Mateko et al., J Inform Tech Softw Eng 2018, 8:3
DOI: 10.4172/2165-7866.1000235

Journal of
Information Technology & Software Engineering

Research Article Open Access

Current BYOD Security Evaluation System: Future Direction

Priscilla M Boadi*, Dr Shikun Zhou and Dr Ioannis K

University of Portsmouth, Hampshire, United Kingdom

Abstract

There are growing vulnerabilities in Bringing Your Own Device (BYOD) implementation which may not have been fully identified by organisations. It is very difficult to identify, monitor and evaluate the fast growing number of threats and vulnerabilities in a BYOD system, leading to delayed time in preparing and loading a patch which is a periodic process (Static) in most organisation, resulting in risk as the process is not continuous (dynamic) Computer security managers have the task to identify and evaluate these vulnerabilities according to their risk and threat to the network. One database which is known to contain identified vulnerabilities is the Common Vulnerabilities and Exposures (CVE), Common Vulnerabilities Scoring System (CVSS) on the other hand provides numeric scores to each vulnerabilities in the CVE database based on their characteristics and security impact. This assessment is on relevant work to check the various data collected on vulnerability and threat related to BYOD and conduct a vulnerability scoring exercise to report on possible scoring framework.

Keywords: BYOD; Vulnerability; CVSS; Security controls

Introduction

Nowadays, more and more organisation allows personally owned mobile devices to access their network either in the organisation or outside the organisation, this phenomenon is known as BYOD [1]. BYOD is the use of personally owned devices within a working environment for professional purposes; this could be smart devices such as smartphones, tablet, mobile devices, and laptops. Thus BYOD affect various parts of people's life, being education, social or economic with it many benefits, as well as vulnerabilities Smart devices can be attacked by means of exploiting vulnerabilities which may be present either in the operation system, application software, hardware (personal device or server), system authentication not properly set-up, or users abuse of a targeted component [2]. An attacker achieves its objective by infiltrating the network against both the user and the organization, they utilise on various vulnerabilities of targeted host, therefore it becomes necessary for both users and organisations implementing BYOD to be aware of the risk pose by each vulnerability. When these attacks ocur, it can cause critical data loss, Denial of Service attack (DOS) etc., harmly both to the user and the organisation. Therefore creating a secure security environment for a BYOD system include devising a vulnerability prediction means to help us identify vulnerabilities, and the assessment of risk can offer quantitative pointers for management of security database exist in other systems which are updated regularly with the discovering of threats, especially also there are firewalls, intrusion detection systems which become weak with the discovering of new vulnerabilities. Therefore, a need for a ranking algorithm to assess possible harm to the organisation, evaluating the severity of vulnerability and referencing it numerically for severity score of each vulnerability is essential [3]. However, computer security administrators lack broad understanding of the standard in measuring the risk of vulnerability in a BYOD facility [4]. Also Dynamicity is not considered in a BYOD measuring of vulnerability, this is because only known serious vulnerabilities are patched and this is time consuming, the security administrators have a passive behaviour and wait on BYOD user complain to look over website for vulnerability databases on information regarding these found vulnerability to either patch up or setup exposed hardware and software appropriately. Some vulnerabilities found in these databases have only describe characteristics with no known illustrated solution.

According to the statistics report from the National Institute of Standard and Technology (NIST) the number of exploited vulnerabilities increased drastically within the last years (2015-2017). Based on the National Vulnerability Database (NVD) found exploited vulnerabilities were from 6,487 to 11,342 with the year 2017 being severe. The labelling of vulnerability can be confusing; therefore institutions have come up with numbering standard structure;

- MITRE Corporation have the CVE identification form of labelling [5].
- National institute of Standards and Technology (NIST) uses the (NVD) (NVD,2017) [6,7].
- FIRST Organisation and SANS Institute labelling uses the CVSS. All these indexed the CVE numbers [8-10].

The underlying overview of this paper is the relative breakdown of present vulnerability scoring systems, for the purpose of informed decision on their various advantages and propose a measuring framework for auditing a BYOD security system. The remaining passage is organised as fellows; section 2 briefly present related works on the issue section 3 Vulnerability Information and section 4 BYOD security evaluation system and finally 5 presents the conclusion.

Related Work

Mobile device have been one of the contributors of information system security breaches in organizations [11]. This then implies that Information technology (IT) managers have greater concern with the degree to which employees using BYOD adhere to information security policies and IT transformations [12]. However, this does not mean consenting to high level of risk by both users and organization. There are different definitions on risk in research publication, but for the purpose of these work, a definition by Aven and Renn is adopted, it states: "An event where the outcome is uncertain" [13]. As stated in the definition the purpose of a scoring system is to evaluate the risk of uncertainty in a BYOD environment in particular [2,14]. The proposed model focuses on an improved security risk potential auditing process, based

***Corresponding author:** Priscilla Mateko B, Faculty of Technology, University of Portsmouth, Hampshire, United Kingdom, Tel: 07424530210; E-mail: up795078@myport.ac.ukg

Received April 20, 2018; **Accepted** May 10, 2018; **Published** May 18, 2018

Citation: Boadi PM, Zhou S, Ioannis DK (2018) Current BYOD Security Evaluation System: Future Direction. J Inform Tech Softw Eng 8: 235. doi:10.4172/2165-7866.1000235

Copyright: © 2018 Mateko PB, et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

on real-time information on a system's Variables (People, Technology and Organisational Policy).

Presently, security administrators have difficulty in the approach of using a comprehensive standard for evaluating the risk of vulnerabilities. Though, there exist limited vulnerability scoring systems, with each having its own strength and weakness in their scoring abilities, these vulnerabilities are scored according to their threat level, such as, projected losses from security incidents, detection rate of security bug in a new software application or network device, intrusion detection system alarms, corrupted number of virus e-mails captured, and others [15-17]. However, an issue arises when these vulnerabilities are too many to tackle and each is scored by distinct scales [18].

For the conversion of vulnerability data into an actionable material, a Vulnerability Scoring System becomes necessary. Some existing security systems have been reviewed, these include:

1) Computer Emergency Response Team Coordination Centre (CERT/CC); it generate vulnerabilities scores in the range of 0 to 180 [19,20]. However it considers whether the Internet infrastructure is at risk and what category of requirements are needed to exploit that vulnerability.

2) The SANS vulnerability analysis scale; its deliberates in case weakness is located among default configurations or client and server systems [21].

3) Microsoft's proprietary scoring system; this is used to analyse the difficulty of threats whether exploitation and the total impact of the vulnerability. Whilst the above mentioned scoring systems are useful, they are made for one-size-fits-all with no consideration to a vulnerability impact on a particular environment (individual and organisation) therefore they can be term as static solutions

4) Common Vulnerabilities Scoring System (CVSS); is an open framework collaborating the characteristics and impacts of IT vulnerabilities. It involves three groups: Base, Temporal and Environmental. With each group generating a numeric score ranging from 0 to 10, and a Vector, a compressed textual representation that reflects the values used to derive the score [22]. CVSS have some difficiency, only its Base Score Group of Vulnerabilities is calculated using the CVSS calculator, leading to improper risk evaluation. This is because, vulerabilites in a system changes over time and situation and its essential for the IT security manager to have the precise evaluation of the threats that imposes the greatess harm to an organisation and individual. Another difficiency with CVSS is that, variety goes low and CVSS cannot distinguish between vulnerability well, this is because only a small variety of distinct values are used for scoring the enormous quantity of vulnerabilities.

Though the CVSS is a good starting point, and might provide some clue about security evaluation in software and hardware, such scoring systems cannot be used to compute the vulnerability posture for BYOD system, but they can act as a foundation to deal with ranking of vulnerability directly ssecurity risk evaluation includes identifying, assessing vulnerabilities and monitoring of all IT platforms by quantifying the factors to conduct an inclusive assessment. It becomes essential to prioritize and amend these threats and vulnerabilities that pose the greatest risk, these threats and vulnerabilities are measured very differently with different scales [23,24]. Also there are security standards providing best practices for information security managements in organisations, such as ISO/IEC 27001:2005, ISO/IEC 27002:2005 [25], COBIT 5 [26,27], and NIST Special Report 800-53. However, these standards do not state clearly security metrics that may be implemented in the case of BYOD situation. In this context, one of the complaints in security standards is that weight is put on auditing with very little about measurement.

As can be noted from the analysis of related works, vulnerability and risk evaluation though are separated; however, they interact with each other. Based on an efficient measurement, constructing an appropriate ranking model is a meaningful task. Moreover, it is the main research objective

Threat, Vulnerability, Risk and Security Controls Information

Vulnerability: According to The International Organization for Standardization, (ISO/IEC FDIS 27001:2005, 2005). Vulnerabilities are "defects or weakness in a system security procedures, design, implementation, or internal controls that could be exploited (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy". In principle, vulnerabilities occur in the organisations resources [28].

- **Threats:** The NIST Special Publication (SP) 800-30 defines threats as a series of occurrences within which a natural or intelligent invader may compromise the confidentiality, integrity, or availability of security system in an illicit manner to cause harm.

- **Risk:** Is the harm resulting from some intended or accidental occurrence that negatively impacts the information security process [29].

- **Security controls:** These are made up of policy, procedure, algorithm, metrics, or other measures used to avoid or minimise the amount of damages cause from one or more threat and vulnerability.

Threats agents gives rise to threats, these exploit vulnerabilities to violate information security properties such as confidentiality, integrity, availability, etc. Security controls implements countermeasures to defend information technology systems (BYOD) by mitigating threats, or plugging vulnerabilities, or both using policies, algorithms and metrics. This has been shown in Figure 1.

An effective, method to measure information security of a BYOD system is to analyse the threats and vulnerabilities that occurs in the security system, with its matching security parameters that are concerned thereon. A BYOD audit framework, should collects and store data on user behaviour, success or failure of an operation and the quality in service performance. Therefore the proposed methodology follows the method of first categorizing the information security threats and vulnerabilities into static and dynamic. To begin with the categorisation let understand what dynamicity and static and is; Dynamicity in general is defined as finding a decision point in a process and categorised or classified them by their business rules [30-33]. Interestedly in the mobile security world as explanation by [34,35], dynamic analysis occurs when researcher have access to a mobile application being executed in a remote environment, such as virtual machine or using an emulator for monitoring. However this is normally done in an auditing section of a security management systems, and dynamic system evaluation is perform in real-time without major interaction from the environment. On the other hand, Morrow explain static analysis as, examining an application to locate any malicious behaviour at an agreed instance [36]. Below is a classification of Static security threat and Dynamic security threats in Tables 1 and 2.

These vulnerabilities could be found in the information on system's variables namely; a) People (misuse by BYOD users), b) Technology

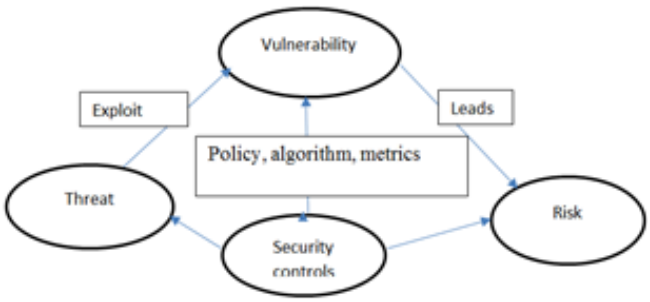

Figure 1: Connections amongst threats, vulnerabilities, risks and security controls.

Static Security Threats and vulnerabilities	Mitigation Approaches
Physical threat end Exposure of confidential data from; • Stolen or loss and decommissioned of devices • Malware, Hacking, Social Engineering	• Personal device storage areas should be Encrypted • Training users not to store sensitive data on personal mobile devices • Shut down of personal devices remotely by IT administrators in the cases of Joss or stolen devices • User education and awareness

Table 1: Static security threat and vulnerabilities.

(mobile devices (operating system, applications), in-appropriate setup of system authentication), c) Processes (Organisational Policy). Therefore making it difficult to define, rank and score.

For the purpose of these review actual CVE vulnerabilities data publication collected from the NVD was use. Most found Vulnerabilities identifications are based on reference numbers or those similar vulnerabilities are identified with different numbers to prevent mix-up [37] (Table 3).

Vulnerability scoring system plan

Vulnerability Prediction data being use is expected to contain information about their particular harshness. Evaluating an organization's BYOD security risk from different exploited vulnerabilities using the metrics as specified by CVSS, the CVSS scores for publicly recognised vulnerabilities are communicated by the NVD. Following in the direction of criticality rankings, which identifies the network setup, business function and likelihood of a misfortune of a BYOD system [22], and a security objective of confidentiality, integrity, and availability with every system allocated into a "potential impact" rankings, of 0-10. The Federal Information Processing Standards 199 uses the ranking of low, medium, or high, thus being the qualitative method of risk and vulnerability evaluation, this the CVSS also conforms to Nevertheless the propose vulnerabilty scoring aim at achieving its security objective based on the quantitative metric of BYOD use situation , scored in the range of 0-10 which is not in the low, medium, or high, thus organisation can score vulnerabilities according to their environmental situation [38,39]. This project express "potential impact" rankings as None (N)=0, Low (L)=1, Low medium=2, Medium (M)=3, High=4 etc.

BYOD Security Assessment System

The Dynamic Cluster-based Auditing Framework for BOYD Security is made up of the following proficient abilities. Firstly using quantitative metrics tools such as the; a) the Mean Time to Compromise

Dynamic Security Threats and vulnerabilities	Mitigation Approaches
Risk of Data Insecurity or Leakage(loss) from Misuse of BYOD • Policy/Access • Insider threat • storing organization's data to Unsecured location	• Encryption of corporate data • BYOD devices should be restricted • Device integrity scanning application should be use • Regular User education and awareness • System Monitoring
Insecure interface and APIs due to • direction from Malicious QR codes (Quick Response Codes) Weak API(application programme interface)	• Untrusted content do\\>loaded on a BYOD device should be avoided • Use secure web gateways, IITTP proxy servers, etc. to validate IJRLS before allowing access • Restrict peripheral use on mobile devices (e.g., disabling camera use) to prevent QR code reading • strong authentication and access control mechanism
Untrusted Networks, application and mobile devices could results in; • Eavesdropping • Man-in-the-Middle attacks • Malware attacks • Downloading Malicious applications to and from	• Mutual authentication procedure should be use for verification from both endpoints • Inactive Network interfaces disabled • third-party application should undergo risk assessment before allowed to be used as a BYOD device • forbid insecure Wi Fi network collection
Insecurity in Virtual Machine Migration or creation	• Location services in mobile devices nun-off in sensitive areas or implement firewalls • Use a separate browser within a secure sandbox for browser-based access related to organization • monitoring through IDS (Instruction Detection System
Broken authentication and session management from • Usage of guessable session ID • Unable to detect repeated guessing trials while there is a mechanism in place • Weak cryptography • Limitation of HTTP • Insecure session handling methods • Weakness in the Inactive session management technique • Use of location services	• Mutual authentication procedure should be use for verification from both endpoints • If possible Choose not to be co1U1ected to internet location services • Two way Authentication process
Risk of Data Insecurity or Leakage(loss) from • Misuse of BYOD Policy/Access • Insider threat • storing organization' s data to unsecured location	• encryption of corporate data • BYOD devices should be restricted • Device integrity scanning application should be use • Regular User education and awareness • System Monitoring
Insecure interface and APIs due to • direction from Malicious QR codes (Quick Response Codes) Weak AP (application programme interface) Insecure interface and APIs due to • direction from Malicious QR codes (Quick Response Codes) Weak AP (application programme interface)	• Untrusted content downloaded on a BYOD device should be avoided • Use secure web gateways, HTTP proxy servers, etc. to validate URLs before allowing access • Restrict peripheral use on mobile • devices (e.g., disabling camera use) to prevent QR code reading • strong authentication and access control mechanism

Table 2: Dynamic security threats.

and the State-time estimation algorithms by and b) VEA-bility by respectively [40-44].

Secondly the environmental variables are on the system factors as updated in the systems' Configuration Management Data Base (CMDB) [45]. For the purpose of this security auditing system Microsoft Access Database is used, this helps in making the scoring models proficient as prediction will be based on the organizational damages on real BYOD environment rather than on user's estimations. Also the information of the environmental variables described in this research settles on data items rather than a whole BYOD security system, hence allowing focused on significance of each data item.

Dynamic Cluster-based Auditing Framework for BYOD Security will be monitoring BYOD devices in real time process meant to detect vulnerabilities thus real time detection of security holes and prevention and alerting organizations' security managers. National Vulnerability Database (NVD) vulnerabilities database is used in the illustration of the background model [46] (Figure 2).

Cluster-based framework using access database (CBFD)

Figure 3 shows the make-up of the Cluster-based Auditing for the BYOD Security. This is a largely made up of database on every significant information in regard to software and hardware that an organisation make use of in terms of their ICT facilities and the various relationships between them. The Cluster-Based Framework defined in this work presented in Table 4 will have information of the BYOD use situation, made up of the following entities: software components, Applications,

CVE VULNERABILITIES ID	CVE-2017-3567 (Oracle Database Server)	CVE-2017-0131(Data Handling)	CVE-2017-4052(BYOD USE)
tDescription	Vulnerability in the OJVM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4 and 12.1.0.2. Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise OJVM. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of OJVM.	A remote code execution vulnerability exists in the way affected Microsoft scripting engines render when handling objects in memory in Microsoft browsers. These vulnerabilities could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	Authentication Bypass vulnerability in the web interface in McAfee Advanced Threat Defense (ATD) 3.10, 3.8, 3.6, 3.4 allows remote unauthenticated users / remote attackers to change or update any configuration settings, or gain administrator functionality via a crafted HTTP request parameter.
CVSS Severity score	CVSS 3.0 Base Score 5.3 (Availability impacts) [23]	V3: 7.5 HIGH V2: 7.6 HIGH	(not available)

Table 3: Example of common vulnerability and exposure.

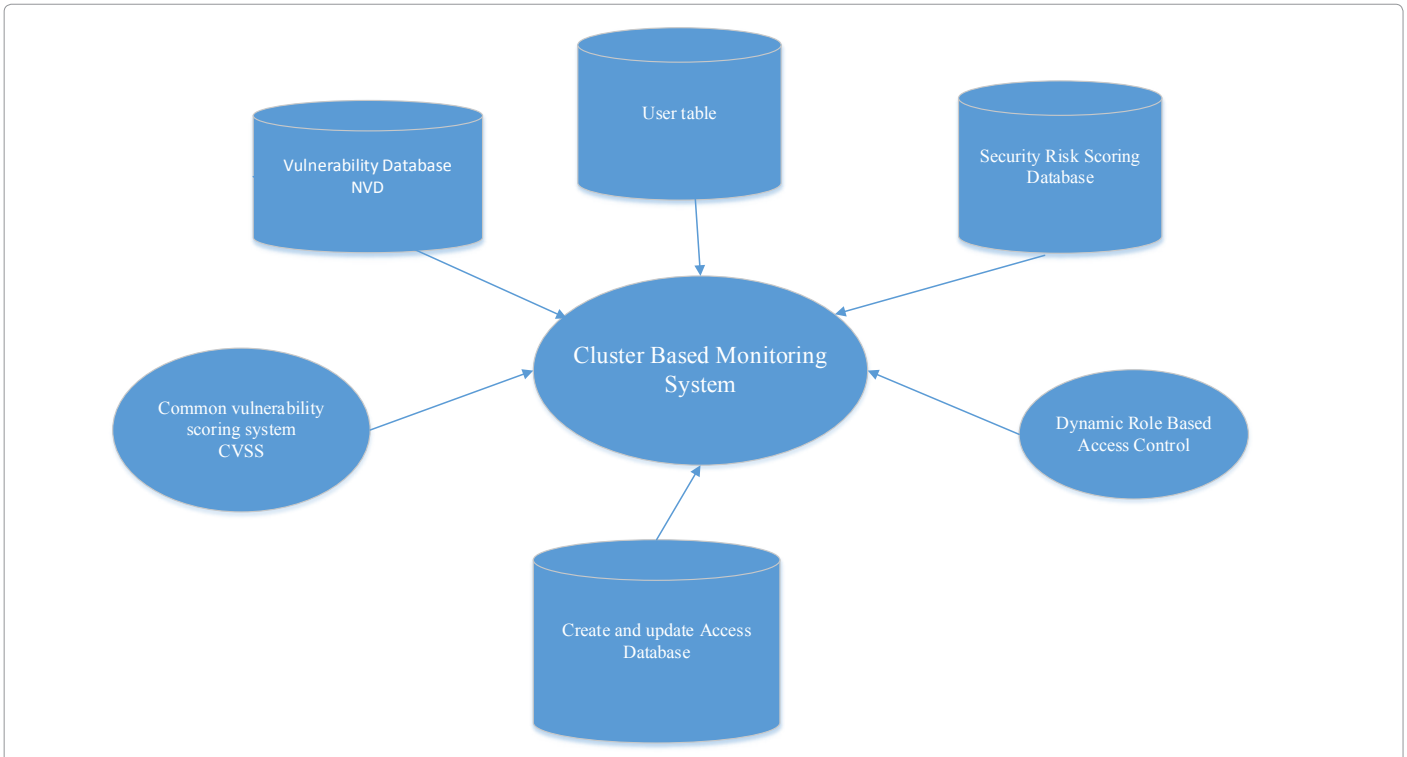

Figure 2: Cluster-based auditing framework.

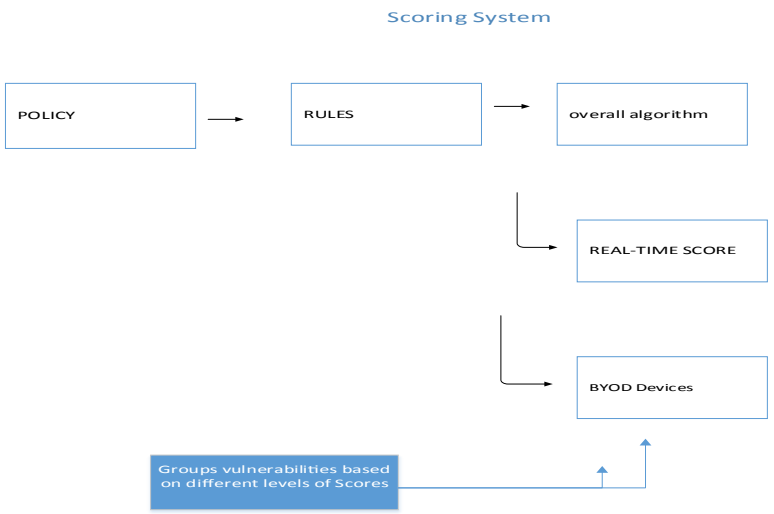

Figure 3: Diagram of a security risk scoring unit.

Column ID	Column Name	Column Description	Value
COMPONENT ID	Software or Hardware(Smartphone, Tablet etc.), Vendor, Serial Nunmber, Version…	Value is equal to component ID in NVD	Unique
COMPONENT TYPE	Hardware Type (Smartphone, Tablet disk…), Software type(Microsoft, Aparche), etc.	For example: Database, Table, Column….	H, S, UI, COMM
CONFIDENTIALITY IMPACT (CI)	Basic parameter	None, Partial, Complete	N, P, C
CR	Confidentiality Requirement	The importance of the affected IT asset to a user's organization, measured in terms of confidentiality	L,M,H
IR	Integrity Requirement	Guarding against improper Information modification or Destruction.	L,M,H
AR	Availability Requirement	Ensuring timely and reliable access to and use of Information…	L,M,H
FINAL EVALUATED RISK SCORE	CVSS final Risk Score based on all basic, temporal and environmental Parameters (people, policy, techology).	Based on all parameters including CI	CR. 0-10

Table 4: CBFD – components table.

system components for instance operating system. For the success of the computational of the risk scoring algorithm each component of the CBFD is stated clearly including the security requirement (NOTE: Confidentiality requirement (CR) is tallied according to these values None = 0, Low=1, Low Medium=2, Medium=3, Medium high=4, High=5).

For the definition, the potential impact is low (1) if the loss of confidentiality, integrity or the availability might be predicted to have a reduced adverse effect on organizational operations, organizational assets (Data) or BYOD user. The potential impact is Medium (4) if the loss of confidentiality, integrity, or availability might be expected to have a serious unfavourable effect on organizational operations, organizational assets or BYOD user [47].

Security risk scoring unit

This is made up of the security risk scoring database (Figure 3).

Conclusion

In this paper, work regarding scoring systems was review. Data gathered specifically on BYOD security threat is term as Dynamic security threats and the general mobile security threats is term as Static security threats these have been tabulated in Tables 1-4. However gaining access to sufficient and relevant data to make knowledgeable decision on BYOD vulnerability scoring is a major challenge. CVSS, CWE, AND CWSS are some of the examples of approaches for scoring vulnerabilities, though CVSS is the most applied of the mentioned above it lack in vulnerability scoring related specifically to BYOD systems in real-time.

This paper introduces a framework purposefully for scoring related to BYOD vulnerability; this considers historic and intrinsic characteristics. Future work include the development of security metric for BYOD system, that is a formal BYOD auditing system based on a data item.

References

1. Micro T (2012) Enterprise Readiness of Consumer Mobile Platforms. Trend Micro 1: 18.
2. Weintraub E (2016) Evaluating Confidentiality Impact in Security Risk Scoring Models. International Journal Of Advanced Computer Science and Applications 7: 156-164.
3. Keramati M (2016) New Vulnerability Scoring System for Dynamic Security Evaluation. IEEE, pp: 746-761.
4. OSVDB (2013) Mobile Devices and Exploit Vector Absurdity.
5. https://www.mitre.org/: http://cve.mitre.org/cve/
6. National Institute of Standards and Technology (2009) Recommended Security Controls for Federal Information Systems and Organizations. NIST, USA.
7. NIST (2012) Guide for Conducting Risk Assessments. NIST SP, pp: 800-830.
8. http://www.first.org/cvss/http:/www.first.org/cvss/
9. https://www.first.org/cvss/cvss-v30-specification-v1.8.pdf
10. https://www.sans.org/newsletters/no-newsletter.php
11. Son JY (2011) Out Of Fear Or Desire? Toward A Better Understanding Of Employees' Motivation To Follow Is Security Policies. Information And Management 48: 296-302.
12. Siponena M, Mahmood AM, Pahnila S (2014) Employees' Adherence To Information Security Policies: An Exploratory Field Study. Information And Management 51: 217-224.
13. http://www.kb.cert.org/vuls/html/fieldhelp
14. Weintraub E (2016) Security Risk Scoring Incorporating Computers' Environment. International Journal Of Advanced Computer Science And Applications 7: 183-189.
15. Patriciu VV, Priescu I, Nicolaescu S (2006) Security Metrics for Enterprise Information Systems. Journal of Applied Quantitatve Method.
16. Wang Y, Wei J, Vangury K (2016) Bring your Own Device Security Issues and Challenges.
17. Zhong Y, Bhargava B, Lu Y, Angin P (2015) A Computational Dynamic Trust Model for User Authorization. IEEE Transactions on Dependable and Secure Computing 12: 1-15.
18. http://www.microsoft.com/technet/security/bulletin/rating.mspx
19. Aven T, Renn O (2009) On Risk Defined as an Event where the Outcome is Uncertain. Journal of Risk Research 12: 1-11.
20. http://www.cert.org/stats/cert_stats.html#vulnerabilities/
21. https://technet.microsoft.com/en-us/security/gg309177
22. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
23. http://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7435.pdf
24. Scarfone K, Mell P (2009) An Analysis Of Cvss Version 2 Vulnerability Scoring. In NI, Esem '09 Proceedings Of The 2009 3rd International Symposium On Empirical Software Engineering And Measurement, Washington, IEEE.
25. https://www.iso.org/standard/50297.html
26. Oliver D, Lainhart J (2012) COBIT 5: Adding Value Through Effective Geit. The EDP Audit, Control, and Security Newsletter 46: 1-12.
27. ISACA (2012) COBIT 5 for Information Security.
28. https://www.iso.org/standard/42103.html
29. Dempsey K, Chawla NS, Johnson A, Johnston R, Jones AC, Orebaugh A (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.
30. Eijndhoven T, Iacob M, Ponisio M (2008) Achieving Business Process Flexibility with Business Rules. 12th International IEEE Enterprise Distributed Object Computing Conference, pp: 95–104.
31. https://www.first.org/
32. Hermosillo G, Seinturier L, Duchien L (2010) Using complex event processing for dynamic business process adaptation. IEEE International Conference on Services Computing (SCC), pp: 466-473.
33. Allodi L, Massacci F (2014) Comparing Vulnerability Severity and Exploits Using Case-Control Studies. TISSEC.
34. Chandramohan M, Tan HK (2012) Computer.
35. Morrow B (2012) BYOD Security Challenges: Control and Protect your Most Sensitive Data. Network Security, pp: 5-8.
36. Choudhury AJ, Kumar P, Sain M, Lim H, Jae-Lee H (2011) A Strong User Authentication Framework for Cloud Computing. Services Computing Conference (APSCC) IEEE Asia-Pacific. pp: 110-115.
37. www.cve.mitre.org
38. Weintraub E, Cohen Y (2015) Continuous Monitoring System Based On Systems' Environment. ADFSL Proceedings.
39. Leversage D, Byres E (2007) Comparing Electronic Battlefields: Using Mean Time-to-Compromise as a Comparative Security Metric. Computer Network Security, pp: 213-227.
40. Leversage D, Byres E J (2008) Estimating a System's Mean Time-to-Compromise. IEEE Security & Privacy 6: 52 - 60.
41. Liu QX (2012) Research on Key Technology of Vulnerability Threat Classification. Journal on Communications 33: 79-86.
42. Mc Queen MA, Boyer WF, Flynn MA, Beitel GA (2005) Time-to-Compromise Model for Cyber Risk Reduction Extimation. Idaho National Laboratory (INL).
43. Tupper M, Zincir Heywood AN (2008) Vea-Bility Security Metric: A Network Security Analysis Tool. Third International Conference On Availability, Reliability And Security.
44. https://www.kb.cert.org/Vuls/Html/Fieldhelp
45. Keller A, Subramanian S (2009). Best Practices for Deploying a CMDB in large-scale Environments. IEEE, pp: 732-745.
46. https://nvd.nist.gov/
47. http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf