Wireless Service at Public University: A Survey of Users Perception on Security Aspects

Arif Ridho Lubis
Department of Computer Engineering and Informatics
Politeknik Negeri Medan
Medan, Indonesia
arifridho@polmed.ac.id

Ferry Fachrizal
Department of Computer Engineering and Informatics
Politeknik Negeri Medan
Medan, Indonesia
ferry_polmed@yahoo.com

Muharman Lubis
School of Industrial Engineering
Telkom University
Bandung, Indonesia
muharman.lubis@gmail.com

Hatim Mohamad Tahir
College of Arts and Science (CAS)
Universiti Utara Malaysia
Kedah, Malaysia hatim@uum.edu.my
hatim@uum.edu.my

***Abstract*—There is an important growth in the application to detect and protect network from the intrusion and unauthorized party as well as create access control among users around the world through this decade. Contextually, the majority of users expected an integrated platform to address the challenges posed by cyber security while also enabling secure access to campus network. Not surprisingly, the large majority of enterprises also have implemented some form of protection mechanism to provide end-to-end security such as firewall, authentication or antivirus, which at some extent it is difficult to design, configure, manage, maintain and monitor. Therefore, many security breaches are occurred because of the misconfiguration resulted the vulnerabilities to be exploited by hackers or caused by compatibility issues between products used in the campus network to reduce budget. Arguably, many security aspects can be strengthen through the improvement of human resource strategy to handle the campus network. This study want to investigate the user perception on security aspect of Wi-Fi performance in Universiti Utara Malaysia to provide some insights on the indicators to be considered by the network administrator.**

***Index Terms*—Wireless, perception, security, strategy.**

I. INTRODUCTION

Currently, any type of information can be shared vastly in split seconds through the internet. Thus, nearly all student activities depend on this tools, such as sending homework through email, downloading presentation slide, browsing for current information about specific topics, opening discussion with fellow student, taking quiz online and other various activities. The existence of wireless service is also quite vital to allow mass connection quickly and easily for the students to use Internet for fulfilling their needs. In addition to Wi-Fi functionality in human routines, the level of Wi-Fi security has become an important point of support to ensure that all activities is protected and prevent damage to the wireless service. Providing strong security mechanism in the wireless network is useful to increase the student satisfaction on wireless service so they can have comfort, calmness, ease, mildness and cosines to finish their task accordingly. In the long run, it can create proudness and loyalty to the institution as the means for them to gather more knowledge and experience. It is also critical to provide filtering mechanism to create sense of belonging to the institution and limit the access free to increase the quality of resource. Moreover, the biggest chal lenges in securing a wireless network is its complexity, capacity, resources and awareness [1][2][3][4]. It is not sufficient to install a firewall, secure passwords and any detailed access control settings if the student installed Trojan incidentally or access scam link coincidentally.

University security strategy and policy is an integral part of any IT implementation with the growing threats to data center and network infrastructures, communications and applications require end-to-end security for maximum protection, although Malaysia has good facilities in term of wireless infrastructure and connectivity [5]. The threat landscape is evolving, in which businesses are heavily reliant on machinery to run the operation [6] creates lack of understanding of the administrator for the fundamental concept and technical detail in network. With the dynamics of an unrelenting increase in number and type of networked devices, IT decision-makers believe their WLANs are exposed in the environment [7]. Despite implementation of a broad range of security measures, wireless LAN infrastructure and access are considered to be at the greatest risk to security breaches. The wireless approach shows many advantages but also has some disadvantages with respect to cabled networks. Mobility is clearly one of the major advantages of wireless with respect to cabled devices, which require plugging. Another advantage lies in the way that the users can dynamically join or leave the network, move among different environments, create ad hoc networks for a limited time, and then leave. It is also simple to deploy and provide cost less than wired LANs at certain context. Nevertheless, the technological challenges involved in wireless networks are not trivial such as lower reliability due to interference, higher power consumption, data security threats due to the inherent broadcast properties of the radio medium, user privacy on personal detail due to continued exposition and lower data rates. This study explore the student perception about the quality of security measurement to align with the human factor consideration and campus policy.

978-1-5386-0954-5/18/$31.00 ©2018 IEEE

II. Literature Review

Generally, wireless technology can be classified into two categories that is based on mobile devices, which is a solution that uses existing cellular communication or paging lines to transmit data (GSM, CDMA, TDMA, CDPD, GPRS/EDGE, 2G, 2.5 G, 3G, UMTS) and wireless communications, which provides ubiquitous characteristics within a limited area, usually between 10-100 meters from the base station to the Access Point (AP). Vulnerability in wireless networks can be grouped into 2 (two) types of attacks, that is, passive and active attacks [8][9][10][11]. Wireless systems have security problems specifically related to the physical attributes, which might affect the security aspects, such the small size and shape that is making it easy to steal or damage. If it is stolen, the information contained or access to critical information may fall into the hands of unauthorized person [12]. Meanwhile, to perform a man attack in the middle in the communication line also can be done more easily because there is no need to look for cable lines. Systems that do not use security encryption and authentication, or use non-standard encryption might be easily modified or manipulated as indicated by the number frequency increases annually [1]. Of the three common security approaches in the wireless service are WEP, WPA and WPA2, but it is not ensure a complete guarantee for protection [13].

According to the ITU [14], the population of mobile users are approximately 6.8 billion worldwide in 2013 while around half population is Internet users. Meanwhile, it has been reported [15][16] that more and more wireless devices are being harassed for cybercrimes or spam, including malicious attacks, hacking, data manipulation, cyber bullying, cyber stalking, information theft and so on. It causes a direct loss of about 83 billion euros with an estimated 556 million users worldwide impacted by several type of cybercrime each year. In general, secure wireless communications should satisfy the requirements of authenticity, confidentiality, integrity and availability [17]. Actually, using WPA is more robust data encryption called temporal key integrity protocol (TKIP) compare to WEP, which is assisted by a message integrity check (MIC) attached to preserve data integrity and confidentiality of Wi-Fi networks [18].

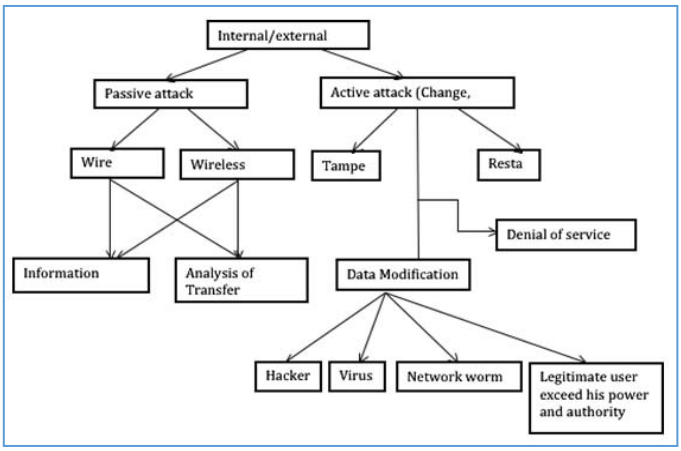

Fig. 1: Type of Network Attacks

In recent years, identity theft has become one of the fastest growing crimes, where the Internet has facilitated this phenomenon, as it is it is an exceptional open access and easy to track confidential information from specific user because its availability in various social media application for those who understand on how to look for them. These attempts to store multiple user identities has certain objective such as spoofing, DDOS, social engineering or fraudulent applications that might inflict great damage to economic, social status, reputation of related users or groups [9]. Therefore data management has long been considered as the main source for an infrastructure problem for IT, which is not limited to the approach used to control but also in ethics and standards [4]. The reality is that data management is the key to success in almost all IT adoptions as sustainable operations with risk management and maintenance [19]. However, some internal problems can create vulnerabilities that allow for the possibility of security attacks such as data accuracy problems, metadata, data changes, data integration, and agent integration [20] that should be anticipated to avoid vulnerabilities in campus security. Therefore, the institution can focus on the development of a security policy to encourage internal resources to obtain an adequate response to avoid security incidents [4]. It also can be through improving the reliability of the communication link by increasing the sources transmit power or decreasing its date rate in quality of service configuration to reduce the outage probability [21]. Moreover, by providing cooperation in the physical layer security with secrecy signaling and coding schemes might guarantee confidentiality against information leakage [22].

The basis of information security in an organization is the security policy where it has to be well developed, enforced and complied with the organization's internal and external business processes [23]. The nature of physical layer of wireless channels have tendency to be exploited by modifying the upper-layer security algorithms, involving the identity authentication or key generation. In term of secrecy, the eavesdroppers may be severely degraded the wireless communication in relation to the time-varying multipath fading effects, which can be mitigated through utilizing a range of diversity-aided techniques, such as frequency, time and spatial diversity [24]. Meanwhile, in network security, there are several issues such as very poor encryption facilities, ineffective physical security, efficient operation of wireless networks depends on coordinated management of the available spectrum and maintaining network security is potentially difficult because any network device can listen to network traffic for any other network device in range due to broadcast signal [25]. Moreover, the intention of having security policy was not to persuade users but to convince them, by letting the users reflect, on their own terms, on why information security is important and on how to react in certain circumstances [4].

III. Research Methodology

This study used quantitative method by using survey questionnaire as data collection method and statistics for data analysis include descriptive, inter item total, reliability and correlation. It has two type variables namely user perception as independent variables and security aspects as dependent variables. Meanwhile, user characteristics also identified to

categorize several items belong to certain group that are similar with. There were five stages generated for the purpose of this research namely problem statement, design structure, pilot study, final survey and result treatment. The type of data to be collected is nominal in user characteristics and ordinal in user perception and security aspects with 5 likert scale. To determine the amount of sample, a standard monogram is applied [26], in which the population in SOC buildings are 873 people with a confidence level of 8%, thus the total sample is 12% of the total population. Consequently, 12% x 873 = 105 people, in which total 109 people selected in this case. Researcher choose Universiti Utara Malaysia as target location, which focus on SOC building. The map layout are provided to the respondent to show them on how the communication work in wireless services, so they can understand the basic concept of security.

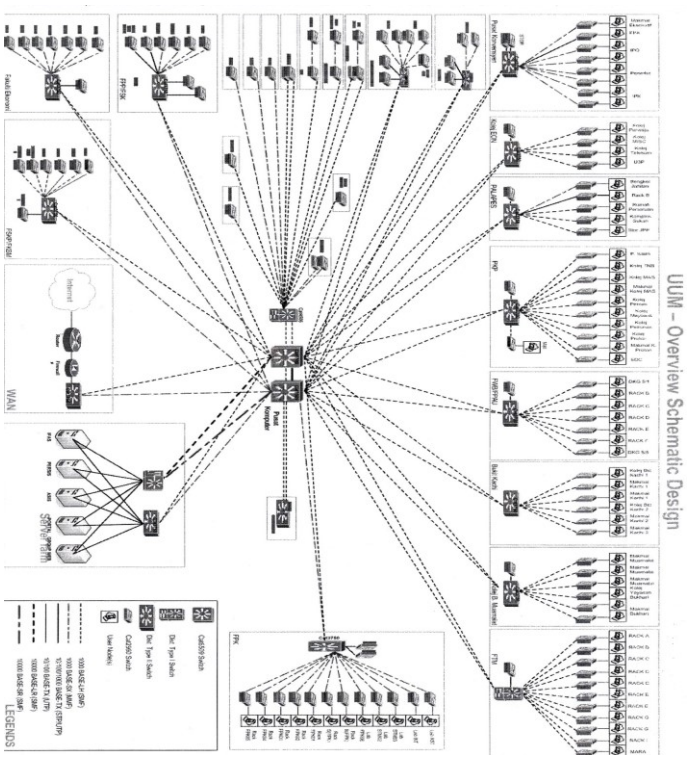

Fig. 2: Network layout in Universiti Utara Malaysia

As we can see from figure 2, it showed the network topology used is three-layer hierarchy consist of core (backbone), distribution (workgroup) and access (desktop) layer switch. There are around 23 rooms with their own access switches have been served by 6 distribution switches in computer center office. By having this kind of layout, it is expected the campus network will have high performance, efficient management and troubleshooting, scalability, redundancy link, link aggregation quality of service, policy creation manageability, maintainability, behavior prediction and security. Arguably, the network layout has much influence over the security, protection of the data and even the performance or the quality of service, which the servers' location with supported firewall and several computers can give significant impact. This study investigate the security aspects in relation to the mapping of layout, the structure used, the type device utilized to perform communication network and type of service to be provided by public university. Meanwhile, user perception consider various criteria related to awareness, satisfaction, understanding and readiness to anticipate security threats or prevent unauthorized access over their own laptops or devices.

IV. Discussion and Results

Security issues are worsened by the fact that nearly all applications do not use secure mechanism such as encryption to connect to the Internet. Actually, if the apps do not implement the correct end-to-end encryption, certain party can look at or monitor data sent easily on an insecure Wi-Fi network [27]. Meanwhile, many WiFi hotspot users also are unaware of the hidden risks posed by the technology, like scamming and compromised accounts [28]. The availability of low-cost equipment also gives attackers the tools to launch attacks against networks that exploit design flaws in the 802.11 standard security mechanisms, both passive and active [29] such as malicious twins, media people, malware, data theft, parking attacks, attacks on temporary key integrity protocols, exploits in shared key authentication and failure to identify assigned services [30].

TABLE I
Units for Security Properties

Attack	On	Solved By
Interception	Confidentiality and privacy.	Encryption / Decryption.
Fabrication	Authenticity.	Authentication.
Modification Replay Reaction	Integrity.	Digital signatures on every message.
Interruption	Availability.	No effective solutions exist for interruption / Denial of Service attacks on availability.
Repudiation	No repudiation.	Non-repudiation currently still suffers of cases of identity theft.

TABLE II
Top Previous Attack in Universiti Utara Malaysia

Top Attacks				
Attack ID	Description	Detail	Events	% of Total
17677	TCP.Out.Of.Range.Timestamp	http://www.fortinet.com/ids/ID17677	31897	93.60
107937793	TCP.Bad.Flags	http://www.fortinet.com/ids/ID107937793	1526	4.48
12699	PHP.Remote.File.Inclusion	http://www.fortinet.com/ids/ID12699	267	0.78
107347978	HTTP.Negative.Data.Length	http://www.fortinet.com/ids/ID107347978	172	0.50
108658691	TCP.Bad.Option.Length	http://www.fortinet.com/ids/ID108658691	110	0.32
107347976	HTTP.Chunk.Overflow	http://www.fortinet.com/ids/ID107347976	61	0.18
16777320	icmp_sweep	http://www.fortinet.com/ids/ID16777320	17	0.05
10756	Working.Resources.Badblue.Malformed.HTTP.DoS	http://www.fortinet.com/ids/ID10756	11	0.03
16777316	icmp_flood	http://www.fortinet.com/ids/ID16777316	4	0.01
10577	MS.IE.File.Request.Zone.Bypass	http://www.fortinet.com/ids/ID10577	4	0.01
107347981	HTTP.Unknown.Tunnelling	http://www.fortinet.com/ids/ID107347981	3	0.01
17806	MS.Windows.Media.Player.Code.Execution	http://www.fortinet.com/ids/ID17806	2	0.01
13448	Mozilla.Firefox.Chrome.Page.Loading.Restriction.Bypass	http://www.fortinet.com/ids/ID13448	2	0.01
20780	MS.IE.Incomplete.Element.Memory.Corruption	http://www.fortinet.com/ids/ID20780	1	0.00
14228	HTTP.Malicious.Request.Double.Slash	http://www.fortinet.com/ids/ID14228	1	0.00
Total			34078	100.00

The network attacked is not necessary create harm to the network directly such as damaging the physical device or slowing the performance, but also take full or partial control and access over part of network indirectly such as through data manipulation or compromised integrity. Based on table 2, it

indicated that TCP.Out.Of.Range.Timestampt signature became the majority attempts to attack the campus network (93.6%), in which firewall block effectively the evasion by drop all subsequent packets after an effort to send duplicate packets with differing TCP timestamps is detected. Interestingly, it can be understood as test water from certain user or party to evaluate the security performance of certain campus network, either to find the vulnerabilities or configuration error. Then, TCP.Bad.Flags signature (4.48%) indicates the detection of a TCP packet with an abnormal flag setting with the following bits set are considered past of reconnaissance activities to allow other attacks such as FIN flag set only, both SYN and FIN flags set, all of the control bits or none of the control bits. The least threat attempt is HTTP.Malicious.Request.Double.Slash that want to crash any webserver. Fortunately, around 34.078 attack attempts have been detected by firewall in the campus network, but there are also indication small amount of network attack cannot be identified, detected or traced by bypassing operators altogether to build their own peer-to-peer network connecting through data networks or by pumping their own traffic over other operators networks. Password is the only one measures in the security measures, changing password regularly through policy awareness is one way of slowing down hackers and fraudster but many measures should be implemented to protect campus network further. Indeed, any security strategy, which is implemented by campus should be kept hidden to avoid the information used to scan the weaknesses.

A. Demographics

Based on table 3 in the demographic table for user characteristics, the majority users are undergraduate (82.56%), browse Internet every day (93.57%) with surfing time more than 4 hours (32.11%), in which they perceive that bad weather and loss of signal in the airwaves can be the condition for security breach (28.44). Then, they think that the type of OS used as the high possible cause for wifi attacked (16.82%) with firewall as the effective method to protect campus network and internal device under for various attempt of network attacks.

TABLE III
User Characteristics in Universiti Utara Malaysia

Internet Use	Freq.	Surfing Time	Freq.
Every Day	102 (93.57)	> 4 hours	35 (32.11)
Once a week	2 (1.83)	3 hours	26 (23.85)
More than once a week	5 (2.58)	2 hours	25 (22.93)
Never	0 (0)	1 hours	23 (21.10)
Security Breaches	**Freq.**	**Possible Causes**	**Freq.**
Bad weather and loss of signal in the air waves	62 (28.44)	The type of OS used	34 (16.82)
Lack of supporting safe techologies	43 (19.72)	A modem laptop	33 (16.33)
Hardware that overhat	12 (5.5)	Using a VPN tunnel client	10 (4.95)
Bad overall security policy	20 (9.17)	An encrypted connection WEP	19 (9.40)
Old computer model	15 (6.88)	An encrypted connection WAP	13 (6.43)
A hardware problem	20 (9.17)	Connecting from the university wireless	31 (15.34)
The miss-configuration of the network	36 (16.51)	Authentication and authorization issues	54 (26.73)
I do not know	10 (4.58)	I don't know	8 (3.96)
Effective Protection	**Freq.**	**Attack type**	**Freq.**
Firewall	59 (28.09)	Virus/Malware	89 (45.64)
Biometrics	3 (1.42)	Email spam	63 (32.30)
IDS	9 (4.28)	Hacking/DoS	22 (11.28)
VPN	25 (11.90)	Web phishing/fraud	21 (10.76)
Antivirus	72 (34.28)	**Qualification**	**Freq.**
Proxy	32 (15.23)	Undergraduate	90 (82.56)
I do not know	10 (4.76)	Postgraduate	19 (17.44)

B. Reliability Analysis

In general, there are two variables to be investigated namely users perception involves understanding, connectivity changes, speed, quality of signal, download, protection trust, customer needs, attacked experience, security threats. Then, security aspects involves self-awareness, data content, suspicious avoidance, financial transaction, self-worries, efficiency, identification, firewall, intrusion detection system, security risk, signature, confidentiality, virtual private network (VPN), and non-repudiation. The results showed internal consistency is good, which indicate that the item measurement used between the user aspect and security aspect is produced different score. In the descriptive analysis, value for the user aspect is 1.67 minimum, maximum 4.33, the mean 0.546 with standard of deviation 3.083, while the security aspect at minimum 1.57, maximum 4.43, mean 3.22 with standard of deviation is 0.431. Because the reliability coefficient of user perception (0.786) and security aspect (0.765) is higher than 0.70, so it is considered as acceptable and suggesting that the items used have high internal consistency.

TABLE IV
Cronbach's Alpha

Cronbach's Alpha	N of Items	Mean	Standard Deviation
0.786	9 (User Perception)	3.0826	0.54693
0.765	14 (Security Aspect)	3.2202	0.43057

C. Correlation Analysis

Correlations analysis is applied to look the relationship strength between two variables, by looking at the Pearson Correlation who has provided one-tailed significance value and must be smaller than 0.01. The table showed that the correlations between the user aspects to the security aspect are significant correlated because they meet the required criteria.

TABLE V
Pearson Correlation

		User Perception	Security Aspect
User Aspect	Pearson Correlation	1	.561**
	Sig. (1-tailed)		.000
	N	109	109
Security Aspect	Pearson Correlation	.561**	1
	Sig. (1-tailed)	.000	
	N	109	109

D. Item-Total Analysis

An item-total correlation test is conducted to validate if any item in the test set is inconsistent with the averaged behavior of the others and thus can be discarded. Values for an item-total correlation between 0 and 0.19 may indicate that the question is not well discriminated, values between 0.2 and 0.39 indicate good discrimination and values 0.4 and above indicate excellent discrimination. From the table 6, it showed that most of items is consistent and do not overlap between each other indicated by score that close and higher than 0.2 so the analysis determine that the item represent the respected variables, except one item (sa11=0.194) but it can be tolerated.

TABLE VI
Security Aspects Scale

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
sa1	58.7333	162.924	.604	.917
sa2	58.1333	168.981	.445	.921
sa3	59.0000	164.714	.420	.922
sa4	59.2667	153.781	.657	.916
sa5	59.0667	150.495	.636	.918
sa6	59.4000	155.257	.602	.918
sa7	59.4000	156.686	.608	.917
sa8	59.0667	162.067	.529	.919
sa9	58.6000	162.114	.739	.915
sa10	59.2000	159.314	.808	.913
sa11	58.8000	176.457	.194	.924
sa12	59.0667	161.352	.666	.916
sa13	58.9333	160.781	.651	.916
sa14	58.9333	150.495	.891	.909
sa15	58.6000	165.543	.588	.918
sa16	58.6667	157.381	.847	.911
sa17	58.7333	161.638	.706	.915

TABLE VII
User Perception Scale

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
ua1	24.2936	19.654	.406	.775
ua2	24.3945	18.871	.543	.754
ua3	24.8716	18.669	.617	.744
ua4	24.7523	19.207	.536	.756
ua5	24.9083	18.843	.538	.755
ua6	24.7064	20.172	.351	.783
ua7	24.6972	19.657	.536	.757
ua8	24.8899	20.803	.343	.782
ua9	24.4312	21.044	.397	.775

V. CONCLUSION

This study presented that majority students in University Utara Malaysia have good perception on various security aspects in the campus network. At some extent, the perception can provide good initial step to produce and implement security measures as campus policy in security assurance. Although there are number of steps need to be done to verify and validate the strategy to guarantee the protection have been met with standard as well as maintain good quality in term of performance and management.

REFERENCES

[1] Kapetanovic D, Zheng G and Rusek F. "Physical layer security for massive MIMO: an overview on passive eavesdropping and active attacks". IEEE Communications Magazine vol. 53 (6), pp. 21-27, 10 June 2015.

[2] Zhao N, Yu FR, Jin M, Yan Q and Leung VCM. "Interference alignment and its applications: a survey, research issues and challenges". IEEE Communications Surveys & Tutorials, vol. 18 (3), pp. 1779-1803, 28 March 2016.

[3] Trappe W. "The challenges facing physical layer security". IEEE Communications Magazines, vol. 53 (6), pp. 16-20, 10 June 2015.

[4] Ahlan A, Lubis M. and Lubis, A.R. "Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures". *Procedia Computer Science*, vol. 72, pp. 361–373.

[5] Kamaruddin KK and Md Noor NL. "From E-Government to T-Government: A Malaysia Citizens' Readiness Study". *Journal of Telecommunication, Electronic and Computer Engineering* 2017, vol. 9, no. 2-9, pp. 15–21.

[6] Abu Bakar MS, Jalil D and Udin ZM. "Knowledge Repository: Implementing Learning Management System into Corporate Environment". *Journal of Telecommunication, Electronic and Computer Engineering* 2017, vol. 9, no. 2-12, pp. 141–145.

[7] Barakovic S, Kurtovic E, Bozanovic O, Mirojevic, Ljevakovic S, Jokic A, Peranovic and Husic JB. "Security issues in wireless network: an overview". 2016 *IEEE International Symposium on Telecommunication*.

[8] Arief MR. "Wireless Security." STMIK AMIKOM, 2009. Retrieved from http://dosen.amikom.ac.id/downloads/artikel/2009/11/20091115_WIRELESS%20SECURITY.pdf

[9] Lubis, M. Ibtisam bt. Yaacob N, Hafizah bt. Reh and Abdulghani MA. "Study on Implementation and Impact of Google Hacking in Internet Security". *Proceedings of Regional Conference on Knowledge Integration in ICT 2010*.

[10] Abdelhalim, A. and Traore I. "The Impact of Google Hacking on Identity and Application Fraud". PACRIM'07.

[11] Pawar MV and Anuradha J. "Network security and types of attacks in network". Procedia Computer Science vol. 48 (2015) pp. 503-506.

[12] Lashkari AH, Mansoori M and Danesh AS. "Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access", 2009 *International Conference on Signal Processing System*, pp 445-449.

[13] Dushuqin and Qin Yi, "WLAN Security System based on the 802.1 & AES" *International Conference on Computer Application & System Modeling (ICCASM),* 2010.

[14] ITU. "The world in 2013: ICT facts and figures," January 2013, available on-line at http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf

[15] Symantec Norton Department. "The 2012 Norton cybercrime report," September 2012, available on-line at http://www.norton.com/2012cybercrimereport.

[16] Mohamed SFP, Ku-Mahamud KR, Ramli R and Abdullah K. "Perception and Use of e-Mail: A Case Study in Universiti Utara Malaysia". *Journal of Telecommunication, Electronic and Computer Engineering* 2017, vol. 9, no. 2-12, pp. 29–35.

[17] Shiu YS, Chang SY, Wu HC, Huang SC-H and Chen HH. "Physical layer security in wireless networks: A tutorial." *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, April 2011.

[18] Tews E and Beck M. "Practical attacks against WEP and WPA." Proceedings of the Second *ACM Conference on Wireless Network Security* (ACM WiSec), Zurich, Switzerland, March 2009.

[19] Lubis M, Kartiwi M. and Zulhuda S. "A Guideline to Enforce Privacy and Data Protection Regulation in Indonesia". *Proceedings Kuala Lumpur International Business, Economics and Law Conferences*, pp. 231–243.

[20] Ibtisam bt. Yaacob N. and Lubis M. "Data Accuracy and Agent Integration in Executive Information System: A Case Study in KUIS". IIUM Press. Kuala Lumpur. ISBN 9789674180843 in Kartiwi, Mira and M.Z.M Khedher, Akram, eds. (2011) Data management: issues, challenges and opportunities.

[21] Zou Y, Wang X, Shen W and Hanzo L. "Security versus reliability analysis of opportunistic relaying". IEEE Transactions on Vehicular Technology, vol. 63 (6), July 2014. Pp. 2653-2661.
[22] Wang HM and Xia XG. "Enhancing wireless secrecy via cooperation: signal design and optimization". IEEE Communications Magazine, vol. 53 (12), pp. 47-53, 17 December 2015.
[23] Abdul Kadir M.R., Norman S.N.S., Abdul Rahman S, Ahmad A. and Bunawan A. "Information Security Policies Compliance among Employees in Cybersecurity Malaysia". *Innovation Management and Education Excellence Vision 2020: Regional Development to Global Economic Growth*. pp 2419–2430.
[24] Zhou Y, Zhu J, Wang X and Hanzo L. "A Survey on Wireless Security: Technical Challnges, Recent Advances and Future Trend". *Proceedings of the IEEE* vol. 104, issues 9, September 2016.
[25] Sandhu GK, Mann GS and Kaur R. "Benefit and security issues in wireless technologies: Wi-fi and WiMax". *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 1, Issue 4, June 2013, pp. 976–982. ISSN 2320-9801.
[26] Idrus M. "Metode Penelitian Ilmu Social Pendekatan Kualitatif Dam Kuantitatif Edisi Kedua". Jakarta: Penerbit Erlangga, 2012.
[27] Bonne B, Rovelo G, Quax P and Lamotte W. "Insecure Network, Unknown Connection: Understanding Wi-Fi Privacy Assumption of Mobile Device Users". *Information* 2017, vol. 8 issue 76.
[28] Private Wifi. "The Hidden Dangers of Public Wifi". *White Paper*. October 2014.
[29] HKSAR. "Wireless Networking Security". Dec 2010. Retrieved from https://www.infosec.gov.hk/english/technical/files/wireless.pdf
[30] Zimeng H. "Security of Mobile Devices and Wi-Fi Networks". *Bachelor's Thesis*, May 2015. Mikkeli University of Applied Science.