# Importance of Information Security Education and Awareness in Ghana

Patrick Kwaku Kudjo
Jiangsu University
China Zhenjiang
P.R.China, 212013

Dickson Keddy Wornyo
Jiangsu University
China Zhenjiang
P.R.China, 212013

Elias Nii Noi Ocquaye
Jiangsu University
China Zhenjiang
P.R.China, 212013

## ABSTRACT

The advent of the computer age has incited an increasing interest in the fundamental data sets that can now easily be stored and investigated. The introduction of computer network and internet bridges the communication barriers between millions of people hereby making security an inevitable issue to deal with. There are several aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting of passwords. One essential aspect for secure communication is that of cryptography, the recent growth in business, education and communication of Ghana's economy cause for a toughly cyber security education and awareness. Most Cyber-attacks are due to lack of education, awareness and users who ignore security practices. We propose to use a survey and experiment to create a model to improve the level of information security education and awareness in the country.

## Keywords

Access Control, Bell-La Padula, Cyber-Security, Cryptography, Education

## 1. INTRODUCTION

The rapid increase in computing and network application as well as the various threats poses by cyber-attacks cause for a need in computer education and awareness in information security. The core resources and data of any organization is always assessed and used by end users, it is therefore prudent to educate users on the current security systems that can be implemented to effectively and efficiently protect these assets. The recent cyber-attacks on institutions in the country clearly indicate the need for education and creating awareness on Informational security issues. A survey by the Federal Bureau of Investigation on cyber-attacks is incredibly serious and growing; cyber intrusions are becoming more commonplace, more dangerous and more sophisticated [1-4]. Various nations' critical infrastructure including both private and public sector networks are targeted by adversaries[5]. Billions of dollars are lost every year repairing systems hit by such attacks. These attacks affect vital systems, disrupting and sometimes disabling the work of hospitals, governmental institutions, schools and banks around the world. This thus cause for a need to enhance the security system of every organization. It is based on this that the Federal Information Security Management Act of 2002[6] was put in place for the purpose of protecting information and systems authorized access, information use, disclosure, disruption, modification, destruction, confidentiality, integrity and availability of information.

The survey identified several factors as the main causes of information security accidents; these include human nature,[7] buggy software[8] and wrong configurations, lack of awareness and education, security makes things harder to use, economic factors e.g. consumers do not care about security; security is expensive and takes time. Over the past five years, Ghana as a nation has experience several cyber-attacks in the banking sector, schools, hospitals and other governmental agencies. The recent report by Ministry of Communication Ghana (2014) reveals a number of websites defaced by hackers, (Alsancak Tim, a nationalist Turkish) these include website of National Communication Authority, the National Information Technology Agency (NITA) etc. and the most important been the website of the Vice President of Ghana all being defaced in recent past. Most cyber security expert in Ghana are of the view that there could be more of such attacks on government agencies and companies as well as important private institutions if the nation does educate create awareness and also develop and implement a cyber security strategy to address this problem. Furthermore over the past five years, the main institution responsible for conducting examination (WACE) in Ghana and even West Africa for Junior High and Senior High had a lot of examination questions been leaked causing a lot of financially loss to the nation and putting much pressure on student. WACE cancelled about two thousand pupils who sat for the exams, due to examination leakage. Another popular menace in the country is "Sakawa" where cyber criminals tend to dupe unsuspecting internet users from Ghana and outside of huge sums of money. These attacks have indented the national image of Ghana and cause for a security education and awareness program and also improving the cyber infrastructure of the country. The institutions mostly affected by cyber-attack in Ghana include but not limited to the following National Defense and Security, Banking and Finance, Information and Communications, Energy, Health Services, Government, Emergency Services and educational institutions.

In this paper a survey was conducted among various student studying in China from Ghana who represent the critical national informational infrastructure sector of the country such as education, National defense & security, healthcare, governmental agencies, Information & Communications financial institutions, Emergency services, insurance companies retail, hospitality and professional services to investigate their level of information security education and awareness on cyber security.

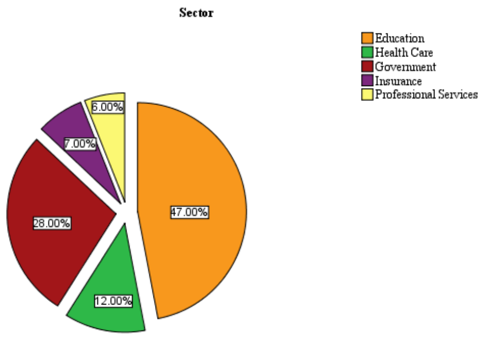

**Fig 1: Representation of the various institutions**

The survey sample 100 Masters and PhD students out of about 170 students studying in the university, 80% represent males and 20% females.

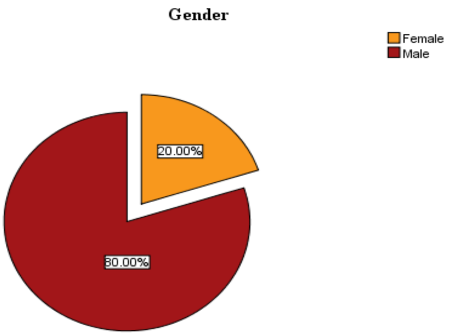

**Fig 2: Gender Representation**

The questionnaires provided by the researchers were to assess the level of information security Education and awareness on five security policy model which include the Bell-La Padula model, Clark-Wilson model, Chinese wall model, BMA model and Jikzi model.

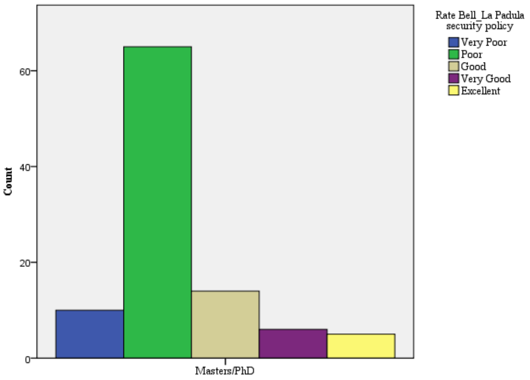

**Fig 3: Respondents Knowledge on Bell-La Padula model**

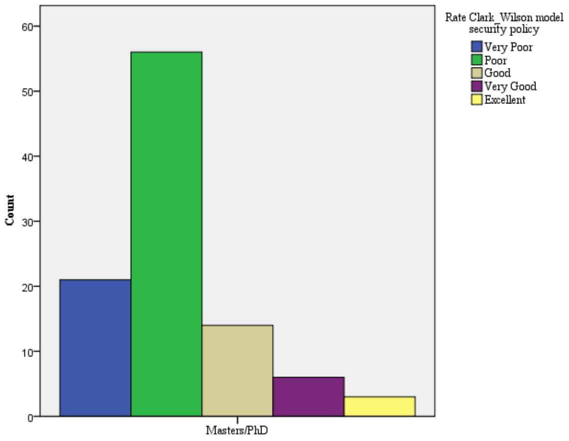

**Fig 4: Respondents Knowledge on Clark-Wilson model**

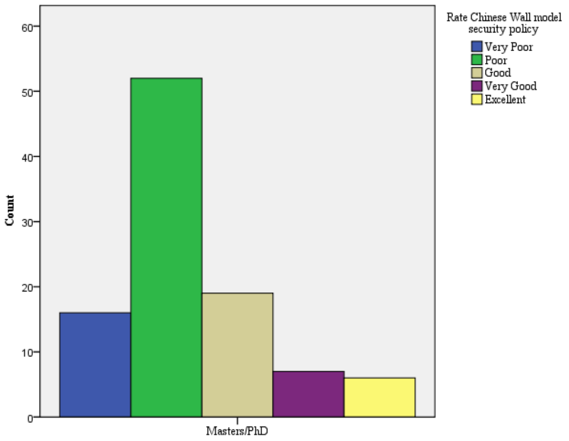

**Fig 5: Respondents Knowledge on Chinese wall model**

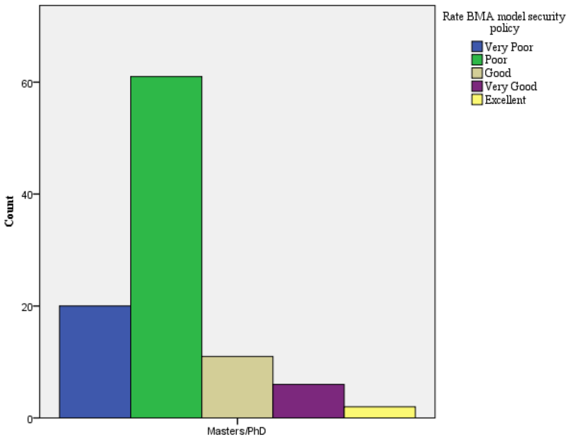

**Fig 6: Respondents Knowledge on BMA model**

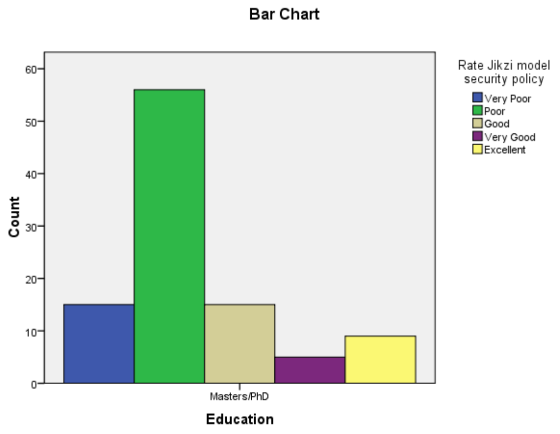

**Fig 7: Respondents Knowledge on Jikzi model**

The weakness related to information security education, awareness and practices were identified and the Bell-La Padula security model has been proposed to help provide confidentiality in the various institutions.

## 2. THE NEED FOR EDUCATION

The various ministries, departments, schools and financial institutions whose website and data were attack contained sensitive data that need to be protected. A recent report by IBM's "2014 [9] indicates that 95 percent of all security incidents involve human error. Many of the successful security attacks from external hackers on the nation are as a result of prey on human weakness and insiders within organizations who unwittingly provide them with access to sensitive information. Again a research conducted by Federal Computer Week reports that, the greatest impacts of successful security attacks involves insiders exposing sensitive data. The research further reported that 59 percent of respondents agree that most information technology security threats that directly result from insiders are the result of innocent mistakes rather that malicious abuse of privileges[9, 10]. Although Ghana has a policy statement on cyber security towards the following sectors;

This policy only aims to develop and establish a comprehensive program and a series of frameworks that will ensure the effectiveness of cyber security controls over vital assets. It however lacks staff development, training on current security trends that can effectively prevent cyber-attacks. Previous research conducted shows regular staff development, training and implementation of security policies [11-15] which attest that regular staff training on cyber security policies is necessary for the nation.

## 3. TYPES OF ATTACKS

Users have to be educated on the various types of attacks and the attacking techniques used by these hackers.

### 3.1. Reconnaissance Attack

The hacker's collects information such as IP address range, server location, running OS software version and types of devices etc. this information will be used in mapping your infrastructure for the next attack[16-18]

### 3.2. Password Attack

In this type of attack, the adversary ties to login using guessed password, they usually implore two main techniques which are brute force attack and dictionary attack. The growth and increase in computer networks have created several opportunities for hackers and intruders to comfortably hack into many information systems. The main objective of these intruders is to gain power and control over the computer system or network. [19, 20]. There are different techniques and methods employed by these intruders to automatically gain access or privileges into these systems, this include password guessing, intercepting, social engineering, virus etc. It is there necessary to educate user on some of the new password authentication schemes such as RSA-Based Password Authentication scheme proposed by Yang an Shieh, they proposed two main password authentication system [21]. Another password authentication scheme that can be used is the one timestamped password authentication scheme [22-24]. Other research conducted on password authentication using smart cards includes a new remote user authentication scheme using smart card, modified remote user authentication scheme using smart card etc. [25-34].

### 3.3 Spoof Attack

Spoofing attacks is as well one of the most dangerous and serious attacks on network or computer system, the intruder send messages to a computer system indicating the message or content is from a trusted entity, they also sometimes changes the sources address of packets so as to receive or assumes that packet comes from someone else, typically bypassing the firewall rules of the system. Spoofing attacks are a serious threat as they represent a form of identity compromise and can facilitate a variety of traffic injection attacks.[35-39]

### 3.4 MITM Attacks

In this attack, an adversary captures data from middle of transmission and changes it, then sends it again to the destination. Receiving person thinks that this message comes from the original source. The whole objective of the attacker is to monitor, capture and control communication.[40-44] This type of attack makes it difficult for organizations and individuals to effectively protect and secure data privately since the attackers can remotely attack using fake addresses. The attack occurs in the following ways, ARP Cache Poisoning, DNS Spoofing, Session Hijacking, and SSL Hijacking[45]. It is therefore necessary to educate the various workers in the country on how to prevent some of these attacks. Research conducted on these types of attackers proposed several tools to help realize MITM attacks, these tools are particularly useful in Local area network environments, and they include Packet Creator, Ethercap, Dsniff, Cain and Abel. [46-49]. Other preventive methods that can be employed are the use of public key Infrastructure, verifying delay in communication and stronger mutual authentication [50-52].

### 3.5 Ping Sweep Attack

In this type of attack, the hacker's pings all possible IP address on a subnet to find out which hosts are up, once he finds up a system, he tries to scan the listening ports. The attackers can then learn from the types of services running on that system based on the listing ports[53]. It thus involves information gathering technique which is used to identify host by pinging them.

## 4. PROPOSED POLICY MODEL

Information Security is deemed to safeguard three main goals; Confidentiality which involves preventing authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information. Integrity on the other hand is guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information. Availability is the process of ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system. Organizing in-service training programs for staff on current security policies such as ways of protecting data, levels of confidentiality, data sensitivity as well reading and acknowledging security policy issues is a critical step.

Information security Policy is a statement that captures the requirements or state of an organization into authorized or unauthorized, secure or unsecure states and set of actions that have to be undertaken to achieve security. The concept of security policy model originated from the Military sector however the Bell- La Padula (BLP) appears to be the most popular and first introduced security policy [54]. The other security policies include Clark –Wilson model, Chinese wall model, the BMA model, Jikzi Model, etc. [55].

However for the purpose of this paper, we propose to use the Bell-La Padula model as a technique to provide confidentiality in the various institutions in Ghana.

Again users will be educated on topics such as how to collect, use, delete data, maintains data quality, records management, and appropriate utilization of IT systems.

The Bell- La Padula (BLP) is a model proposed by David E Bell and Leonard J. La Padula that focuses on mandatory and discretionary access control techniques[56, 57]. It main objective is to keep secret data secret and share this data when it is allowed to be shared. This technique use two main restrictions model known as the read down and write up. Reading down model is to prevent users from gaining access to information above their security clearance and when a subject can append access to objects whose security level is higher than its current clearance level is known as writing up. A set of access rights are as well given to subjects, read only, append, execute and read write. The security level of the model is arranged in a linear order from the top secret or highest to the lowest level, and the levels as well consist of a set of subjects(s) and objects (o). The subjects L(s) have security Clearance whiles the objects have security classification L (o). The model has a simple security property, i.e. a subject s may have read access to an object o only if

$L(o) \leq L(s)$ and a subject who has read access to an object o may have write access to an object p only if $L(o) \leq L(p)$. Bell and La Padula modeled the behavior of a protection system as a finite state machine and defined a set of state transitions that would not violate the security of the system. The following operations guarantee a secure system:

### 4.1.1 Get access

Used by a subject to initiate access to an object (read, append, execute etc.)

#### 4.1.1.1 Release access:

This type of access is used by a subject to give-up an initiated access.

#### 4.1.1.2 Give access:

Controller of an object can give a particular access (to that object) to a subject.

#### 4.1.1.3 Rescind access:

Controller of an object can revoke a designated access (to that object) from a subject.

#### 4.1.1.4Create object:

Allows a subject to activate an inactive object

#### 4.1.1.4Delete object:

Allows a subject to deactivate an active object and Change security level: Allows a subject to change its clearance level ( below an initial assigned value) educating and Enforcing this access control in government and military applications will help reduce security attack

## 5. RELATED WORK

Burcu Bulgurcu et al.[11] investigated the impact of information security awareness on outcome beliefs and an employee's attitude towards compliance with ISP, they want to ascertain the relationality based factors that drive an employee to comply with requirements of the ISP with regards to protecting the organizations information and technology resources. Their findings indicate that an employee's intention to comply with the ISP is influenced by attitude, normative beliefs, and self-efficacy to comply

Kruger HA et al. [58] in a similar way stated that in order to realize the value of information security awareness and education program in an organization, it is necessary to have a set of methods to study and measure its effect. They therefore use a prototype model for measuring information security awareness in an international mining company.

R. S. Shaw et al. identified three main levels of security awarness which include perception, comprehension, and projection. They further reported on a laboratory experiment that investigates the impacts of hypermedia, multimedia and hypertext to increase information security awareness among the three awareness levels in an online training environment. The results of the experiment shows that the techniques adopted is useful and could be used by educators and training designers to create meaningful information security awareness materials [59].

B. D. Cone et al. in their work indicated that, cyber-security education and awareness programs should be tailored to address the policies and requirements of a particular organization. They also show that most cyber-security education and awareness programs were typically rote learning which does not allow users to think and apply security concepts hence the proposed highly interactive video game as a tool that can support organizational security training and awareness which is very effective for general computer users [60].

C. McCoy and R.T Fowler conducted a research on information security awareness program to educate staff, faculty and students on the importance of information security issues. They proposed a framework of establishing a flexible information security program that can be adapted to meet current and future demands [61].

## 6. CONCLUSION

Information security education and awareness are vital to any organization. The sample population used for the study indicates very basic knowledge and techniques with regards to information security, there is therefore the need to properly educate the various critical national information sectors stated in the report and also implement current security techniques that protect data and resources. Further research can be conducted on other security policies using different techniques in cryptography

## 7. ACKNOWLEDGMENTS

Our thanks goes to Professor Jinful Chen and Professor Changda Wang all of Jiangsu University for their guidance and support.

## 8. REFERENCES

[1] R. Power, *2002 CSI/FBI computer crime and security survey*: Computer Security Institute, 2002.

[2] R. Richardson and C. Director, "CSI computer crime and security survey," *Computer Security Institute,* vol. 1, pp. 1-30, 2008.

[3] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Richardson, "2006 CSI/FBI computer crime and security survey," *Computer Security Journal,* vol. 22, p. 1, 2006.

[4] R. Power, "CSI/FBI Computer Crime and Security Survey, 1999," *Computer Security Issues & Trends,* vol. 5, 1999.

[5] S. Collier and A. Lakoff, "The vulnerability of vital systems: how ‘critical infrastructure’became a security problem," *The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitisation,* pp. 40-62, 2008.

[6] D. M. White, "Federal Information Security Management Act of 2002: A Potemkin Village, The," *Fordham L. Rev.,* vol. 79, p. 369, 2010.

[7] J. J. Gonzalez and A. Sawicka, "A framework for human factors in information security," in *WSEAS International Conference on Information Security, Rio de Janeiro,* 2002, pp. 448-187.

[8] J. D. Howard, "An analysis of security incidents on the Internet 1989-1995," DTIC Document1997.

[9] M. Carlton and Y. Levy, "Expert assessment of the top platform independent cybersecurity skills for non-IT professionals," in *SoutheastCon 2015*, 2015, pp. 1-6.

[10] A. Singh and B. Kapoor, "Analysis of the Human Factor behind Cyber Attacks," 2016.

[11] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS quarterly,* vol. 34, pp. 523-548, 2010.

[12] F. Cervone, "Understand the Big Picture So You Can Plan for Network Security," *Computers in libraries,* vol. 25, pp. 10-15, 2005.

[13] M. Siponen and A. Vance, "Neutralization: new insights into the problem of employee information systems security policy violations," *MIS quarterly,* pp. 487-502, 2010.

[14] J. L. Spears and H. Barki, "User participation in information systems security risk management," *MIS quarterly,* pp. 503-522, 2010.

[15] E. McFadzean, J.-N. Ezingeard, and D. Birchall, "Perception of risk and the strategic impact of existing IT on information security strategy at board level," *Online Information Review,* vol. 31, pp. 622-660, 2007.

[16] D. Zagar and K. Grgic, "IPv6 security threats and possible solutions," in *2006 World Automation Congress,* 2006, pp. 1-7.

[17] S. Standard, R. Greenlaw, A. Phillips, D. Stahl, and J. Schultz, "Network reconnaissance, attack, and defense laboratories for an introductory cyber-security course," *ACM Inroads,* vol. 4, pp. 52-64, 2013.

[18] N. C. Rowe and H. C. Goh, "Thwarting cyber-attack reconnaissance with inconsistency and deception," in *Information Assurance and Security Workshop, 2007. IAW'07. IEEE SMC,* 2007, pp. 151-158.

[19] G. Dua, N. Gautam, D. Sharma, and A. Arora, "Replay attack prevention in Kerberos authentication protocol using triple password," *arXiv preprint arXiv:1304.3550,* 2013.

[20] T. Xiang, K.-w. Wong, and X. Liao, "Cryptanalysis of a password authentication scheme over insecure networks," *Journal of Computer and system Sciences,* vol. 74, pp. 657-661, 2008.

[21] W.-H. Yang and S.-P. Shieh, "Password authentication schemes with smart cards," *Computers & Security,* vol. 18, pp. 727-733, 1999.

[22] C.-K. Chan and L.-M. Cheng, "Cryptanalysis of a timestamp-based password authentication scheme," *Computers & Security,* vol. 21, pp. 74-76, 2001.

[23] L. Fan, J.-H. Li, and H.-W. Zhu, "An enhancement of timestamp-based password authentication scheme," *Computers & Security,* vol. 21, pp. 665-667, 2002.

[24] N. Haller, "The s/key (tm) one-time password system," in *Symposium on Network and Distributed System Security,* 1994, pp. 151-157.

[25] M.-S. Hwang and L.-H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics,* vol. 46, pp. 28-30, 2000.

[26] H.-M. Sun, "An efficient remote use authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics,* vol. 46, pp. 958-961, 2000.

[27] C.-T. Li and M.-S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network and computer applications,* vol. 33, pp. 1-5, 2010.

[28] E.-J. Yoon, E.-K. Ryu, and K.-Y. Yoo, "Further improvement of an efficient password based remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics,* vol. 50, pp. 612-614, 2004.

[29] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," *IEEE*

*transactions on Consumer Electronics,* vol. 50, pp. 629-631, 2004.

[30] H.-Y. Chien, J.-K. Jan, and Y.-M. Tseng, "An efficient and practical solution to remote authentication: smart card," *Computers & Security,* vol. 21, pp. 372-375, 2002.

[31] J. Lee, S. Ryu, and K. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," *Electronics Letters,* vol. 38, p. 1, 2002.

[32] C.-C. Chang and S.-J. Hwang, "Using smart cards to authenticate remote passwords," *Computers & Mathematics with Applications,* vol. 26, pp. 19-27, 1993.

[33] W. Shiuh-Jeng and C. Jin-Fu, "Smart card based secure password authentication scheme," *Computers & Security,* vol. 15, pp. 231-237, 1996.

[34] I.-E. Liao, C.-C. Lee, and M.-S. Hwang, "A password authentication scheme over insecure networks," *Journal of Computer and System Sciences,* vol. 72, pp. 727-740, 2006.

[35] V. B. Srinivas and S. Umar, "Spoofing attacks in wireless sensor networks," *International Journal of Science, Engineering and Computer Technology,* vol. 3, p. 201, 2013.

[36] M. Bishop and L. Heberlein, "Attack class: Address spoofing," in *Proceedings of the Nineteenth National Information Systems Security Conference*, 1996, pp. 371-377.

[37] E. W. Felten, D. Balfanz, D. Dean, and D. S. Wallach, "Web spoofing: An internet con game," *Software World,* vol. 28, pp. 6-8, 1997.

[38] V. Santiraveewan and Y. Permpoontanalarp, "A graph-based methodology for analyzing ip spoofing attack," in *Advanced Information Networking and Applications, 2004. AINA 2004. 18th International Conference on*, 2004, pp. 227-230.

[39] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *IEEE Wireless Communications,* vol. 14, pp. 85-91, 2007.

[40] A. Ornaghi and M. Valleri, "Man in the middle attacks," in *Blackhat Conference Europe*, 2003.

[41] F. Callegati, W. Cerroni, and M. Ramilli, "Man-in-the-Middle Attack to the HTTPS Protocol," *IEEE Security and Privacy,* vol. 7, pp. 78-81, 2009.

[42] D. Kügler, "“Man in the Middle” Attacks on Bluetooth," in *International Conference on Financial Cryptography*, 2003, pp. 149-161.

[43] I. Dacosta, M. Ahamad, and P. Traynor, "Trust no one else: Detecting MITM attacks against SSL/TLS without third-parties," in *European Symposium on Research in Computer Security*, 2012, pp. 199-216.

[44] A. Ornaghi and M. Valleri, "Man in the middle attacks Demos," *Blackhat [Online Document],* vol. 19, 2003.

[45] S. Gangan, "A review of man-in-the-middle attacks," *arXiv preprint arXiv:1504.02115,* 2015.

[46] J. Belenguer and C. T. Calafate, "A low-cost embedded IDS to monitor and prevent Man-in-the-Middle attacks on wired LAN environments," in *The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007)*, 2007, pp. 122-127.

[47] P. Thermos, "Two attacks against VoIP," *Symantec, Retrieved March,* vol. 13, p. 2011, 2006.

[48] M. Maxim and D. Pollino, *Wireless security*: McGraw-Hill/Osborne, 2002.

[49] X. Gu and R. Hunt, "Wireless LAN attacks and vulnerabilities," *the proceeding of IASTED Networks and Communication Systems,* 2005.

[50] R. Housley and T. Polk, *Planning for PKI: best practices guide for deploying public key infrastructure*: John Wiley & Sons, Inc., 2001.

[51] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Transactions on Smart Grid,* vol. 1, pp. 99-107, 2010.

[52] C. Latze, "Stronger Authentication in E-Commerce-How to protect even naıve Users against Phishing, Pharming, and MITM attacks," *RVS Retreat 2007 at Quarten,* 2007.

[53] I. M. Hegazy, T. Al-Arif, Z. T. Fayed, and H. M. Faheem, "A multi-agent based system for intrusion detection," *IEEE Potentials,* vol. 22, pp. 28-31, 2003.

[54] D. E. Bell and L. J. LaPadula, "Secure computer systems: Mathematical foundations," DTIC Document1973.

[55] T. Y. Lin, "Chinese Wall Security Policy Models: Information Flows and Conflicting Trojan Horses," 2003.

[56] D. F. Brewer and M. J. Nash, "The chinese wall security policy," in *Security and Privacy, 1989. Proceedings., 1989 IEEE Symposium on*, 1989, pp. 206-214.

[57] J. McLean, "Security models and information flow," in *Research in Security and Privacy, 1990. Proceedings., 1990 IEEE Computer Society Symposium on*, 1990, pp. 180-187.

[58] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *computers & security,* vol. 25, pp. 289-296, 2006.

[59] R. S. Shaw, C. C. Chen, A. L. Harris, and H.-J. Huang, "The impact of information richness on information security awareness training effectiveness," *Computers & Education,* vol. 52, pp. 92-100, 2009.

[60] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen, "A video game for cyber security training and awareness," *computers & security,* vol. 26, pp. 63-72, 2007.

[61] C. McCoy and R. T. Fowler, "You are the key to security: establishing a successful security awareness program," in *Proceedings of the 32nd annual ACM SIGUCCS conference on User services*, 2004, pp. 346-349.