I.J. Wireless and Microwave Technologies, **2020, 6, 27-35**
Published Online December 2020 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2020.06.04

A Metric for Evaluating Security Models based on Implementation of Public Key Infrastructure

Sigsbert Rwiza and Mussa Kissaka
University of Dar es Salaam, College of Information and Communication Technologies, Department of Electronics and Telecommunications Engineering, Dar es Salaam, 255, Tanzania
Email: rwiza2010@yahoo.com, mkissaka@yahoo.com

Kosmas Kapis
University of Dar es Salaam, College of Information and Communication Technologies, Department of Computer Science and Engineering, Dar es Salaam, 255, Tanzania
Email: kkapis@gmail.com

Received: 19 July 2020; Accepted: 28 October 2020; Published: 08 December 2020

Abstract: International security evaluation metrics are too general and not focused on evaluating security models implemented using Public Key Infrastructure (PKI). This study was conducted to develop the metric for evaluating security models based on implementation of PKI by using insights from literature. Literature review was done based on inclusion and exclusion criteria. The developed metric was tested using ranking attributes and ranking scales. The results reveal that the developed metric is applicable for evaluating security models based on implementation of PKI. This is verified by the tabular results indicating evaluation of selected security models based on implementation of PKI by using ranking attributes and ranking scales. This study contributes to the body of knowledge a metric for evaluating security models based on implementation of PKI.

Index Terms: Metric, Security Models, PKI, Implementation, Evaluating

1. Introduction

Security models developed based on implementation of PKI are strong due to the fact that PKI is designed to enforce integrity, confidentiality, authentication and non-repudiation security mechanisms. Previous studies have developed security models based on enhancement of existing models; however, in such studies, a metric for evaluating security models is not clearly presented [1,2]. Without such metric it is not easy to tell how a particular security model is better than the other in terms of enforcement of security mechanisms.

A Metric for evaluating security models based on implementation of PKI is appropriate for organizations in choosing the right security model as a basis for developing secure information systems. Hence, before a security model is developed, a metric for evaluating existing ones would assist organizations in choosing appropriate security models to adapt in developing security models to serve the purpose of their information security objectives.

The United States (US) National Institute of Standards and Technology (NIST) proposes security metrics in evaluating security models; the Center for Internet Security (CIS) defined twenty eight security metrics in management, operational, and technical aspects of a system. However, these efforts are exclusively geared towards cyber defense administrations and operations. To the best of our knowledge, there has been little discussion on how security metrics may be used as parameters in evaluating security models based on implementation of PKI [3].

In our previous work, we developed the methodology for evaluating security in MNO financial service model [4], the outcome of which was the establishment of security requirements for developing a secure MNO financial service model. The previous work motivates us to investigate on the metric for evaluating security models based on implementation of PKI as a further strategy for establishing security requirements in developing security models. Hence, this study is motivated by our previous work as the strategy for establishing security requirements for developing secure models and secure information systems.

This study was conducted to develop the metric for evaluating security models based on implementation of PKI and to test the developed metric in evaluating security models. To achieve such objectives, this paper is organized in five sections. Section one is the introduction explaining on research problem, objectives and motivation of the study. Section two elaborates on metrics for evaluating security models. Section three describes the methodology applied in the study for achieving the research objectives. Section four presents results and discussions on the study. Section five

sums up on the conclusions and recommendations of the study. We, de facto, realize that this paper contributes to the body of knowledge a metric for evaluating security models based on implementation of PKI.

2. Related Works

Security metrics refer to assigning values to security objects for quantifying security attributes such as strong, excellent, good, fair or poor. How to develop security metrics has been identified as one of the hard problems by many key organizations [3]. Literature indicates that security metrics assist in evaluating security of information systems. In some of the organizations, security in information systems is implemented using Public Key Infrastructure (PKI). PKI handles public key management and solves the weaknesses existing in symmetric encryption [5]. Unlike symmetric encryption, in which the secret key is vulnerable to exposure, PKI uses private and public keys; the sender and receiver of data both have private and public keys and hence there is no need of sharing keys [6]. As far as encryption is concerned, the sender of data encrypts the data using the public key of the receiver and the receiver of the data decrypts the data using his private key. PKI is used to enforce integrity, confidentiality, authentication and non-repudiation security mechanisms. Hence, PKI is used to implement encryption, hashing, digital signatures and digital certificates [5].

In PKI, there is Certificate Authority (CA) that issues certificates to entities participating in the communication. Certificates are issued, renewed and revoked [7]. The use of certificates validates entities participating in the communication; hence certificates enforce authentication security mechanisms [8]. Private and public keys in PKI are used to enforce encryption of data. The use of digital signatures in PKI enforces non-repudiation [9]. The use of hashing algorithms in PKI enforces data integrity [10]. PKI may be implemented at the institutional or national level using certificate authorities and security protocols. One way of implementing PKI is by using CA. To secure data in transit from one point to the other, Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols are implemented using PKI. In the implementation of TLS protocol using PKI, systems validate each other using TLS handshake protocol; encryption is enforced using private and public keys; hashing takes place in the record layer protocol and is enforced using Hash-based Message Authentication Code (HMAC) function [11].

Security models enforce at least one of the four security mechanisms namely hashing for integrity, encryption for confidentiality, digital certificates for authentication and digital signatures for non-repudiation security services [12]. Security service is enforced using cryptographic algorithms. However, the security models implemented using PKI, are more trusted in terms of security strengths [13]. They are used in developing secure information systems in which integrity, confidentiality, authentication and non-repudiation security mechanisms are enforced [14].

Security models are evaluated before they are used in developing systems. Security metrics are used to evaluate security models. Several empirical studies have investigated on security models as guidelines for developing secure information systems [12,15]. Such studies elaborate on the performance of such security models with reference to other models that are insecure based on improvements performed in developed models. In the context of this work, a metric is a standard of measurement for ranking security services in security models and serves as a criteria for analyzing performance of a secure model [16].

Secure models are information system frameworks and architectures accompanied by descriptive guidelines for explaining the applied security mechanisms. Most security models are developed based on application of cryptographic mechanisms.

One way of implementing cryptographic mechanisms is by using PKI to enforce integrity, confidentiality, authentication and non-repudiation security mechanisms [17]. Security models that are developed based on implementation of PKI use asymmetric encryption in which public and private key pairs are used to enforce confidentiality security mechanisms [18]. Asymmetric encryption though superior to symmetric encryption in terms of security performance, has high overheads in execution speed due to high computation resources required in security algorithms for enforcing encryption, hashing, digital signatures and digital certificates.

The study by [19] investigates on metrics for information security vulnerabilities referred to as CVSS (Common Vulnerability Scoring System) which provides a tool to quantify the severity and risk of a vulnerability to an information asset in a computing environment. The few criteria for a good metric mainly objectiveness, repeatability, clarity and easiness are covered. CVSS provides a simple tool to define information system vulnerabilities reflecting the overall severity and risk presented by those vulnerabilities. The study provides the quantitative metric that is measurable and that reduces subjective nature of security metrics. This study has implication to this research since it provides a metric for quantifying security vulnerabilities. The quantification process is adapted to develop the metric for evaluating security models. Although the metric offers the criteria for a good security metric, it does not show how implementation of PKI in a security model that can be measured to address enforcement of integrity, confidentiality, authentication and non-repudiation security mechanisms.

The security metrics for the android ecosystem by [19] measures vulnerabilities in android devices based on the updates provided by manufacturers to android devices. The metric is applied to select the secure devices based on the patching history of those devices and thus helping users of android based devices to choose the better devices in terms of security. Likewise, this study has implication to this research since it provides a metric for quantifying security vulnerabilities. The quantification process is adapted to develop the metric for evaluating security models. The

presented metric is quantifiable and has good attributes of objectiveness, repeatability, clarity and easiness; however, it does not present ranking attributes and ranking scales that would be used to evaluate security models based on implementation of PKI for enforcing integrity, confidentiality, authentication and non-repudiation security mechanisms.

There are guiding standards of security metrics such as the Federal Information Processing Standard Publication (FIPS) 140-1/2, Information Technology Security Evaluation Criteria (ITSEC), Trusted Computer System Evaluation Criteria (TCSEC), Common Criteria (CC) and National Institute of Standards and Technology (NIST) Special Publication 800-55. Such security standards are widely used; however, they are too broad and without precise definitions. They do not provide inputs for developing and testing metric for evaluating security models based on implementation of PKI to enforce integrity, confidentiality, authentication and non-repudiation security mechanisms [20].

The information security standard published jointly by International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) (ISO/IEC 27004) helps organizations to evaluate the effectiveness and efficiency of their ISO 27000 Information Security Management Systems (ISMS) by providing information necessary to manage and improve the ISMS systematically [21]. ISO/IEC 27004 provides guidelines intended to assist organizations in evaluating the information security performance and the effectiveness of an information security management system in order to fulfill the requirements of ISO/IEC 27001. It establishes: (i) the monitoring and measurement of information security performance (ii) the monitoring and measurement of the effectiveness of an information security management system (ISMS) including its processes and controls (iii) the analysis and evaluation of the results of monitoring and measurement. ISO/IEC 27004 assumes that the organization has performed information security risk assessment in accordance with ISO/IEC 27005 and is aware of the information security risks it has to deal with when developing measures and initiating measurement [21]. However, ISO/IEC 27004 standard does not provide specific information that would form a metric to evaluate security models based on implementation of PKI to enforce integrity, confidentiality, authentication and non-repudiation security mechanisms.

3. Methodology

The methods employed in this study are based on insights from literature. The insights from literature provide evidence on the lack of appropriate metric for evaluating security models based on implementation of PKI. They provide appropriate quantification processes in developing security metric. This helps to achieve research objectives which are mainly developing and testing security metric. In developing the metric for evaluating security models, we conducted literature review to identify studies focusing on security metrics and evaluation of security metrics [22]. We further used literature review to select security models available for testing the developed security metric. Studies were selected based on defined inclusion and exclusion criteria. Including or excluding literature in the study was based on titles and abstracts of selected studies.

A. Developing the Metric for Evaluating Security Models

The metric was developed based on three processes for evaluating security in MNO financial service model as adapted from [4]. As indicated in Figure 1, the three processes are establishing security context, performing security threat analysis and establishing security strengths and weaknesses.

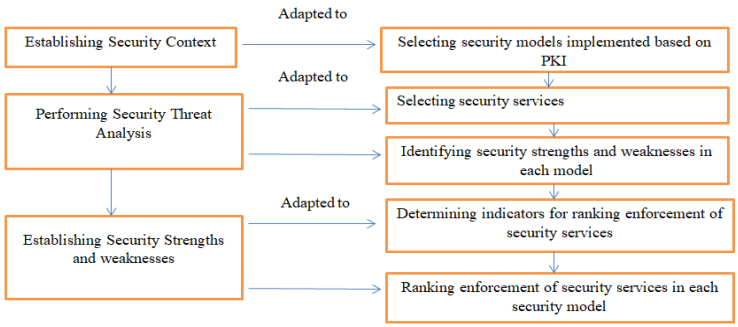

Fig. 1. Methodology for developing the Metric [20]

Establishing the context was adapted to selecting security models implemented based on implementation of PKI due to the fact that PKI enforces all the key security services covering integrity, confidentiality, authentication and non-repudiation security services. The process for performing security threat analysis was adapted to two processes namely selecting security services and identifying security strengths and weaknesses in each model. The process for establishing security strengths and weaknesses was adapted to determining indicators for ranking enforcement of security services and ranking enforcement of security services in each security model. As indicated in Figure 2, the

workflow for developing the metric to evaluate security models consists of three parts; namely, the input activities, intermediate output and the output.

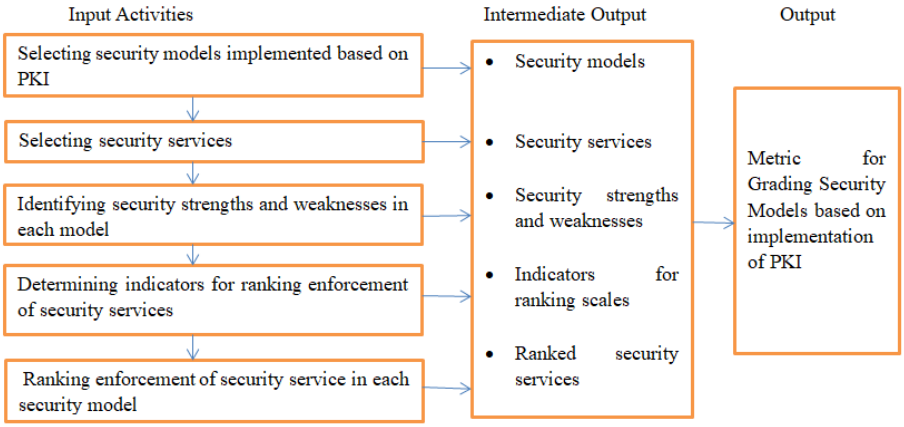

Fig.2. Workflow for developing the Metric to evaluate security models

Each input activity has the intermediate output. For instance, the intermediate output for the input activity "select security models implemented based on PKI" is security models. Other intermediate outputs are security services, security strengths and weaknesses, indicators for ranking scales and ranked security models. The output for all the input activities is the metric for evaluating security models based on implementation of PKI. The workflow for developing the metric to evaluate security models has five processes which are expounded hereunder.

(i) Selecting security models implemented using PKI

In selecting literature to review, two criteria were used namely; the nature of the research problem and the experience of the researcher as adapted from [23]. As far as the research problem was concerned literature dealing with security models were selected. Secondly, the authors selected papers that were related to their previous work on the methodology for evaluating security in MNO financial service model [4]. Out of 160 information security models reviewed only 4 security models were developed based on PKI. The 4 security models were obtained based on literature reduction process as adapted from [22].

(ii) Selecting security services

PKI implementation differs among organizations whereas one organization may use Secure Socket Layer (SSL) to implement PKI in order to achieve authentication and confidentiality security services, the other organization may use Transport Layer Security (TLS) protocol to enforce integrity and non-repudiation security services. Based on security models by [1,2,12,14], integrity, confidentiality, authentication and non-repudiation security services were selected as security performance evaluation criteria.

(iii) Identifying security strengths and weaknesses in each model

Reviewed security models were implemented using encryption, hashing, digital certificates and digital signatures for achieving confidentiality, integrity, authentication and non-repudiation security mechanisms. Security strengths were identified by noting availability of appropriate security mechanisms in reviewed models; for instance, hashing and encryption algorithms. Security weaknesses were identified by noting encryption and hashing algorithms that are already cracked in selected security models. Security weaknesses were also determined through identification of security vulnerabilities due to lack of PKI implementation in organizations for enforcing security mechanisms. Security strengths for the 4 selected models are summarized in Table 1.

Table 1. Security Strengths and Weaknesses in Selected Security Models

S/N	Selected Security Models	Strength(s)	Weakness(s)
1.	Enhanced Security Model for Mobile banking Systems in Tanzania	• Uses AES symmetric cipher for encrypting data to provide confidentiality while targeting users of mobile phones with low memory capacity that cannot support high overheads. • Uses asymmetric encryption for sharing the secret key between the client application and the bank server	Does not use PKI to enforce encryption.
		Improved authentication from a 4 digits PIN to a PIN consisting various characters, letters and numbers	Does not use PKI to enforce authentication; for instance by using digital certificates
		Provides non-repudiation using encryption / decryption key for users transacting from the client application to the bank application server	Does not use PKI to enforce non-repudiation; for instance by using digital signatures.
2.	Proposed SMS Banking Secure Model	Provides data integrity by using both symmetric encryption and hash algorithms	Does not use PKI to enforce integrity security service.
		Provide confidentiality of data using symmetric encryption due to most of users using mobile phone with low memory capacity	Does not use PKI to enforce data confidentiality.
		Provide authentication of users using PINs and account numbers	Does not use PKI to enable participating systems validate each other
		Provides non-repudiation through the use of the PIN, one time password and sequence number that are known only to the client and the bank.	Does not use PKI to enforce digital signatures for achieving non-repudiation
3.	Enhancing Security and Privacy in Traffic-Monitoring Systems	Provides data integrity using keyed hash function. Other security models have used Keyed hash function [Hash-based Message Authentication Code-(HMAC)] to implement PKI using TLS protocol for achieving both integrity and authentication security services in the communication channel.	Does not use PKI to enforce data integrity
		Ensures confidentiality by providing encrypting location and speed samples from probe vehicles to the traffic server (TS) using Key pairs of TS public Key K_{TS} and TS private key $K_{TS'}$	Does not use PKI to enforce confidentiality. .
4.	A secure Model for Remote Electronic Voting: A Case Study of Tanzania	Provides integrity using asymmetric and hash algorithms where hash values resulting from ballot encrypted by the voter is compared with hash value produced by the voter storage server (which is sent along with the receipt to the voter). If the two hash values match then the vote was not changed.	Does not use PKI to achieve integrity
		Provides authentication using National digital identity cards (e-cards) with Public Key Infrastructure (PKI).	Does not use PKI to enforce authentication
		Provides confidentiality (secrecy and privacy) of votes using asymmetric algorithm in which the voter encrypts the ballot using the Public key of the voter counting server and the voter counting server uses its private key to decrypt the votes under the condition that the private key is only available when the voting is closed (i.e. at the time of counting or tabulation).	Does not use PKI to enforce confidentiality.

(iv) Determining indicators for ranking enforcement of security services

The method for determining indicators to rank enforcement of security services was adapted from [23,24]. The indicators for ranking enforcement of security services were excellent, good, fair and poor. This implied that security service in a particular security model was termed as excellent, good, fair or poor based on the security mechanisms implemented in the model using PKI. In evaluating security model, the attribute *excellent* refers to the use of PKI in

implementing security mechanism for instance, encryption or hashing algorithm. Hence, the more the lack of the PKI implementation, the weaker the ranking attribute (for instance, *fair* or *poor*).

(v) Ranking enforcement of security services

The ranking of enforcement of security services was done using ranking scales. The ranking scales were 4 for excellent, 3 for good, 2 for fair and 1 for poor. Hence, in ranking the security model based on PKI, the evaluator has to judge the security mechanism using ranking attributes namely excellent, good, fair or poor by expressing them in terms of scales or just numbers. The process of ranking security mechanisms (services) of security models in terms of ranking attributes and ranking scales forms the metric for evaluating security services based on implementation of PKI.

B. Testing the Metric for Evaluating Security Models based on Implementation of PKI

Analytical experiment for testing developed metric was done in order to confirm if the developed metric can be applied for evaluating security models based on implementation of PKI. The testing of the developed metric followed four processes as explained below.

(i) Selected four security models implemented using PKI

Based on insights from literature, four security models were selected namely (i) Enhanced Security Model for Mobile banking Systems in Tanzania (ii) Proposed SMS Banking Secure Model (iii) Enhancing Security and Privacy in Traffic-Monitoring Systems and (iv) A secure Model for Remote Electronic Voting: A Case Study of Tanzania.

(ii) Selected security services

Four security services were selected as the evaluation criteria for security models namely; integrity, confidentiality, authentication and non-repudiation security services due to the fact PKI is designed to provide such security services. Implementation of SSL and TLS protocol using PKI enforces integrity, confidentiality, non-repudiation and confidentiality security services.

(iii) Identified security strengths and weaknesses in each model

Security strengths and weaknesses in each model were identified and summarized as indicated in Table 2. Security strengths were identified by noting availability of appropriate security mechanisms in reviewed models; for instance, hashing and encryption algorithms. Security weaknesses were identified by noting encryption and hashing algorithms that are already cracked in selected security models. Security weaknesses were also determined through identification of security vulnerabilities due to lack of PKI implementation in organizations for enforcing security mechanisms. Security strengths for the 4 selected models are summarized in Table 1.

(iv) Determined indicators for ranking enforcement of security services

In this phase, ranking attributes and ranking scales were determined and they were distinguished from each other using appropriate descriptions. The ranking attributes were excellent, good, fair and poor. The ranking scales were numerical representations of the ranking attributes namely; 4 for excellent, 3 for good, 2 for fair and 1 for poor.

(v) Ranked enforcement of security services

Each security model was ranked with one of the four ranking scales namely (i) 4 if its ranking attribute was excellent (ii) 3 if its raking attribute was good (iii) 2 if its ranking attribute was fair and (iv) 1 if its ranking attribute was poor respectively. Having performed the five processes, the each security model was evaluated and results were tabulated.

4. Results and Discussion

The aim of the study was to develop the metric for evaluating security models based on implementation of PKI and to test the developed metric in evaluating security models. To achieve the first research objective, the metric for evaluating security models based on implementation of PKI has been developed. Furthermore, to achieve the second research objective the results for the test of the proposed metric have been obtained. The results are detailed below.

A. Metric for Evaluating Security Models based on Implementation of PKI

As indicated in Table 2, the metric for evaluating security models based on implementation of PKI consists of evaluation criteria, ranking attributes and ranking scales. The evaluation criteria are the security services namely integrity, non-repudiation, authentication and confidentiality security services. The ranking attributes are excellent, good, fair and poor. The ranking scales are 4 for excellent, 3 for good, 2 for fair and 1 for poor. The evaluator should make specific descriptions for ranking attributes to make sure that there is a clear difference between one ranking attribute and the other.

Hence, what gives the difference between excellent and good is the description for excellent and that for good. For example, as far as evaluation of integrity security service is concerned, the evaluator may rank the integrity security mechanism as excellent due to the fact that PKI system is used and supports excellent hashing algorithms for protecting data. The evaluator may rank integrity security mechanism as good simply because PKI system is not used but good hashing algorithms are used for protecting data. In Table 2 and Table 3, EC represents evaluation criteria, I, N, A and C represents integrity, non-repudiation, authentication and confidentiality respectively.

Table 2. Metric for evaluating security models based on implementation of PKI

EC	Excellent	Good	Fair	Poor
	4	3	2	1
I	PKI system is used and supports excellent hashing algorithms for protecting data	PKI system is not used but good hashing algorithms are used for protecting data	Hashing algorithm used is already broken based on literature evidence	There are no hashing algorithms used to prevent data modification
N	PKI system is used and supports excellent use of digital signatures to achieve accountability of participating entities	There is good use of digital signature to achieve non-repudiation security mechanism but not based on PKI system	Digital signatures are not used but some other non-repudiation security mechanisms are used	There is no use of non-repudiation security mechanisms at all
A	There is use of PKI system and explanation is provided on how it supports validation of systems before exchanging information	PKI system is used but there is no explanation on how it supports validation of systems before exchanging	PKI system is not used but there are other authentication security mechanisms used	There are no authentication security mechanisms used at all
C	PKI system is used and provides excellent encryption algorithms for preventing data exposure	PKI system is used but explanation is not provided on how it achieves encryption to prevent data exposure	PKI is not used but some other confidentiality security mechanisms are used.	There are no encryption algorithms used for protecting data exposure.

With this example, there is a clear demarcation between the descriptions for the ranking attributes *excellent* and *good*. Following similar process, the descriptions for ranking attributes for authentication, non-repudiation and confidentiality were obtained as indicated in Table 2.

B. Evaluating Four Security Models based on Developed Metric

As far as Table 3 is concerned, the evaluation of security services for the secure model for remote electronic voting [12] indicated that as far as integrity is concerned the model has not implemented PKI system; however, the model uses good hashing algorithms for protecting data. As far as authentication is concerned, the model was ranked as good due to the fact that PKI system is used but there is no explanation on how it supports validation of systems before exchanging information.

The model for enhancing security and privacy in traffic monitoring [1] was evaluated with ranking attributes fair (2), poor (1), fair (2) and fair (2) for integrity, non-repudiation, authentication and confidentiality security services respectively. The model is graded as fair in terms of integrity because of using hashing algorithms that are already broken based on literature evidence. The model is ranked as poor in terms of non-repudiation since it does not use non-repudiation security mechanisms at all.

Table 3. Evaluating security models based on implementation of PKI

S/N	Security Model	I	N	A	C
1.	Secure model for remote electronic voting [12]	3	2	3	3
2.	Model for enhancing Security and Privacy in Traffic monitoring [1]	2	1	2	2
3.	Enhanced Security Model in Mobile Banking Systems [14]	2	2	2	2
4.	Proposed SMS Banking Secure Model [2]	3	2	2	2

5. Conclusions

This study contributes to body of knowledge the metric for evaluating security models based on implementation of PKI. There are several security metrics for evaluating security models; however in such metrics the evaluation is not based on implementation of PKI. PKI is the security solution with capabilities for enforcing integrity, confidentiality, non-repudiation and authentication security mechanisms. This study was conducted to develop the metric for evaluating security models based on implementation of PKI and to test the developed metric in evaluating security models. The metric has been developed based on insights from literature and was also tested successfully using ranking attributes and ranking scales.

However, this study faces subjectivity validity threats. The ranking scales, though they are numerical and quantifiable in nature, they are derived from ranking attributes that are purely qualitative. Thus, care should be taken in making clear descriptions for ranking attributes so that the differences in numerical representations reflect same difference in qualitative representations. This implies that the ranking attributes and scales should be done clearly so that the difference from the number 4 for excellent and 3 for good should match the differences in descriptions for excellent and that for good.

The validity threat comes in due to the fact that though numbers 4 and 3 (representing excellent and good respectively) may be numerically different, the descriptions for excellent and good may not be different and thus making the ranking attributes and scales futile. Further studies would be conducted to establish metrics for evaluating security models based on implementation of PKI. Such studies would include performing cryptographic experiments to test applied integrity and confidentiality security mechanisms.

References

[1] B. Hoh, M. Gruteser, and H. Xiong, "Enhancing Security and Privacy in Traffic-Monitoring Systems," IEEE Pervasive Computing. November*:* 38-46, 2006.

[2] E. Abuyang, "Mobile Banking in Developing Countries : Secure Framework for Delivery of SMS-banking Services," *Int. Bus. J.*, vol. 3, no. August, pp. 12–23, 2007.

[3] M. Pendleton, R. Garcia-Lebron, J. H. Cho, and S. Xu, "A survey on systems security metrics," *ACM Comput. Surv.*, vol. 49, no. 4, 2016, doi: 10.1145/3005714.

[4] S. Rwiza, M. Kissaka, and K. Kapis, "A Methodology for Evaluating Security in MNO Financial Service Model," in IST-Africa 2020 Conference Proceedings, 2020, pp. 1–10.

[5] A. Albarqi, E. Alzaid, F. Al Ghamdi, S. Asiri, and J. Kar, "Public Key Infrastructure: A Survey," *J. Inf. Secur.*, vol. 06, no. 01, pp. 31–37, 2015, doi: 10.4236/jis.2015.61004.

[6] A. Jancic and M. J. Warren, "PKI - Advantages and Obstacles.," *Aism*, pp. 104–114, 2004.

[7] L. Harn and J. Ren, "Generalized digital certificate for user authentication and key establishment for secure communications," *IEEE Trans. Wirel. Commun.*, vol. 10, no. 7, pp. 2372–2379, 2011, doi: 10.1109/TWC.2011.042211.101913.

[8] P. Morrissey, N. P. Smart, and B. Warinschi, "The TLS handshake protocol: A modular analysis," *J. Cryptol.*, vol. 23, no. 2, pp. 187–223, 2010, doi: 10.1007/s00145-009-9052-3.

[9] J. L. Hernandez-Ardieta, "Enhancing the reliability of digital signatures as non-repudiation evidence under a holistic threat model," no. February, pp. 1–380, 2011.

[10] M. Elkhodr, S. Shahrestani, and K. Kourouche, "A proposal to improve the security of mobile banking applications," *Int. Conf. ICT Knowl. Eng.*, no. November 2012, pp. 260–265, 2012, doi: 10.1109/ICTKE.2012.6408565.

[11] C. Cremers, M. Horvat, J. Hoyland, S. Scott, and T. Van Der Merwe, "A comprehensive symbolic analysis of TLS 1.3," *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 1773–1788, 2017, doi: 10.1145/3133956.3134063.

[12] S. Kimbi and I. Zlotnikova, "A Secure Model for Remote Electronic Voting : A Case of Tanzania," *Int. J.*, vol. 3, no. 4, pp. 95–106, 2014.

[13] A. Kukec, S. Groš, and V. Glavinić, "Implementation of certificate based authentication in IKEv2 protocol," *Proc. Int. Conf. Inf. Technol. Interfaces, ITI*, no. July 2007, pp. 697–702, 2007, doi: 10.1109/ITI.2007.4283856.

[14] B. Nyamtiga, A. Sam, and L. Laizer, "Enhanced Security Model for mobile Banking systems in Tanzania," *Intl. Jour. Tech. Enhanc. Emerg. Eng. Res.*, vol. 1, no. 4, pp. 4–20, 2013.

[15] R. K. A. Ahmed, "Overview of Security Metrics," *Softw. Eng.*, vol. 4, no. 4, pp. 59–64, 2016, doi: 10.11648/j.se.20160404.11.

[16] A. Satapathy and J. Livingston, "A Comprehensive Survey on SSL/ TLS and their Vulnerabilities," *Int. J. Comput. Appl.*, vol. 153, no. 5, pp. 31–38, 2016, doi: 10.5120/ijca2016912063.

[17] S. Misra, S. Goswami, C. Taneja, A. Mukherjee, and M. S. Obaidat, "A PKI adapted model for secure information dissemination in industrial control and automation 6LoWPANs," *IEEE Access*, vol. 3, pp. 875–889, 2015, doi: 10.1109/ACCESS.2015.2445817.

[18] S. Rwiza, M. Kissaka, and K. Kapis, "A Methodology for Evaluating Security in MNO Financial Service Model," in *IST-Africa 2020 Conference Proceedings*, 2020, pp. 1–10.

[19] A. Ju, A. Wang, M. Xia, and F. Zhang, "Metrics for Information Security Vulnerabilities," *J. Appl. Globable Res.*, vol. 1, no. 1, pp. 48–58, 2008.

[20] D. R. Thomas, A. R. Beresford, and A. Rice, "Security metrics for the android ecosystem," *SPSM 2015 - Proc. 5th Annu. ACM CCS Work. Secur. Priv. Smartphones Mob. Devices, co-located with CCS 2015*, pp. 87–98, 2015, doi: 10.1145/2808117.2808118.

[21] J. A. Wang, H. Wang, M. Guo, and M. Xia, "Security metrics for software systems," *Proc. 47th Annu. Southeast Reg. Conf. ACM-SE 47*, 2009, doi: 10.1145/1566445.1566509.
[22] K. Petersen and N. Bin Ali, "Operationalizing the requirements selection process with study selection procedures from systematic literature reviews," *CEUR Workshop Proc.*, vol. 1342, pp. 102–113, 2015.
[23] H. Jo, S. Kim, and D. Won, "Advanced information security management evaluation system," *KSII Trans. Internet Inf. Syst.*, vol. 5, no. 6, pp. 1192–1213, 2011, doi: 10.3837/tiis.2011.06.006.
[24] J. Breier, "Security Evaluation Model based on the Score of Security Mechanisms," *ACM Slov*14.

Authors' Profiles

Sigsbert Rwiza has BSc. in Computer Engineering and Information Technology and MSc. in Electronics Engineering and Information Technology from the University of Dar es Salaam (UDSM) in Tanzania.

Currently, he is a PhD student at the University of Dar es Salaam, College of Information and Communication Technologies (CoICT).

Dr. Mussa Kissaka has BSc. in Electrical Engineering from the University of Dar es Salaam (UDSM) in Tanzania and PhD in Telecommunications Engineering from University of Manchester, UK.

Currently he is a Senior Lecturer at the University of Dar es Salaam, College of Information and Communication Technologies (CoICT).

Dr. Kosmas Kapis has Master of Engineering Science in Telecommunications and Networking from the University of Curtin in Australia. He has PhD in Computer Science from Open University of Tanzania.

Currently, he is a Lecturer at the University of Dar es Salaam, College of Information and Communication Technologies (CoICT).

How to cite this paper: Sigsbert Rwiza, Mussa Kissaka, Kosmas Kapis, " A Metric for Evaluating Security Models based on Implementation of Public Key Infrastructure ", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.10, No.6, pp. 27-35, 2020.DOI: 10.5815/ijwmt.2020.06.04