurang masa menerusi IRS atau penindakbalasan dilaksanakan. Selain daripada IRS dilihat lebih penting daripada IDS, pengurangan jurang masa ke atas IRS dilihat akan memperlengkapkan lagi keseluruhan penyelidikan pengurangan jurang masa yang melibatkan IDS dan IRS.

Dengan ini, dapatlah diringkaskan bahawa penyelidikan ini akan menumpukan usaha untuk mengurangkan jurang masa di antara pengesanan dan penindakbalasan dengan memfokuskan penyelidikan ke arah penindakbalasan atau IRS.

Bagi memastikan usaha ke arah pengurangan jurang masa menerusi penindakbalasan berjaya dilaksanakan, salah satu teknik penindakbalasan telah dipilih. Ini adalah berdasarkan kepada kebaikan yang ada kepada teknik penjejakan berbanding dengan teknik-teknik penindakbalasan yang telah di senaraikan oleh (Carver, 2001). Secara umumnya, kaedah penindakbalasan penjejakan menawarkan penindakbalasan seterusnya setelah punca pencerobohan diketahui. Penjejakan pencerobohan diperlukan sebagai keperluan untuk membangunkan penindakbalasan segera (Dong-li, 2002).

Teknologi penjejakan boleh dibahagikan kepada dua kategori utama, Penjejakan IP dan Penjejakan Sambungan (Buchholz, 2002). Fokus akan diberikan ke arah Penjejakan Sambungan berikutan oleh penjejakan IP memerlukan penglibatan komponen perkakasan (selalunya penghala) (Tatsuya dan Shigeyuki, 2002) sebagai komponen utama dan ini adalah tidak bersesuaian dengan persekitaran penyelidikan yang akan dilakukan dan merupakan salah satu kekangan terhadap penyelidikan ini.

Daripada tinjauan ke atas teknik-teknik penjejakan sambungan (Snap, 1991), (Staniford-Chen dan Heberlein, 1995), (Zhang dan Paxon, 2000), (Yoda dan Etoh, 2000) dan (Schnackenberg dan Djahandari, 2000), teknik penjejakan berasaskan-rangkaian (*network-based tracing*) merupakan teknik yang menjadi pilihan penyelidikan berbanding dengan teknik penjejakan berasaskan-hos (*host-based*) dan penjejakan pasif lebih digunakan berbanding dengan pendekatan aktif (Wang *et al.*, 2001). Sehingga ke saat ini, penyelidikan penjejakan sambungan seperti (Yung, 2002) dan (Dohono *et al.*, 2002) masih tertumpu kepada teknik penjejakan sambungan berasaskan-rangkaian.

Keseluruhan teknik penjejakan sambungan berasaskan-rangkaian cuba untuk menyelesaikan masalah yang dikenali sebagai pengesanan batu loncatan. Batu loncatan merupakan kaedah yang digunakan oleh penceroboh untuk melindungi jejak pencerobohnya dengan cara mempergunakan hos atau perantara sebelum melakukan pencerobohan yang sebenar (Zhang dan Paxon, 2000). Ini dapat dilihat menerusi penyelidikan yang telah dilakukan oleh penyelidik-penyelidik seperti (Snap, 1991), (Staniford-Chen dan Heberlein, 1995), (Zhang dan Paxon, 2000), (Yoda dan Etoh, 2000) dan (Schnackenberg dan Djahandari, 2000). Di sebabkan oleh penyelidik-penyelidikan menunjukkan kepentingan kajian terhadap pengesanan batu loncatan, algoritma pengesanan batu loncatan ini diselidiki dengan mendalam. Hasil daripada penyelidikan terhadap algoritma ini kemudiannya dioptimumkan ke arah untuk menghasilkan algoritma pengesanan batu loncatan yang dapat mengesan batu loncatan dengan lebih pantas.

Oleh yang demikian, keseluruhan penyelidikan ini akan bertumpu kepada pengurangan jurang masa penindakbalasan dengan mengoptimumkan algoritma pengesanan batu loncatan.

1.2 Latar Belakang

Penyelidikan yang dilakukan oleh (Cohen, 1999) mendapati bahawa kejayaan sesuatu serangan itu bergantung kepada jurang masa di antara pengesanan dan penindakbalasan.

Daripada tinjauan yang telah dilakukan oleh (Carver, 2001) menerangkan IDS semasa mempunyai mekanisme yang terhad berbanding dengan ancaman semasa. Penindakbalasan masih lagi menggunakan proses manual dan ini dibuktikan akan menghasilkan jurang masa yang besar di antara pengesanan dan penindakbalasan (Cohen, 1999).

Walaupun penyelesaian terhadap permasalahan ini telah pun diselidiki oleh (Carver, 2001) melalui pendekatan pengesanan, namun demikian penyelidikan yang dilakukan di dalam tesis memilih untuk menyelesaikan masalah ini menerusi pendekatan penindakbalasan. Ini adalah disebabkan oleh pendekatan penindakbalasan dilihat lebih baik daripada penyelesaian sebelumnya (pendekatan pengesanan). Penyelidikan difokuskan ke arah teknik penjejakan pencerobohan yang disenaraikan oleh (Carver, 2002) sebagai salah satu teknik penindakbalasan yang perlu diambil perhatian.

Teknik penjejakan yang di dalamnya terkandung pelbagai teknik diselidiki yang hasil daripada penyelidikan yang dilakukan mendapati bahawa teknik penjejakan berasaskan rangkaian adalah lebih sesuai untuk dikaji selanjutnya. Ini adalah berdasarkan penyelidikan seperti (Staniford-Chen dan Heberlein, 1995) (Zhang dan Paxon, 2000) dan (Yoda dan Etoh, 2000) serta beberapa penyelidikan terbaru seperti (Dohono *et al.*, 2002) dan (Wang *et al.*, 2002) yang masih menumpukan usaha ke arah menyediakan teknik penjejakan yang lebih berkesan.

Keseluruhan teknik penjejakan berasaskan rangkaian ini memfokuskan kepada masalah untuk menyelesaikan masalah yang dikenali sebagai pengesanan batu loncatan. Algoritma untuk menyelesaikan masalah batu loncatan ini dikaji dan penyelidikan untuk mengoptimumpkannya ke arah untuk menghasilkan satu algoritma yang lebih baik dijalankan.

1.3 Pernyataan Masalah

“Adakah dengan mengoptimumpkan algoritma pengesanan batu loncatan dapat mengurangkan jurang masa di antara pengesanan dan penindakbalasan”

Masalah pengesanan batu loncatan difokuskan dan dinyatakan seperti berikut

Sambungan c_i adalah sambungan tunggal daripada hos komputer H_i (sumber) kepada H_{i+1} (destinasi). Pengguna mungkin log melalui jujukan hos-hos komputer $H_1, H_2, H_3, \dots, H_{n+1}$ melalui Rangkaian Sambungan $c_1, c_2, c_3, \dots, c_{n-1}$ di mana sambungan c_i adalah login jauh (*remote login*) daripada hos H_i hingga ke hos H_{i+1} .

Sekiranya diberi sambungan c_n ,

“Bagaimanakah kaedah untuk menawan, mengenal pasti dan membandingkan sambungan-sambungan lain $c_1, c_2, c_3, \dots, c_{n-1}$ di dalam rangkaian, dan sambungan manakah yang terlibat”

“Bagaimanakah pengoptimuman dapat dilakukan untuk menjadikan algoritma pendekatan pengesanan batu loncatan dapat dilakukan dengan lebih pantas”

“Bagaimanakah menentu-ukur masa yang digunakan untuk penjejakan pencerobohan sama ada masa sebelum pengoptimuman dan selepas pengoptimuman”

1.4 Tujuan

Tujuan utama penyelidikan ini adalah untuk pengoptimuman keseluruhan penindakbalasan (IRS) dengan cara mengoptimumkan algoritma pengesanan batu loncatan bagi mengurangkan jurang masa di antara pengesanan dan penindakbalasan (IDS).

1.5 Objektif

Berikut disenaraikan objektif untuk penyelidikan ini.

- i. Untuk menyelidik pendekatan mengurangkan jurang masa penindakbalasan (IRS) dengan memfokuskan kepada pendekatan pengesanan batu loncatan.
- ii. Untuk mengoptimumkan algoritma pengesanan batu loncatan.
- iii. Untuk membandingkan algoritma pengesanan batu loncatan sedia ada dan algoritma yang telah dioptimumkan.

1.6 Skop

Berikut disenaraikan pula skop untuk penyelidikan ini.

- i. Penyelidikan ini hanya terhad kepada pengoptimuman pendekatan penindakbalasan (atau lebih tepat lagi algoritma pengesanan batu loncatan) untuk menghasilkan satu pendekatan yang lebih optimum.
- ii. Pengoptimuman algoritma pengesanan batu loncatan hanya melibatkan pengesanan di dalam satu-satu segmen Kawasan Rangkaian Setempat (LAN) yang memungkinkan pencerapan paket rangkaian dilakukan hanya melalui satu titik segmen itu sahaja.
- iii. Data yang digunakan di dalam algoritma pengesanan batu loncatan hanyalah tertumpu pada paket TCP (atau lebih tepat lagi paket TELNET).
- iv. Data yang digunakan adalah hasil daripada penjanaan skrip TELNET (Telnet Scripting Tools v1.0) menggunakan prasarana rangkaian sebenar. Ini adalah bagi memastikan data adalah sama dengan data sebenar rangkaian dan tetap untuk setiap pengujian yang dilakukan.
- v. Pencerapan data masa dalam menentu-ukur algoritma sama ada optimum atau tidak bergantung kepada fungsi (*System.millisecond()*) dalaman bahasa pengaturcaraan java versi 1.4.1_04 (Java versi 2).

1.7 Andaian

Berikut adalah andaian yang telah diberikan untuk penyelidikan ini

- i. Pengesanan batu loncatan terhad untuk mengenal pasti hos yang merupakan sumber kepada serangan. Pengenalpastian dan penentusahan pengguna sebenar hos adalah di luar bidang pengesanan. Pengesanan batu loncatan adalah terhad kepada penjejakan hos yang digunakan sahaja.
- ii. Persekitaran LAN yang digunakan membolehkan pencerapan maklumat keseluruhan paket rangkaian dilakukan hanya pada satu titik di dalam rangkaian tersebut.

1.8 Kepentingan Kajian

Penyelidikan pengoptimuman algoritma pengesanan batu loncatan di dalam pendekatan penindakbalasan dilakukan bagi mengurangkan masa jurang masa penindakbalasan (IRS). Kejayaan mengurangkan jurang masa penindakbalasan bukan sahaja berjaya menyelesaikan sebahagian masalah jurang masa, namun berjaya juga melengkapkan pasangan penyelidikan sebelum ini yang mengurangkan jurang masa melalui pengesanan (IDS). Kejayaan mengurangkan jurang masa ini dilihat berfaedah dari segi untuk mengurangkan kadar peratusan pencerobohan selepas pengesanan oleh IDS. Penyelidikan ini dilihat berpotensi untuk diterapkan di dalam IDS sedia ada yang hanya berkeupayaan untuk mengesan pencerobohan sahaja. Pihak yang bertanggungjawab seperti Pentadbir Sistem atau Rangkaian kini boleh memastikan pencerobohan rangkaian tidak hanya dikesan tetapi diketahui sumbernya dan diberi penindakbalasan dengan lebih cepat dan efisien.

1.9 Hasil Jangkaan

Hasil jangkaan penyelidikan ini adalah berupa algoritma pengesanan batu loncatan yang lebih optimum berbanding dengan algoritma-algoritma pengesanan batu loncatan sedia ada. Melalui pengoptimuman algoritma ini, apabila digunakan sebagai komponen di dalam penindakbalasan (IRS), akan mewujudkan penindakbalasan yang lebih baik dan ini seterusnya akan mencapai matlamat mengurangkan jurang masa di antara pengesanan dan penindakbalasan secara umumnya dan mengurangkan jurang masa penindakbalasan secara khususnya.

1.11 Organisasi Tesis

Penyelidikan ini membincangkan pengurangan jurang masa penindakbalasan melalui pengoptimuman algoritma pengesanan batu loncatan. Bab 1 memberikan pengenalan, latar belakang, pernyataan masalah, tujuan, objektif, kepentingan kajian, skop, andaian dan hasil jangkaan keseluruhan penyelidikan ini. Bab 2 pula menghuraikan kajian latar belakang yang telah dilakukan sepanjang tempoh penyelidikan dilakukan. Bab 3 menerangkan kerangka kerja Penyelidikan. Bab 4 membincangkan rekabentuk yang dilakukan di dalam penyelidikan ini. Bab 5 pula menerangkan implementasi yang dilakukan. Bab 6 membincangkan pengujian yang dilakukan di dalam penyelidikan ini. Bab 7 memberikan hasil, analisa dan keputusan yang diperolehi daripada sesi pengujian yang dijalankan. Bab 8 menutup penyelidikan ini dengan membincangkan perihal sejauh mana penyelidikan ini mencapai objektifnya, sumbangan penyelidikan, kekurangan dan diakhiri dengan cadangan masa hadapan yang boleh dilakukan.

RUJUKAN

- Adam, J., A. (1992). Data security-cryptography=privacy?. *Spectrum IEEE*. 29(8): 29-35.
- Arbaugh, W., A. (2003). Firewall an outdated defence. *Computer*. 36(6): 112-113.
- Baba, T., dan Matsuda., S. (2002). Tracing Network Attacks to Their Sources. *IEEE Internet Computing*. 6(2): 20-26.
- Burroughs, D., J., Wilson, L., F., dan Cybenko, G., V. (2002) Analysis of Distributed Intrusion Detection Systems Using Bayesian Methods. *21st IEEE International Performance, Computing, and Communications Conference*. April 3-5. Phoenix, Arizona: IEEE, 329 - 334.
- Calvert, K., L., Bhattacharjee, S., Zegura, E., dan Sterbenz, J. (1998). Direction in Active Networks. *IEEE Communication Magazine*. 36(10): 72-78.
- Carver., A., C., Jr., Humphries., J., W., Pooch., U., W., dan Ragsdale., D., J. (2000). Adaptation Techniques for Intrusion Detection and Intrusion Response Systems. *IEEE International Conference on Systems, Man, and Cybernetics* .October 8-11. Nashville, TN: IEEE, 2344-2349.
- Carver., A., C. (2000). A Methodology for Using Intelligent Agents to provide Automated Intrusion Response. *Proceedings of the 2000 IEEE Workshop on Information Assurance and Security*. June 6-7. United State Military Academy, West Point, NY: IEEE, 110-116.
- Carver, C., A. dan Pooch U., W. (2000) An Intrusion Response Taxonomy and its Role in Automatic Intrusion Response. *Proceedings of the 2000 IEEE Workshop on Information Assurance and Security*. Jun 6-7. United States Military Academy, West Point, New York: IEEE, 110-116.
- Carver., A., C. (2001). Limiting Uncertainty in Intrusion Response. *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*. June 5-6. United State Military Academy, West Point, NY: IEEE, 142-147.

- Carver., C., A. (2002). Intrusion Response Systems: A Survey. Department of Computer Science, Texas A&M University, College Station, USA, TX77843-3112.
- CERT, (1999). Result of the Distributed System Intruder Tools Workshop. Software Engineering Institute, Carnegie Mellon University. unpublished.
- Cho, S. (2002). Incorporating Soft Computing Techniques Into a Probabilistic Intrusion Detection System. *IEEE Transactions On Systems, Man, and Cybernetics – Part C: Application and Reviews*. 32(2): 154-160.
- Chang., H., Y., Narayan., R., Vetter., B., Wu., S., F., Brown., M., Wang., X., Yuill., J., Sargor., C., Gong., F., Jou., F. (1999). DecIdUouS: Decentralized Source Identification for Network-Based Intrusion. *In Proceeding of the 6th IFIP/IEEE International Symposium on Integrated Network Management*. May 24-28. Boston, Mass., USA: IFIP/IEEE, 701-714.
- Cohen., F. (1999). *Simulating Cyber Attacks, Defenses, and Consequences*. Fred Cohen & Associates, Feature Article.
- Cunningham, R., K., Lippmann, R., P., dan Webster, S., E. (2001). Detecting and Displaying Novel Computer Attacks with Macroscope. *IEEE Transaction On Systems, Man, and Cybernetics – Part A: Systems And Humans*, 31(4): 275-281.
- Degionni, L. (2000). *Development of an Architecture for Packet Capture and Network Traffic Analysis*. Politecnico Di Torino: Tesis Ph.D.
- Degioanni, L., Baldi, M., Risso, F., dan Varenni, G. (2003) Profiling and Optimization of Software-Based Network-Analysis Applications. *Proceeding of the 15th Symposium on Computer Architecture and High Performance Computing*. November 10-12. Sao Paulo, Brazil: IEEE, 226-234.
- Dohono., D., L., Flesia., A., G., Shankar., U., Paxson., V., Coit., J., Staniford., S. (2002). Multiscale Stepping-Stone Detection: Detecting Pairs of Jittered Interactive Streams by Exploiting Maximum Tolerable Delay. *Fifth International Symposium of Recent Advance in Intrusion Detection*. October 16-18. Zurich, Switzerland: Springer, 1-15.
- Dong-li, S. (2002). *Trend & Technique of Intruder Traceback*. ITU-T Workshop on Security. May 13-14. Seoul, Korea: ERTI, 1-14.
- Eng, P., E., dan Haug, M. (2004). *Automatic Response to Intrusion Detection*, Agder University College: Tesis Masters.

- Forouzan., B., A. (2000). *Data Communication and Networking*. Education, North America: McGraw-Hill Higher
- Foundation, Inc. (2000). *Managed Security Service*. 2 Venture Street, Suite 100, Irvine, CA 92618.
- Fulvio, R. dan Loris D. (2001), An Architecture for High Performance Network Analysis, *Proceedings of the 6th IEEE Symposium on Computers and Communications*. July 3-5. Hammamet, Tunisia: IEEE, 686-693.
- Ferguson, P., dan Senie, D. (1998). *Network Ingress Filtering: Defeating Denial of Service Attack which employ IP Source Address Spoofing*. *Internet Engineering Task Force*, RFC 2267.
- Jang., H. dan Kim., S. (2000). A Self-Extension Monitoring for Security Management. *Computer Security Applications 16th Annual Conference 2000*. December 11-15. New Orleans, Louisiana: ACSAC, 196-203.
- Jason., W., P. (2000). *Mobile Agent Technology for Intrusion Detection and Response Systems*. Class Presentation, Department of Computer Science and Statistics University of Southern Mississippi. unpublished.
- Jensen., W., Karygiannis., T., Mell., P., Marks., D. (1999). Applying Mobile Agents to Intrusion Detection and Response. National Institute of Standards and Technology – A Computer Security Division. Technical Report.
- Kemmerer, R., A., dan Vigna, G. (2002) Intrusion Detection: A Brief History and Overview. *SECURITY & PRIVACY-2002*. 35(4): 27-30.
- Kent, S. (2000). On the trail of intrusions into information systems. *IEEE Spectrum*. 37(12): 52-56.
- Kulin, A. (2000). *A distributed security management system based on mobile agents*. Technical University of Vienna: Tesis Master.
- Leckie, T., dan Yasinsac, A. (2004). Metadata for Anomaly-Based Security Protocol Attack Deduction. *IEEE Transaction On Knowledge And Data Engineering*, 16(9): 1157-1167.
- Matsuda., S., Baba., T., Hayakawa., A., Nakamura., T. (2002). Design and Implementation of Unauthorized Access Tracing System. *Proceedings of the 2002 Symposium on Applications and the Internet*. January 28-February 1. Nara City, Japan: IEEE, 74-81.

- McCanne, S., dan Jacobson, V. (1992). The BSD Packet Filter: A New Architecture for User-level Packet Capture. *1993 Winter USENIX conference*. January 25-29. San Diego, CA: USENIX, 259-270.
- Mishra, A., Nadkarni, K., dan Patcha, A. (2004) Intrusion detection in wireless ad hoc networks, *IEEE Wireless Communication*. 11(1): 48-60.
- MuseMagic. (1999). MuseMagic Engineering, *An overview of optimization techniques*. United State of America, DSPworld.
- Ohta, K., Mansfield., G., Takei., Y., Nemoto., Y. (2000). Detection, defence, and tracing of Internet wide illegal access in distributed manner. *In Proceeding of INET 2000*. July 18-21. Yokohama, Japan: INET, 412-420.
- Park., K.dan Lee., H. (2000). *On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack*. Technical Report, Purdue University, CSD-TR 00-013.
- Paxson, V. (1999). Bro: A System for Detecting Network Intruders in Real-Time, *Computer Network*. 31(23-24): 2435-2463.
- Petkac, M., dan Badger, L. (2000). Security Agility in Response to Intrusion Detection. *16th Annual Computer Security Applications Conference* December 11-15. New Orleans, Louisiana: IEEE, 11-20.
- Puketza., N., J., Zhang., K., Chung., M., Mukherjee., B., dan Olsson., R., A. (1996), A Methodology for Testing Intrusion Detection Systems. *IEEE Transactions On Software Engineering*. 22(10): 719-729.
- Potlapally, N., R., Ravi, S., Raghunathan, A. (2002). Optimizing Public-Key Encryption for Wireless Clients. *IEEE International Conference on Communication*. April 28-May 2. Singapore: IEEE, 1050-1056.
- Rankin, A. dan Liber, S. (2004). *An Assessment of Autonomic Intrusion Detection Analysis and Response Methods in Strategic Network Defense*. unpublished.
- Schnackenberg, D., dan Djahandari, K. (2002). *Cooperative Intrusion Traceback and Response Architecture (CITRA)*. San Diego, California, #02-008.
- Schnackenberg, D., dan Djahandari, K. (2000). Infrastructure for Intrusion Detection and Response. *Proceeding of the DARPA Information Survivability Conference and Exposition 2000*. January 25-17. Hilton Head. S.C: IEEE, 1003-1011.

- Savege., S., Wetherall., D., Karlin., A., Aderson., T. (2000). Practical Network Support for IP Traceback. *In Proceeding of the 2000 ACM SIGCOMM Conference*. August 28-September 1. Stockholm, Sweeden: ACM, 295-306.
- Snap., S. (1991). DIDS (Distributed Intrusion Detection System) – Motivation, Architecture and Early Prototype. *In Proceeding of 14th National Computer Security Conference*. October 14. Washington, USA: ACM, 167-176.
- Song., D., X. dan Perrig., A. (2000). *Advance and Authenticated Marking Schemes for IP Traceback*. Technical Report, University of California at Berkeley, UCB/CSD-00-1107.
- Spatscheck, O., Hansen, J., S., Hartman, J., H. dan Peterson, L., L. (2000). Optimizing TCP Forwarder Performance, *IEEE/ACM Transaction On Networking*. 8(2): 146-157.
- Staniford-Chen., S. dan Heberlein., L., T. (1995). Holding Intruders Accountable on the Internet. *In Proceeding of IEEE Symposium on Security and Privacy*. May 8-10. Oakland, CA: IEEE, 39-49.
- Stone., R. (2000). CenterTrack: An IP Overlay Network for Tracking Dos Floods. *In Proceeding of the 9th USENIX Security Symposium*. August 14-17. Denver, Colorado: USENIX, 199-212.
- Tatsuya., B. dan Shigeyuki., M. (2002). Tracing Network Attacks to Their Source. *IEEE Internet Computing Journal*, 6(2): 20-26.
- Wang, X., Reeves, D., S., dan Wu, S., F. (2001). Tracing Based Active Intrusion Response. *Journal of Information Warefare*. 1(1): 50-61.
- Wang, X., Reeves, D., S., dan Wu, S., F. (2002). Inter-Packet Delay Based Correlation for Tracing Encrypted Connection Through Stepping Stones. *7th European Symposium on Research in Computer Security*. October 14-16. Zurich, Switzerland: Springer, 244-263.
- Watson, D., Smart, M., dan Jahanian, F. (2004). Protocol Scrubbling: Network Security Through Transparent Flow Modification. *IEEE/ACM Transaction On Networking*. 12(2): 261-273.
- Wu, Y., Foo, B., Matheny, B., Olsen, T., Bagchi, S. (2004). *ADEPTS: Adaptive Intrusion Containment and Response using Attack Graphs in an E-Commerce Environment*. School of Electrical & Computer Engineering, Purdue. No 2003-33.

- Yoda., K. dan Etoh., H. (2000). Finding a Connection Chain for Tracing Intruders. *6th European Symposium on Research in Computer Security*. October 4-6. Toulouse, France: CEPIS, 191-205.
- Yung., K., H. (2002). Detecting Long Connection Chains of Interactive Terminal Sessions. *Fifth International Symposium on Recent Advance in Intrusion Detection*. October 16-18. Zurich, Switzerland: Springer, 1-16.
- Zhang., Y. dan Paxon., V. (2000). Detecting Stepping Stones. *In Proceedings of 9th USENIX Security Symposium*. August 14-17. Denver, Colorado: USENIX, 171-184.

BIBLIOGRAFI

- Analyzer (2004). <http://analyzer.polito.it/>
- Burks.
(2004).<http://burks.brighton.ac.uk/burks/language/modula2/adps/ch2/ch23.htm>
- Bellovin., S., Leech., M., Taylor., T. (2001). *ICMP Traceback Message*. Internet draft, draft-ietf-itrace-02. unpublished.
- CERT. (2004), http://www.cert.org/stats/cert_stats.html
- Cerebro. (2004). <http://cerebro.cs.xu.edu/~smbelcas/howto.html>
- Darvinmag (2004).
<http://www.darvinmag.com/learn/curve/column.html?ArticleID=115>
- Digital Equipment Corporation (1992). *packetfilter(4)*. Ultrix V4.1 Manual.
- Ethereal. (2004). <http://www.ethereal.com/>
- Footfall. (2004). <http://footfall.csc.ncsu.edu>
- Flyzip. (2004) <http://www.fly-zip.com/page.php?m1=Technology&m2=Technology>
- Huang, X. (2000). *LIDS Hacking HOWTO. Document for LIDS*, v1.0.
- Information-technology Promotion Agency. (2004).
<http://www.ipa.go.jp/about/english/index.html>
- Libpcap. (2002). <http://sourceforge.net/projects/libpcap/>
- Netiq. (2002). <http://www.netiq.com/products/chr/default.asp>
- PCAUSA. (2000). <http://www.rawether.net>
- Snort. (2004). <http://www.snort.org>
- Sun Microsystem Inc. (1990). *SUN MICROSYSTEM INC. NIT(P4), SunOS, 4.1.1.1, Reference Manual*, Mountain View. CA, 800-5480.
- Tcpdump. (2004). <http://www.tcpdump.org/>
- Tfgen. (2004). <http://www.st.rim.or.jp/~yumo/pub/tfgen.html>
- Webopedia. (2004). <http://www.webopedia.com>
- Webster. (2004). <http://www.webster-dictionary.org/definition/algorithm>

Wikipedia. (2004a). <http://en.wikipedia.org/wiki/Algorithm>

Wikipedia. (2004b). [http://en.wikipedia.org/wiki/Optimization_\(computer_science\)](http://en.wikipedia.org/wiki/Optimization_(computer_science))

Windump. (2004). <http://windump.polito.it/>

WinPcap. (2004). <http://winpcap.polito.it/>