A Review of Defense in Depth Physical Security Model

* Mohd Nizam Zakaria[1], Hafiza Abas[2], Azizul Azizan[3]
Advance Informatics Department
Razak Faculty of Technology and Informatics
Universiti Teknologi Malaysia
Jalan Sultan Yahya Petra, 54100, Kuala Lumpur
azmurinuri@gmail.com[1], hafiza.kl@utm.my[2], azizulazian@utm.my[3]

Article history

Received:
9 Sept 2019

Received in revised form:
31 Oct 2019

Accepted:
20 Dec 2019

Published online:
30 Dec 2019

*Corresponding author
azmurinuri@gmail.com

Abstract

Physical security, parameter protection and access control in government agencies especially in State Government localities have suffered severe negligence and disrepair. Local state governments, many established over four decades ago, applied obsolete security and safety measures within its compound. The main problems faced such as building maintenance scheme, lack of security measures and implementation and poorly documented security references are further described in this paper. The foundation of physical security protection design lay the groundwork as a basis of research. Then, mechanical physical protection schemes are investigated to mitigate the lack of safety and security mentioned. To complement these measures, Crime Prevention Through Environmental Design (CPTED) Principles and Security Education, Training and Awareness (SETA) techniques are further explored in hopes to establish an all-encompassing security model. This study will use a mix method design by incorporating qualitative and quantitative analysis. Main data collection came from sets of questionnaires and observation checklists by using CPTED, Physical Security Plan and SETA principles. The finding of this study is to prove whether this model can increase overall security in the State Government localities. This study hopes to propose a complete physical security model that can be reproduced and most importantly, increases overall security in State Government and the Federal Institution compound in general.

Keywords: *Physical Security, Access Control, CPTED, Security Awareness*

1. Introduction

In physical security study, territoriality, physical access control and perimeter protection plays a vital role in determining a facility security posture. The concept of territoriality is actually geographical boundaries made by people organizing space for their own aim [1] (Gottmann,1975). Considerable difficulty arises in defining exactly what territory consists of, and what role it must be assigned in the recognition and functions of a national state. In a geographer standpoint, territory is defined as a portion of concrete space accessible by human activities.

In an urban setup, security complexity has become more intertwined with networks of urban expansions, hardware and software aspects [2] (Coaffee, Clarke, & Davis, 2016). In order to address this issue, the European Union has funded a security project to develop a comprehensive, multi - faceted, yet mutually reinforcing concept to improve urban infrastructure and development of security, resilience and sustainability. Called the HARMONISE project, the main finding

* *Corresponding author. azmurinuri@gmail.com*

concludes that there are misalignments of emergency planning, national security, urban planning, climate change and sustainability, crime and community security.

Similar situation exists in Malaysia's physical security environment. There are significant misalignments in planning, building design, security measures, policies and general awareness that leads to the point of careless neglection in security aspects.

Therefore, the objectives of this paper is to find the solutions by identifying the current problems in physical security and access control within Federal and State Institution facility, analyze best practices in area security implemented in other country or external agencies, to implement the best options available to be integrated into Malaysia's security environment and to propose a security model that will increase overall security and accessibility. As a start, Kota Bharu Municipal Council (KBMC) has been selected to be the experimental ground in this security study.

For that, this paper will propose a physical security model called Defense in Depth that tries to bind together vulnerability assessment, mechanical physical security setup, Crime Prevention Through Environmental Design (CPTED) principles, Security Awareness and Education into one cohesive model. It will try to uncover both human related and technological factors that contribute to the problems while at the same time provide a feasible solution that will benefit both organization and the field of physical security study.

Background, related studies, method for conducting research, initial impact of security assessments using the model and discussions for the next step of implementation are presented in consecutive sections in the paper.

2. Background

Factors contributing to the problems mentioned in Section 1 are building maintenance scheme, lack of security measures and implementation and poorly documented security references.

2.1 Building Maintenance Scheme

According to Crespo Márquez, Moreu de León, Gómez Fernández, Parra Márquez, & López Campos [3], maintenance management are divided into two (2), first part is the maintenance policy, objective and strategy and the second part is the implementation of the former. In Malaysia, management of building maintenance dealt with ineffective policies and ineffective procedures based on an ad hoc or reactive basis [4] (Abdul-Rashid & Ahmad, 2011). This has been proven a problem because to prolong a lifespan of a facility, a proper and systematic approach in maintenance must be adopted especially in public centered buildings [5] (Khalid, Abdullah, Hanafi, Said, & Hasim, 2019). Poor financial returns compared to other professional interests and due to a lack of in-depth training in maintenance management, materials technology and low maintenance status in the construction industry contribute to these problems.

2.2 Lack of Security Measures and Implementation

According to Khalid et al., [5], security is a tradeoff between threat and protection. In other words, security can be seen as the proportion of potential threat to be realized in relation to efforts to prevent it from occurring. As the paper is focused on security and maintenance posture in public facility, there are certain loose ends in maintaining level of security. Most of security measure heavily rely on guards and perimeter protection such as walls, fences and gates are insufficient and does not meet current standards set by Ministry of Housing and Local Government (MHLG) [6]. (Department of Town and Country Planning Malaysia, 2009).

2.3 Poorly Documented Security References

Standardization is a way of promoting best practices and requirements that must be fulfilled in a transparent manner on world markets. At the same time, it is a means of establishing conformity mechanisms whether these products or services comply with International Organization for Standardization standards [7]. Poorly documented procedures and guidelines are among several problems detected in most government bodies. According to Boyd, Pucciarelli, & Webster [8], poorly documented policies, procedures and ineffective document driven process will cause processes not functioning properly, resulting in high business costs.

3. Related Studies

A literature review was conducted to find a feasible solution to the problems mentioned in Section 2. There are no one stop solution to address the problems in one swoop, therefore several fields of studies have been investigated to create the proposed physical security framework. Relevant studies for the proposed solution are summarized in Sections 3.1 to 3.6.

3.1 Facility Security and Protection Foundation

The paper based its foundation on the concept of facility security and protection with the study conducted by Garcia [9]. This paper described the basic tenets of physical security needs that most facilities in other countries adopts. Although quite thorough, it does not cover problems encountered in real situation for most government establishment, especially on maintenance and the importance of proper policies that are needed to address it.

3.2 Facility Vulnerability Assessment

A study conducted by Kemp [10], outlines the guides for facility vulnerability assessment. It is important to understand why a facility need to be protected and provide a benchmark in evaluating the security posture of a building and surrounding adjacent compound. Table 1 shows the ranking system and matrix of vulnerability for a facility.

Table 1: Facility Vulnerability Ranking

Type	Ranking/Score
Negligible Vulnerability	0 – 9 points
Low Vulnerability	10 – 18 points
Medium Vulnerability	19 – 27 points

High Vulnerability	28 – 36 points
Critical Vulnerability	37 – 45 points

3.3 Physical Security Posture

To evaluate Physical Security Posture, 3 main studies namely Effective Facility Security Plan [11]. Effective Physical Security [12] and Ministry of Housing and Local Government (MHLG) Crime Prevention Through Environmental Design (CPTED [6] are used. Not only basic physical security is evaluated, the ultimate goal for a security setup is to deter crimes that can or may be committed within the facility's compound. All these criteria will be integrated into the proposed security model in Section 3.7.

3.4 Facility Maintenance Posture

Maintenance plays a big part in defining whether a facility is properly cared for. Buildings that are not properly maintained will leave an impression of abandonment, thus making it a target for vandalism or even worst, crime. By evaluating maintenance posture as pointed out by Abdul-Rashid & Ahmad [4] and Khalid [5] current state of maintenance scheme for KBMC are laid out.

3.5 Employee Security Awareness

In order to produce a complete framework, factors involving awareness and education are also evaluated. It is useless to provide bleeding edge security concepts and technologies if the employees operating it are oblivious to security awareness. By evaluating employees security best practice and awareness proposed by Tsohou [7], it provided an insight for the level of readiness if an organization wants to adopt the model.

3.6 Employee Security Education

By having adequate security education and training for an organization as stated by Defense Security Services, [13] and ISO/IEC, [14], the proposed security framework will have a longer lasting effect on overall security for the facility adopting it. That's why this criterium is important for the model to be in full effect.

3.7 Proposed Defense in Depth Security Model

By using related studies in security presented in sections 3.1 to 3.6, initial proposed physical security model is as shown in Figure 1.

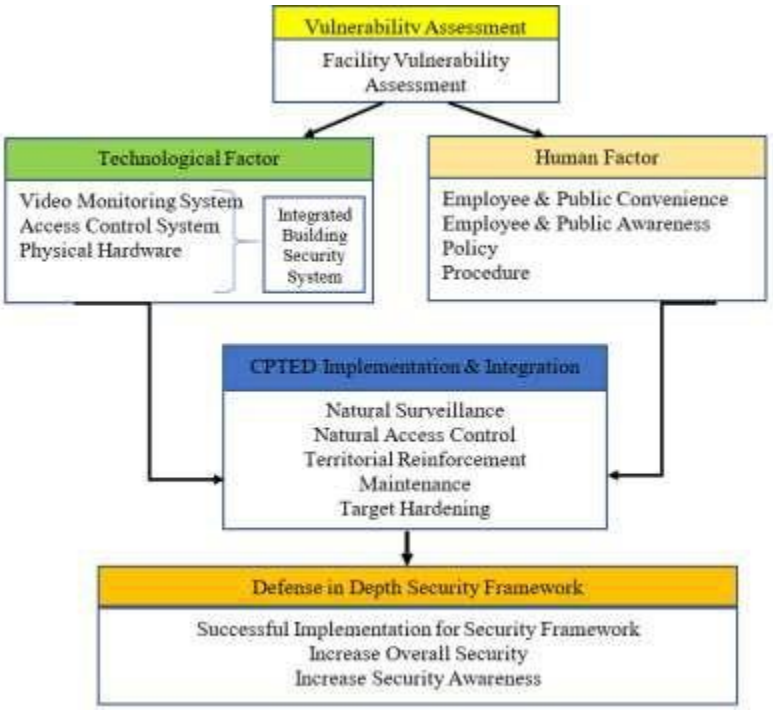

Figure 1: Initial Proposed Physical Security Framework

4. Methodology

4.1 Population Sampling

Sampling size to conduct data collection is determined by the average number of visitors and employees present at the public administration organization at a particular time. From information gathered, usually there will be around 250 to 300 people inside the compound conducting their activities. Therefore, according to Krejcie & Morgan, [15], sampling size that closely represents the population is 170. Stratified sampling is used that basically has 2 strata namely the employees and the public. The stratified sampling from both employee and public visitors are then randomly selected using Simple Random Sampling according to departments (employees) and age group (visitors).

4.2 Approach for Data Collection and Analysis

Table 2 depicts the tools and methods for data collection and analysis.

Table 2: Data Collection and Analysis

Assessment Criteria	Data Collection	Field of Study/Reference
Facility State of Vulnerability	Observation Checklist	Facility Vulnerability Assessment
Physical Security Posture	Observation Checklist	Facility Security Plan
	Observation Checklist	Effective Physical Security
	Observation Checklist	CPTED

	Questionnaire	CPTED
Facility Maintenance Posture	Observation Checklist Observation Checklist	Old building management Maintenance of public buildings
Employee Security Awareness	Questionnaire	Security Best Practice and Awareness
Employee Security Education	Questionnaire Questionnaire	Facility Security Officer Training Course ISO/IEC 27001 Information Security Management

4.3 Measuring Variables and Proving Hypothesis

The hypothesis that the paper is trying to prove is "Overall security can be improved using the proposed model". In order to do that, 8 variables have been identified for measurement. All the variables are shown in Table 3.

Table 3: Variables and Methods

Variables	Method to Measure
CCTV Monitoring	Security model for Video Surveillance (Kim & Han, 2012) [16]
Access Control	Security Criteria for Access Control (Mihajlov, Blažič, & Josimovski, 2011) [17]
Planning Physical Security	Physical Security Plan [11]
Employee & Public Convenience	SUS (Brooke, 1986) [18]
Employee & Public Awareness	Value Tree [19] Scorecard [20], AHP [21]
SOPs	Based on availability
Policies	Based on availability
CPTED	Cronbach Alpha Index &Spearman's Rho Correlation [22]

5. Initial Security Assessment

As a start, Kota Bharu Municipal Council (KBMC) was picked to be the test bed of the proposed model. Security posture of the facility is assessed according to the criteria in the model.

5.1 KBMC Vulnerability Assessment

Total score for vulnerability for KBMC is 28 which is classified as High Vulnerability. There are 9 criteria of assessment in Kemp [10], which are Visibility Level, Site Criticality to Jurisdiction, Impact of the Site Outside Jurisdiction, Accessibility to the Site for Public, Possible Hazards Located on Site, Height of the Building, Building Construction Type, Population Capacity on Site and Potential for Mass Collateral Casualties. In the matrix, the higher the score, the more it is susceptible to danger. Table 4 shows each evaluated criteria.

Table 4: KBMC Vulnerability Rating

Vulnerabilities	Ranking	KBMC Score
Visibility Level	KBMC Scale = 4; well known in the state of Kelantan	4
Site Criticality to Jurisdiction	KBMC Scale = 5; critical for the administration of Kota Bharu City	5
Impact of the Site Outside Jurisdiction	KBMC Scale = 5; Huge impact for business, public or other government bodies as any activities to be conducted the city must go through Municipal Council	5
Accessibility to the Site for Public	KBMC Score = 4; has open access to the public and has few unprotected open space	4
Possible Hazards Located on Site	KBMC Score = 0; no hazards inside compound	0
Height of the Building	KBMC Score =2; height of buildings in the compound is no more than 5 story high	2
Building Construction Type	KBMC Score = 4; has mixed wood and concrete construction	4
Population Capacity on Site	KBMC Score = 2; around 250 – 300 people inside compound at a given time	2
Potential for Mass Collateral Casualties	KBMC Score = 2; around 500 – 1,000 people can be affected in collateral casualty, the area is in close proximity with main road and other buildings	2
Total Score		**28**

5.2 Physical Security Posture

To evaluate initial security posture, a set of questionnaires was produced to collect response on 25 selected employees in KBMC. Out of the 25 respondents, only 17 responded back. Aside from questionnaire, an observation was also carried out to record the findings using checklist. For this initial study no score or matrix system was used to give any rating. Summary of results are as shown in Table 5 for building and Table 6 for compound assessment.

Table 5: Building Physical Security Posture

Evaluation	Findings	Comment
Door Grills	Door grills are present for	In good condition

	doors leading to offices	
Doors	Doors are sturdy	Most of the doors are not fire resistance
Locks	Locks are present and in good condition	Can be improved by installing deadbolt locks
Windows	Naco Louvre window type for all windows in the building	No window grills are installed
Access Control to Building	Proper access control to offices are not practiced/present	Visitors have unrestricted access to office space. Could lead to security breaches
Corridors	Corridors have ample walking space	Corridors are cluttered with old furniture/debris
Natural Surveillance	Hindered by tall furniture inside the office	Can be improved by rearranging the furniture
CCTV Surveillance	Fitted in critical departments (Finance and IT/server room)	Not functioning/broken
Open Spaces	Only 1 open space inside the building that housed the public services counters	The space is well lit and offer good viewing. Placement of help desk is inappropriate. It should be able to observe visitors entering/exiting
Lightings	Lighting within the building are sufficient	-
Inside Office Space	Tight office space	Difficult to maneuver in case of emergencies
Inside Office Layout	Very tight and obscure view to the outside	Most of the furniture inside the office obscure view to the windows
Building Layout Plan	Not present	Should be in place for easy reference in cases of emergencies

Table 6: Compound Physical Security Posture

Evaluation	Findings	Comment
Walls and Fences	Walls surrounding the compound are easily scaled. Fences behind building can easily be cut by wire cutter	Perimeter walls should be at least 5 feet high. MPKB have 3 feet walls
Gates	Gates are stainless steel but show signs of rust	Easily knocked down in vehicle ram raid
Traffic routes	One-way traffic route inside compound. Blind bends present	No security mirrors at blind road bends
Entrances	1 main entrance, 2 side entrance	2 side entrances can be closed or only allowed to open during certain

		period of time
Access Control to Compound	Controlled by guards and MPKB enforcers	Enough guards present for security and surveillance
Pedestrian Walkways	Narrow walkways	No visible road dividers between walkways and traffic route. Dangerous for pedestrian
Natural Surveillance	Natural surveillance inside compound are poor	Hindered due to many blind bends and secluded areas
CCTV Surveillance	CCTV surveillance towards the compound are inadequate	CCTV surveillance are set up to monitor main road adjacent to the compound
Parking Spaces	Parking spaces are not enough	Main parking space are easy to monitor
Lightings	Lighting inside compound are sufficient	-
Secluded Area	Exist behind the compound, not easy to monitor or observed, no patrol to the back of the compound	No CCTV monitoring
Security Personnel	Sufficient security personnel	Area patrols only done at night
Guard Post	Old guard post, made of wood. No protection/buffer from main road	Very vulnerable to ram raid
Compound Plan	Not present	Should be erected for easy public reference

5.3 Facility Maintenance Posture

Overall maintenance posture for KBMC is evaluated using an observation checklist and questionnaire. Table 7 portrayed the summarized findings.

Table 7: Facility Maintenance Posture

Evaluation	Findings	Comment
Trees	Tall trees obscure view to outside of the compound	Lowest tree branches are less than 2 meters high, easy to scale and enter compound
Shrubs	Well maintained	-
Fences/Walls	Not well maintained	Should be replaced
Gates	Old gate, rusted	Can be considered to replace
Walkways and	Not well maintained	Cluttered with debris

Corridors		
Signage	Not enough	Add more signage
Electronic/Mechanical Surveillance	Not well maintained	Need proper maintenance
Garbage Disposal	No issue in garbage disposal	-
Lightings	Well maintained	-
Guard Post	Poor condition and made of wood	Should be replaced

5.4 Employee Security Awareness & Education

Table 8 summarized the initial finding of employee security awareness and education

Table 8: Employee Security Awareness and Education

Evaluation	Findings	Comment
ISO 9002 Standard	Municipal council have received accreditation	-
ISO 27001 Standard	Not practiced	Should be informed and educated
Facility Security Training	Only KBMC enforcers and Guards are trained	Other staff should be educated
Internal Security Audit	Not been done	Internal body should be designated
External Security Audit	Done 2-3 years ago	Should be scheduled properly
Security Awareness Program	No programs scheduled	Should be programmed properly
Inhouse Security Training	Never been done	No schedule for in-house training
External Security Training	Done 3 years ago	No scheduled training with outside agencies
Classroom or Facility for Training	Not present	Need to designate a proper facility

6. Discussion

6.1 CPTED Principles for Effective Physical Security Framework

By implementing CPTED principles in the overall design of the security model, an organization will not need to rely heavily on just the technological solutions. Human factors will also benefit from CPTED because employees will be responsible for their surrounding and indirectly promote a sense of security awareness. This is because CPTED can increase security features into a security model and help authorities in preventing crimes relying through a very natural and humane concept [23].

6.2 Security Education, Training and Awareness

SETA programs will enhance and promote awareness among users who will assume security roles proactively. Overall security can be achieved with proper integration of technology, policy, crime prevention design and human cooperation in the newly proposed model. This will enhance the perception that the employee's efforts will lead to the successful performance of the desired safety behavior [24]

7. Conclusion

Government agencies can benefit extensively from the security model that aim to cover all aspects of security. Not only will it increase awareness among employees but cost for expensive system, state of the art detectors and other peripherals can be reduced. The paper also hopes to bridge the gap of security implementation and knowledge that plague most government agencies while at the same time not hindering core services that they intend to provide. The biggest limitation faced is the implementation process may take some time to complete because current lack of resources and budget. Suggestion for future works are to implement the model and additional data collection to prove the hypothesis.

Acknowledgments

The authors would like to recognize the participation of the Kota Bharu Municipal Council employees in the conduct of this study.

8. References

[1]. Gottmann, J. (1975). The evolution of the concept of territory. *Social Science Information*, *14*(3), 29–47. https://doi.org/10.1177/053901847501400302

[2]. Coaffee, J., Clarke, J., & Davis, P. T. (2016). A HARMONISE'd approach to building security-driven urban resilience: a call to arms. *Journal of Financial Management of Property and Construction*, *21*(1), 73–80. https://doi.org/10.1108/JFMPC-01-2016-0003

[3]. Crespo Márquez, A., Moreu de León, P., Gómez Fernández, J. F., Parra Márquez, C., & López Campos, M. (2009). The maintenance management framework. *Journal of Quality in Maintenance Engineering*, *15*(2), 167–178. https://doi.org/10.1108/13552510910961110

[4]. Abdul-Rashid, R., & Ahmad, A. G. (2011). The implementation of maintenance works for historical buildings - A review on the current scenario. *Procedia Engineering*, *20*, 415–424. https://doi.org/10.1016/j.proeng.2011.11.184

[5]. Khalid, E. I., Abdullah, S., Hanafi, M. H., Said, S. Y., & Hasim, M. S. (2019). The consideration of building maintenance at design stage in public buildings. *Facilities*, F-04-2018-0055. https://doi.org/10.1108/F-04-2018-0055

[6]. Department of Town and Country Planning Malaysia. (2009). Implementation Guide of Crime Prevention Through Environmental Design (CPTED). *Crime Prevention Through Environmental Design (CPTED): Implementation Guide*, 60.

[7]. Tsohou, A., Kokolakis, S., Lambrinoudakis, C., & Gritzalis, S. (2010). A security standards' framework to facilitate best practices' awareness and conformity. *Information Management & Computer Security*, *18*(5), 350–365.

[8]. Boyd, A., Pucciarelli, J., & Webster, M. (2012). It's worse than you think: poor document processes lead to significant business risk. *Framinham: IDC*.
[9]. Mary Lynn Garcia. (2007). Design and evaluation of physical protection systems
[10]. Kemp, R. L. (2007). Assessing the vulnerability of buildings. *Disaster Prevention and Management: An International Journal*, *16*(4), 611–618. https://doi.org/10.1108/09653560710817075
[11]. Roop, M. R. (n.d.). An Effective Facility Security Plan, (630).
[12]. Perry, M., & Fennelley, L. J. (2016). *Effective Physical Security (Fourth Edition)*. https://doi.org/10.1016/B978-0-12-415892-4.00001-8
[13]. Defense Security Services. (2015). Facility Security Officer (FSO) training courses – Facility Security Clearance (FCL) Portal. Retrieved April 12, 2019, from http://facility-clearance.com/security-officer-fso-training/
[14]. ISO/IEC. (2005). ISO/IEC 27001:2005, Information Security Management Systems-Requirements. *Information Systems*, *2005*.
[15]. Krejcie, R. V, & Morgan, D. (1970). Determining sample size for a research, 607– 610.
[16]. Kim, G. W., & Han, J. W. (2012). Security model for video surveillance system. *International Conference on ICT Convergence*, 100–104. https://doi.org/10.1109/ICTC.2012.6386789
[17]. Mihajlov, M., Blažič, B. J., & Josimovski, S. (2011). Quantifying usability and security in authentication. *Proceedings - International Computer Software and Applications Conference*, (December 2014), 626–629. https://doi.org/10.1109/COMPSAC.2011.87
[18]. Brooke, J. (1986). SUS - a quick and dirty usability scale, *13*(5), 531–536. https://doi.org/10.4236/9781618961020_0002
[19]. Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, *25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008
[20]. Belton, V., & Stewart, T. (2002). *Multiple criteria decision analysis: an integrated approach*. Springer Science & Business Media.
[21]. Saaty, T. L. (2002). Decision making with the Analytic Hierarchy Process. *Scientia Iranica*, *9*(3), 215–229. https://doi.org/10.1504/ijssci.2008.017590
[22]. Sakip, S. R. M., & Abdullah, A. (2012). Measuring Crime Prevention through Environmental Design in a Gated Residential Area: A Pilot Survey. *Procedia - Social and Behavioral Sciences*, *42*(July 2010), 340–349. https://doi.org/10.1016/j.sbspro.2012.04.198
[23]. Davey, C. L., & Wootton, A. B. (2016). Integrating crime prevention into urban design and planning. *Journal of Place Management and Development*, *9*(2), 153–165. https://doi.org/10.1108/jpmd-09-2015-0043
[24]. Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., & Courtney, J. F. (2015). Assessing the role of security education, training, and awareness on insiders' security-related behavior: An expectancy theory approach. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2015-March*, 3930–3940. https://doi.org/10.1109/HICSS.2015.471

Authors

Mohd Nizam Zakaria, Postgraduate student at UTM Razak School of Advance Informatics, UTMKL. Currently working in MINDEF

Dr. Hafiza Abas, UTM Senior Lecturer at UTM Razak School of Advance Informatics, UTMKL

Dr. Azizul Azizan, UTM Senior Lecturer at UTM Razak School of Advance Informatics, UTMKL