SURVEY ON BYOD SECURITY RISKS AND ARCHITECTURES

P.Soubhagyalakshmi[1], J.Anitha[2]

Asst.Prof (ISE), YDIT, Visvesvaraya Technological University
eMail Id: slakshmi.p@gmail.com
Professor (CSE), DSATM, Visvesvaraya Technological University
eMail Id: anitha.jayapalan@gmail.com

Abstract

With the advent of new devices like smart devices and tablets and with the technology transformations in the way devices are getting connected coupled with the paradigm shift in the way information and services are brought together the usage of these smart devices has become a common entity in personal and professional environments. Organizations are encouraging the usage of these smart devices via varying connectivity mechanisms like wireless and wired technologies. This model of "Bring your Own Device (BYOD)" significantly improves the productivity and enriches economy growth. However it poses a greater threat to information and infrastructure security. This paper discusses security policies (BYOD polices) to secure organizational data and resources along with solutions to resolve the attacks on the device and corporate network. This paper also presents evaluation of possible outcomes of solutions based on the X.800 security architecture.

***Keywords:** Bring Your Own Device (BYOD), Trusted Execution Environment (TEE), Trusted Execution Environment Application (TEEA), Advanced Persistent Threat (APT),Control Program(CP), Portable Trusted Module (PTM), Trusted Platform Module (TPM),Traffic Control (TC).*

--***--

I. INTRODUCTION

Using the employee's own devices at work place is the passion. Most of the organizations allow the employees to use their own devices at the workplace. So that, The employees get the greater work satisfaction at the work place. Hence, it is the requirement and becoming as a strategy of the organizations. This motivates the employees to carry their work with pleasure. As the devices are portable, the devices are used for office work inside and outside of the organizations. Hence, employees are able to use the resources of organization all the time to do the firm's work and even the workmen are used of multi platform devices with the latest technologies as they are comfortable with their own devices. This is an upcoming trend to use their own devices for work in the offices. Using the own devices to carry the work in the work place is the future need of all kinds of companies by 2016. IT industries, government domains and other sectors have the vision for adopting this upcoming trend. Allowing the employees to use own devices at office increases their morale and ethical values.

A. Advantages

Following are the advantages and benefits by allowing the own gadgets or devices to carry the work at work place.

1. The organization's productivity improves as the employees are using their own device to carry the work at work place.
2. The employees access the organization resources for 24*7 to do the work. This increases the organization's quality and productivity. Thus business objectives are aimed.
3. Employees are comfortable and flexible to use their own devices with the latest technology. This improves the cost cutting of new technology in the organizations. Hence, it is the business benefit.
4. As the installation, maintenance configuration data, a setting of the latest technologies exists in the employee's own devices will improve the cost savings for the new technology.
5. Organizations have no control on the employee's own devices used to carry the work in the firm. Hence, employees can use different devices with different CPU architecture.
6. Employees use their own end to end devices at their affordable price which reduces the budget requirements in the firm.
7. The employee work satisfaction is at greater level as they are using their own end to end devices. This improves the ethical and moral values towards employer.
8. This is the passion and current trend to use employee's owned devices for work at work place.
9. The ease of using devices fetches the information efficiently as employees are used of multi platform devices.

Various scalable advantages of the organizations are emerging as the business is the important objective of the organization.

II. CHALLENGES

Following are the security risks introduced as the employee's own devices allowed for work at work place.

1. Confidential data of organization such as documents, files, applications etc are accessed through the compromised device as it is attached to the corporate network.
2. If the device is compromised it is possible to access the personal information of the customers such as username, password, banking information, E-mail account details etc.
3. The device contains personal data and business data. If the device is stolen or lost then the data contained in the device is unsecured.
4. As the devices attached to the corporate network, eaves malware get installed in the device and makes use of the device for unauthorized access.

Following are the various threats injected into the organization as it is allowing the employee's owned devices for work at work place.

1. Malware causes the devices to loss the sensitive data and makes the device useless by disturbing the applications work.
2. Spam is the messages received through the corporate network which wastes the resources of the organization infrastructure such as bandwidth and memory.
3. The threats like phishing causes the user to access the fake web site in turn to access the sensitive business data such as reports, accounts etc.,
4. SQL injection vulnerabilities steal the organization's data through the compromised device.
5. If the organizations information does not have encryption then this possibility gives the chance for the attacker to hack the device through the advanced persistent threat. This attack targets the organization through the compromised device and performs eaves activities periodically over a long period of time.
6. Man- in –the middle attack propagates into the corporate network easily through the unprotected network and causes the malicious activities. For example, modifying the confidential data or deleting the important data.

Following are the other security challenges described below.

1. Personal data and business data co-exist in the device. So, better access methods are required to distinguish personal with private data.
2. The organization cannot use the same infrastructure support for the various kinds of devices. Because, the operating speed of devices are different and having the different operating systems.
3. As the multi platform devices are allowed, there is no control on the devices and it is difficult to enforce the security on the devices. Hence, it is required to manage the devices according to the organization policies.
4. The organization policies for security should comply with laws and standards.
5. The organizations data and intellectual property required to protect.
6. It is difficult to provide security for the business that runs outside of the infrastructure. But it is required to concern this security issue.
7. As the size and scope of the organization grows, it is difficult to maintain consistent security for the critical assets of the organization.
8. Better security measures (defense methods) should be mapped with security risks with the business objectives.
9. Unified security measures have to be derived for any type of end to end device.

III. METHODOLOGIES AND ARCHITECTURES

Following are the various mitigation techniques to resolve the security risks. Their respective cons and pros have been discussed below.

A. Control Programs

This is a software program being installed in the gadget. The structure and content required for the control program as follows:

1. Identify the risk factors introduced by gadgets.
2. List the security policies required for the devices. Map these polices with the security risks.
3. Build the control program with the following functionalities:

a. Device Management Routine
b. Application control
c. Audit reports of policies
d. Wiping data when the device lost
e. Encryption for device and data
f. Reset access rights to devices when relationship of employee changed to guest.
g. Reset access rights to devices when employees leave the organization.

4. Evaluate solution
5. Measure impact of the security tool on the existing network.
6. Implement solutions
7. Periodical assessment of solutions.

Analysis: As the number of risks increases, then it is required to add and map new security policies. The solution needs to be modified as the various kinds of security risks faced by the network.

Comparison of analysis of evaluation shown in the Table 2.

B. Mobile Security Reference Architecture

This architecture is suitable to resolve security issues on the mobile phones and tablet but do not challenge security issues on the laptops and other gadgets.

The Mobile Security Reference Architecture contains following components.

Table 1: The main components of MSRA and its key explanation [13]

Components	Key Explanation
Virtual private Network	Provide a robust method for creating secure connections between mobile devices and D/A while using unmanaged networks.
Mobile Device management	Process or tool intended to manage applications, data, and configuration settings on mobile devices. The main focus is to centralize and optimize the functionality and security management of a mobile communication.
Mobile Application Management	Provides in-depth distribution, configuration, data control, and life-cycle management for specific applications installed on a mobile device.
Identity and access management	Integrate services such as authentication and authorization across the mobile solution to form a cohesive security profile for each user.
Mobile application Store	A repository of mobile applications. A selection of approved applications that can be downloaded and installed on approved devices by the users of the device.
Mobile application Gateway	Software that provides application-specific network security for mobile application infrastructures. Is to act as a network proxy, accepting connections on behalf of the application's network infrastructure, filtering the traffic, and relaying the traffic to mobile application servers.
Data loss prevention	Focus on preventing restricted information from being transmitted to mobile devices, or from mobile devices to unauthorized locations outside the organization. May include monitoring and auditing.
Intrusion detection	A set of heuristics to match known attack signatures against incoming network traffic and raise alerts when suspicious traffic is seen. To detect potentially malicious activity from connecting mobile devices.
Gateway and security stack	Serve to filter unwanted network traffic and are usually configured in a "stack" with traffic traversing each filter in sequence.

Analysis: The Mobile Security Reference Architecture able to mitigate the security risks only for mobile devices.

Comparison of analysis of evaluation shown in the Table 2.

C. Architecture of Trusted Execution Environment

The TEE architecture supports to resolve security issues for multi platform devices as the desktop and mobile devices have different CPU architecture and operating systems.This is better security tool compare to the MSRA. Architecture of trusted Execution Environment achieved the objectives such as data integrity and confidentiality, isolated access for the private data and personal data, secured access to the data in the device is secured, device identification,authorization and authentication to avoid the unauthorized device access.

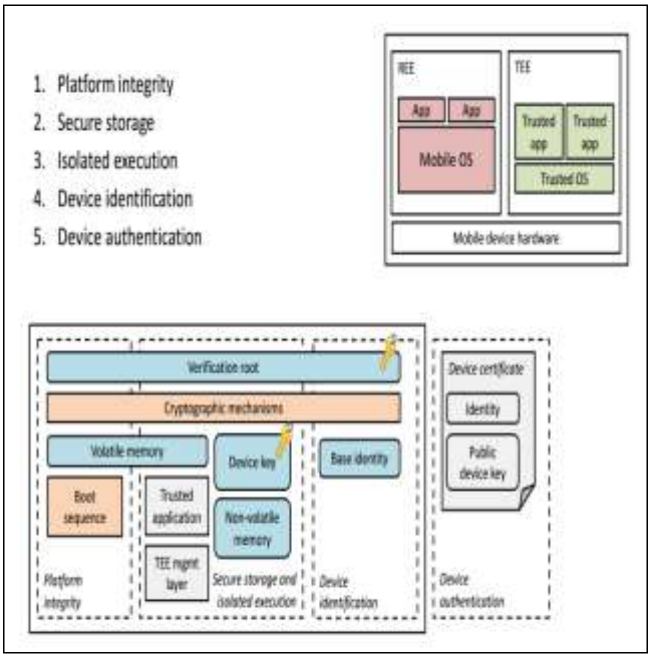

Figure 1: Overview of TEE architecture diagram [13]

This architecture model provides the trusted computing environment for users. Portable trusted module (PTM) is similar to trusted platform module (TPM) built on USB key. The PTM binds a user and provides the trust for the secure access of user applications. PTM is the platform independent concept for the mobile devices. The TEEA supports multiple traffic control (TC) modules for the mobile devices to provide secured access of information. TC uses cryptographic library containing SHA256 and Elliptic curve cryptograph (ECCC) [23]. ECC is better compare to RSA with respect to fast computing, memory and efficiency savings and key sizes. SHA-256 is better than SHA-1 as it is supportable for distributed computation and this algorithm remains unbroken over the internet. TEE proposed with new authorization protocol named as session key authorization protocol (SKAP) [23]. It is the replacement for the existing protocols (OSIP and OSAP) [24].

The objectives of Architecture of Trusted Execution Environment are evaluated using X.800 security architecture. As a result of this, Access control, data integrity and confidentiality constraints are achieved by TEEA. But device authentication and non-reproduction are not achieved. This is the limitation with the Architecture of Trusted Execution Environment.

Analysis: The Architecture of Trusted Execution Environment able to mitigate the security risks for multi platform devices with different CPU Architecture.

Comparison of analysis of evaluation shown in the Table 2.

D. BlueBoxEx

This framework provides security for the devices to mitigate various kinds of attacks by focusing on the following security policy strategies [25][26][27][28].

1. The BlueBoxEx implements the mobile device management strategy policies through the following,
   a. *Device Enrollment:* The device identified with a unique APIs key on the server. Each user created with an account and login details. These details of the device are used for verification as it is connected to the VPN gateway.
   b. *Security Functions:* Security for the device provided through the remote locking, feature lock.
   c. *Employee privacy control:* Two modes of privacy control contained in this application. In work mode, device able to access the data. In private mode, employee personal information is accessible.

2. The BlueBoxEx implements the security for mobile devices through the strong authentication method, antivirus software and loss of device protocol.
3. The BlueBoxEx implements application management policies to categorize the applications as whitelisting or blacklisting. If the applications cause high security issues then such applications must be removed and these applications come under the category known as blacklisting. If wiping the blacklisting application is not possible then lock the device containing these applications.
4. The BlueBoxEx implements data protection implemented through the encryption libraries contains the methods such as RSA algorithm.

BlueBoxEx program evaluated using X.800 security architecture. As a result of this, Access control, data integrity, confidentiality, device authentication and non-reproduction constraints are achieved by BlueBoxEx. Still it is required to support these constraints for all other types of gadgets using this program.

Analysis: The BlueBoxEx program able to mitigate the security risks for multi platform devices with different CPU Architecture.

Comparison of analysis of evaluation shown in the Table 2.

Table 2: The Key evaluation of various methodologies based on X.800 Security Services.

Non-repudation	Data Integrity	Data confidentiality	Access control	Authentication	X.800 security services	
No	No	Yes	Yes	No	**CP**	**Achieved**
No	Yes	Yes	No	No	**MSRA**	
No	Yes	Yes	Yes	No	**TEEA**	
Yes	Yes	Yes	Yes	Yes	**BlueBoxBx**	
None	None	Monitoring and auditing	Authentication and authorization	Authentication	**CP**	**Key Evaluation**
None	None	Monitoring and auditing	Authentication and authorization	Authentication	**MSRA**	
None	SHA-256 and ECC	SHA-256 and ECC	SKAP authorization protocol. PTM module	None	**TEEA**	
Unique APIs key	Data encryption	Secure network architecture. Lost of device handling protocol	VPN gateway	Two factor authentication using biometric and API key	**BlueBoxBx**	

IV. FUTURE WORK

Unified defense methods, a set of control programs and various methodologies required to be developed for multi-platform devices with any CPU architecture for various device needs as well on going threat models. This needs the scalability and applicability for various deploy models needs to be assessed on a ongoing basis to make the dynamic security needs. Various certification models for various business verticals needs to be established and integrated with the security systems and tools. Develop a suitable model to mitigate the security issues of organization as well as privacy issues of workmen at workplace. Still more security policies and control objectives has to be defined. Developing integrated tool to be useful in other domains to mitigate the security risks.

V. CONCLUSION

Introducing this concept in the organization increases their productivity and minimizes the budget requirements in the business. A successful control program allows the employees to use their own end-to-end devices outside the organization after the scheduled time to carry the organizations work. This results into the growth of the organization’s business. This concept implementation in the organization is supportive to the employee morals and employer attractive.

VI. REFERENCES

[1] K. W. Miller, J. Voas, G. F. Hurlburt, *BYOD:* Security and Privacy Concerns, 2013

[2] L.Phifer , Contributor in http://searchsecurity.techtarget.com, *BYOD* security strategies: Balancing BYOD risks and rewards, Jan 28, 2013
[3] T. Bradley, Pros and cons of bringing you own devices to work, PCWorld, Dec. 20, 2011, Accessed on Nov 28 2013.
[4] White paper, *BYOD* Security Challenges in Education: Protect the Network, Information, and Student, Cisco, 2012
[5] D. Wiech, The Benefits And Risks Of BYOD, Jan 28, 2013.
[6] A. Scarfò, New security perspectives around BYOD, IEEE 978-0-7695-4842-5/12, 2012
[7] G. Eschelbeck, BYOD Risks and Rewards , A Sophos Whitepaper,2013
[8] " IBM: Sorry, Siri. You're Not Welcome Here ", http://www.informationweek.com/news/security/mobile/240000882, InformationWeek, Accessed on Nov 27, 2013
[9] IBM BYOD -- Bring Your Own Device -- United States http://www.ibm.com/mobilefirst/us/en/bring-yourowndevice/byod.html, Accessed on Nov 28, 2013
[10] 10 myths of BYOD in the enterprise. http://www.techrepublic.com/blog/10-things/10-myths-of-byod-in-theenterprise/,TechRepublic, Accessed on Nov 28, 2013
[11] Happiness Is ... Bringing Your Own Computer Devices to Work. <http://www.retailwire.com/discussion/16188/happiness-is-bringingyour-own-computer-devices-to-work> Retailwire, Accessed on Nov.27, 2013
[12] SearchCompliance.com's IT Compliance FAQ series, Oct 25 2013, Accessed on Nov 27, 2013.
[13] Manmeet Mahinderjit Singh, Soh Sin Siang,Oh Ying San, Nurul Hashimah, Ahamed Hassain Malim**,** Azizul Rahman Mohd Shariff The School of Computer Sciences, Universiti Sains Malaysia, 11800 Penang, Malaysia, Accessed on October 2014, SECURITY ATTACKS TAXONOMY ON BRING YOUR OWN DEVICES (BYOD) MODEL
[14] BRING YOUR OWN DEVICE (BYOD): SECURITY RISKS AND MITIGATING STRATEGIES: RESEARCH PAPER, April 2013.ISSN-2229-371X. Available at www.jgrcs.info
[15] BYOD: Implementation and Security Issues Harsh Kishore Mishra ,M.Tech. Cyber Security, Centre for Computer Science & Technology , Central University of Punjab, Bathinda (Punjab)
Registration number: CUPB/MTECH-CS/SET/CST/2013-2014/01
[16] SISG Survey, http://esg-global.com/blogs/a-multitude-of-mobile-
security-issues (as accessed on 1st February 2013)
[17] Bill Morrow (December 2012), Science Direct.com-Network Security-BYOD security challenges: control and protect your most sensitive data, Volume 2012, Issue 12, Pages 5-8.
[18] http://en.wikipedia.org/wiki/Security_controls (as accessed on 1st February 2013)
[19] AarnoHarteveld blog, http://blogs.msdn.com/b/arnoha/archive/2012/04/25/building-a-byod-strategy.aspx (as accessed on 1st February 2013)
[20] http://www.govinfosecurity.com/webinars/mobile-learn-from-intels-ciso-on-securing-employee-owned-devices-w-264 (as accessed on 1st February 2013)
[21] Best Practices for Mobile Device Management, Maas360.com, from http://www.valleytalk.org/wp-content/uploads/2013/03/AST-0079353_mdm_bestPractices.pdf.
[22] "Forrsights Workforce Employee Survey, Q4 (Nov 2011)"www.forrester.com/Forrsights+Workforce+EmployeeArnab Ghosh *et al*, Journal of Global Research in Computer Science, 4 (4), April 2013, 62-70 © JGRCS 2010, All Rights Reserved 70
[23] Kathleen N. McGill, " Trusted Mobile Devices: Requirements for a Mobile Trusted Platform Module " ,
Johns Hopkins APL Technical Digest, vol. 32, 2013.
[24] Allen Bethea (2012), What is the difference between SHA-1 and SHA-256, [Online] Available: http://www.ask.com/explore/difference-between-sha1-sha256-2062, Last accessed date: 23 May 2014.
[25] Check Point Software Technologies Dimensional Research, "The Impact of Mobile Devices on Information Security", June, 2013.
[26] Mark Shepherdson, Trustmarque, " BYOD – the biometric implications" Volume 2013, Issue 4, Pages 5–7, April 2013
[27] John Thielens, " Why APIs are central to a BYOD security strategy ", ScienceDirect network security Volume 2013 , Issue 8, Pages 5–6 August 2013
[28] Khoula Alharthy, Wael Shawkat, Implement Network security control solutions in BYOD environment, 2013 IEEE international conference on control system, computing and engineering, Penang, Malaysia, 29 Nov-1 Dec 2013