SECURITY ATTACKS TAXONOMY ON BRING YOUR OWN DEVICES (BYOD) MODEL

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.

ABSTRACT

Mobile devices, specifically smartphones, have become ubiquitous. For this reason, businesses are starting to develop "Bring Your Own Device" policies to allow their employees to use their owned devices in the workplace. BYOD offers many potential advantages: enhanced productivity, increased revenues, reduced mobile costs and IT efficiencies. However, due to emerging attacks and limitations on device resources, it is difficult to trust these devices with access to critical proprietary information. Therefore, in this paper, the potential attacks of BYOD and taxonomy of BYOD attacks are presented. Advanced persistent threat (APT) and malware attack are discussed in depth in this paper. Next, the proposed solution to mitigate the attacks of BYOD is discussed. Lastly, the evaluations of the proposed solutions based on the X.800 security architecture are presented.

KEYWORDS

Bring Your Own Device (BYOD) model; Advanced Persistent Threat (APT) attack, Malware; Smartphone; Security

1. INTRODUCTION

With the introduction of smart phones and tablet to the consumer market, it has forever changed the mobile device computing landscape for enterprise IT. Trending consumer mobile platforms, specifically Android, iOS, and Windows phone devices, have surpassed Blackberry and Palm devices as the preferred mobile computing platform for daily business and personal use. This lead to the grow of a new phenomenon where employee demand to connect their latest iOS, Android, and Windows device to the corporate network, which widely accepted to be addressed as Bring Your Own Device (BYOD). BYOD is the new phenomenon that has emerged in the business environment which allows employees to use their personal device to access company resources for work. The BYOD phenomenon is being fueled primarily by four trends [1]:

- Employees want the latest and greatest performance hardware which is better and newer devices than their employer provides for them.
- A growing number of employees work at home as part of telework program.
- Many IT departments often cannot afford all the tools that employee needs and the vetting process for these applications is too slow to meet user's expectations.
- The blurring of work and personal life.

The figures for using mobile devices for work related tasks in 2016 are estimated at 350 million users of mobile devices, of which 200 million will be using their own personal devices for work-

DOI : 10.5121/ijmnct.2014.4501

related tasks as well [2]. This huge amount of market growth of popularity was not possible with the enhancement of the following main aspect: the connectivity, application access through the web and the mobile device advancement. However, the BYOD concept itself has also brought in the new division of areas such as Bring Your Own Technology (BYOT) and Bring Your Own Software (BYOS) in which employees use non-corporate software and technology on their device [2]. This increases productivity of work and choices of scope that an employee can work on. There are three basic benefits that BYOD can provide which are corporate costs can be reduced, employee morale can be improved and organizations can keep up with the latest and greatest hardware [1]. However, this in turn creates many challenges for the organization. The utmost concern of BYOD is the consequences of the usage of the unsecured personal mobile devices for handling corporate data. Mobile devices that are insufficiently secured lead to the possibility of the breaches of the fundamental values of confidentiality, integrity and authenticity of company data. Besides that, the malware infection is one of the security concerns related to BYOD. This paper will study in depth on the security challenges of the BYOD model along with the proposed solution. The objectives of the studies are i) to study in depth on the security challenges of BYOD model, ii) to identify and propose possible solutions to mitigate the security challenges based on the findings and iii) to evaluate the proposed solution based on the X.800 security services.
In the next section, further explanation of the security concerns and attack of BYOD is presented. In Section 3, related work on BYOD is presented. Section 4 and 5 present two important attacks that will be chosen and discussed in details. Proposed solution and its evaluation based on X.800 will be included in the section as well. Besides, the discussion will be presented in section 5. Lastly, conclusion and future work will be presented in the last section.

2.0 SECURITY CONCERNS AND ATTACKS OF BYOD

BYOD significantly impacts the traditional security of protecting the company or client data. The greatest security risk posed by the use of personally owned devices was the main focus on the company. Hence, the general security concerns are presented and the taxonomy attacks of BYOD are shown.

2.1 General Security Concern

The data is the critical components for organizations. As BYOD has dramatically increased the number of expensive security incidents. The sensitive corporate information and client data can be easily transported and lost. There are a few of key findings related to BYOD in loss company or client data. Increasing numbers of mobile devices connect to corporate networks where 93% have mobile devices connecting to their corporate networks [3]. As BYOD grows quickly and creates problems for organizations. Customer information on mobile devices causes security concerns where 53% report, there is sensitive customer information on mobile devices [3]. Besides that 94% indicate lost or stolen customer information is critical concern in a mobile security incident [3]. From the 2013 Information Security survey results, the top three security concerns are loss of company or client data (75 percent), unauthorized access to company data and systems (65 percent) and malware infections (47 percent) [4]. The overall survey result is as shown in Figure 1.

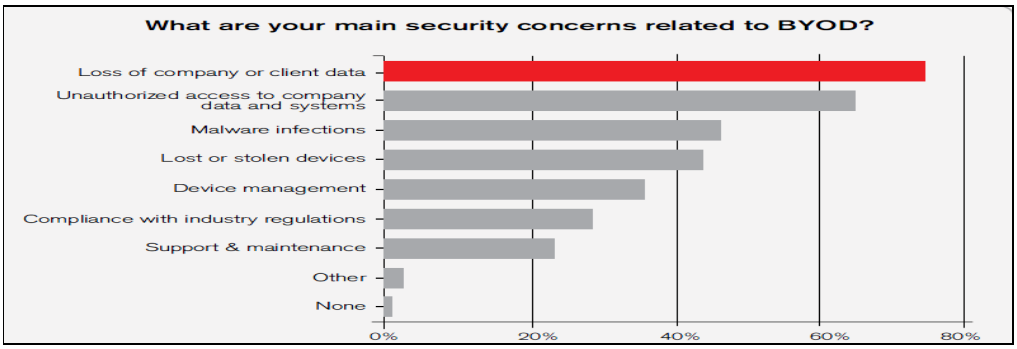

Figure 1 The survey result of the security concern of BYOD [4]

Owasp has listed the top 10 mobile security risks as shown in the figure 2 . Each of the consequences of the respective risk will be discussed in following section.

Figure 2: OWASP Top 10 mobile security risks [6]

- Weak server side control

  This vulnerability corresponds to the technical impact of the associated vulnerability that the adversary is exploiting via the mobile device. For example, an adversary may exploit a Cross-Site Scripting (XSS) vulnerability via the mobile device [6].

- Insecure data storage

  Insecure data storage can result in data loss, in the best case, for one user. In the worst case, for many users. Common valuable pieces of data seen stored, including user name, authentication tokens, passwords, cookies, location data, transaction histories and any confidential data [6].

- Insufficient transport layer protection

  This flaw exposes an individual user's data and can lead to account theft. If the adversary intercepts an admin account, the entire site could be exposed. Poor SSL setup can also facilitate phishing and MITM attacks [6].

- Unintended data leaked
  This vulnerability may result in the following technical impacts: extraction of the app's sensitive information via mobile malware, modified apps, or forensic tools [6].
- Poor authorization and authentication
  Authentication failures may expose underlying authorization failures as well. When authentication controls fail, the solution is unable to verify the user's identity. This identity is linked to a user's role and associated permissions. If an attacker is able to anonymously execute sensitive functionality, it highlights that the underlying code is not verifying the permissions of the user issuing the request for the action [6].
- Broken cryptography
  This vulnerability will result in the unauthorized retrieval of sensitive information from the mobile device.
- Client side injection
  Injection attacks such as SQL Injection on mobile devices can be severe if the application deals with more than one user account on a single application or a shared device or paid-for content [6]. Other injection points are meant to overflow application components, but are less likely to achieve a high impact result because of the managed code protections of the application languages.
- Security decision via untrusted inputs
  Security decision taken via untrusted inputs will put the whole security model or architecture of the organization at risk.
- Improper session handling
  Improper session handling occurs when the session token is unintentionally shared with the adversary during a subsequent transaction between the mobile app and the backend servers [6]. In the worst-case scenario,the adversary is impersonating an administrative user and issuing a request for administrative functionality that is dangerous in nature.
- Lack of binary protection
  Binary protections prevent an adversary from modifying the underlying code or behavior to disable or add additional functionality on behalf of the adversary. This is likely to occur if the app stores, transmits, or processes personally identifiable information (PII) or other sensitive information assets like passwords or credit cards [6]. Code modification often takes the form of repackaging or insertion of malware into existing mobile apps.

2.2 ***Bring Your Own Devices (BYOD) Attack Vectors***

In order to proposed solution to mitigate the problems in BYOD, the potential attack vectors that could be used against personal devices in a BYOD environment are needed to identify and categorize into different taxonomy. In this section, the potential attacks of BYOD introduced and the taxonomy of the potential attacks are showed.

2.2.1. Lost or stolen mobile devices

Mobile devices are easy to lose or steal and that is not going to change. Then, most of the people store much personal information and company sensitive information on the mobile devices. There are some facts regarding the lost or stolen of mobile devices, approximately 1.3 million mobile phones are stolen each year in the United Kingdom only [7]. Besides that, major United States corporation lose by theft 1075 smartphones and 640 laptops each week [7]. Hence, lost devices account for a significant amount of lost data. In spite of the amount of data lost through stolen devices, but nothing is done to actually protect company information or client data on personal devices. Therefore, lost or stolen mobile devices are a significant attack and impacts the security concerns of BYOD.

2.2.2. Eavesdropping

Mobile devices are highly vulnerable through Common Vulnerabilities and Exposures (CVE) holes and most likely are infected with eavesdropping software. In addition to WIFI connectivity, the attackers may be operating on cellular networks and they can eavesdrop through the network, which could caused the exposing organization's information [8]. Similarly, any information such as mail messages and passwords transmitted through a LAN or WIFI connectivity is subject to eavesdropping [8].

2.2.3. SQL injection

SQL injection is using a code injection technique to target applications and websites, then insert data-stealing malware. SQL injection attack has been at the center of many data breaches due to the BYOD trend in the workplace. Through the Security Week research, 42 per cent of all breaches are due to the SQL injections [9]. BYOD makes understanding the root causes of an SQL injection attack more difficult. Because of the trend for employees to use their BYOD in the workplace.

2.2.4. Advanced Persistent Threat (APT)

APT is a set of stealthy and continuous hacking processes [10]. APT usually targets organizations or nations for business. In fact, APT processes require a high degree of covertness over a long period of time, unlike the other instant attacks [11]. APT consists of three important components which is advanced, persistent and threat. APT attacks against endpoints when the attackers found anomalous exfiltration traffic on the network. BYOD might let the unauthorized people to access the organization's server and the no encryption of the company information in the mobile devices which could give the opportunity for an attacker to conduct the APT attack.

2.2.5. Data privacy for company and client

Monitoring and accessing data and applications on a personally owned device raises legal concerns around data privacy. Many of these issues raise because of the main characteristics of BYOD that the employee owns and to some extend maintains and supports the device. The company is very hard to make sure that the company or client information will not leak to non-employees such as family members who use the device. Hence, the data privacy is the significant attack when the employees use BYOD for the working purposes either in working hours or non-working hours.

2.2.6. Social engineering

Social engineering is the technique of acquiring sensitive or confidential data through psychological manipulation. The objective for an attacker to carry out social engineering is to get hold of sensitive and valuable data. Technique of social engineering in BYOD environment, including phishing, baiting and virus hoaxes. Malicious link and unauthorized mobile app are the common attacking vector that used by attackers to perform social engineering.

2.2.7. Malware

As the growth of malware in mobile devices has been outrageous for the past 2 years, it has certainly become one of the biggest threat to corporate and organization that practice BYOD. Various attacking vectors are available for malwares to transmit and release their payload, including especially in BYOD environment. This attack will be further discussed in details in this paper.

2.2.8. Secure socket layer attack

The secure Socket layer attack is a type of attack that focus on breaching the vulnerabilities of the network protocol. SSL/TLS is the common protocol that targeted by the attacker for this attack. Heartbleed is the most suitable case study to demonstrate the purpose and objective of this attack. As the result of the outbreak of Heartbleed, one third of the username and password stored in the various server in this world were hacked. In BYOD environment, this attack brings more risks to unprotected mobile device that contain corporate data. For example, Android version 4.1.1 is vulnerable to Heartbleed [12] and there is an estimated of 50 million users are affected by this outbreach.

2.2.9. Man-in-the mobile

Man in the mobile is the recent term for mobile version of man in the middle. Malicious keylogger or spyware can be installed into any unprotected mobile devices and man in the mobile attack can be carried out easily. For example, zitmo (zeus in mobile) can be installed in an Andoird device, and read and intercept SMS. Sensitive data, such as mTan can be easily retrieved by the attacker using this type of attack.

2.3 **Taxonomy of BYOD Attacks**

There are many attacks have been discussed in the previous section. The taxonomy of BYOD attacks is categorized into components and security attacks. The components are including user, network, software, physical and web. On the other hand, the security attacks are divided into active attacks, passive attacks and privacy attacks. Under the user components, there are man-in-the-middle attack, social engineering, eavesdropping, and data privacy. Man-in-the-middle and social engineering involving user to carry out the attack and both of the attacks are active attacks. This is because the attackers will change the data or information when conducting the attack. While eavesdropping is the passive attack this is because the attacker is just analyzed and monitor the information transmitted through the network without make any changes to it. In addition, the attacker is accessing the user or client's information without the consent from them. So the data privacy is categorized under the privacy attack. Under the network components, SSL attack is the active attack under the network component. This is due to the SSL attack is attack through the network protocol, especially when the data, such as names and passwords is not encrypted. This allows attackers to steal data directly from the services and users. For the software component, the malware and APT are the common active attacks. Malware could infect the application or mobile applications instantly so that the attackers can steal the data or information from the mobile devices. Besides that, the APT is unauthorized access to the company's system and steals data. The lost or stolen mobile devices obviously are categorized into physical component. The last component is the web, the attacks under this component is SQL injection. Usually the SQL injection is attacked through web and it is the active attack this is because the attacker to inject the code and insert malware to steal data instantly. The data privacy is involved in all of the components and it is under privacy attack. Since the attacks and the components are concerned about the sensitive or confidential data which is offense the data privacy of the company and user. The overall taxonomy of BYOD attacks is as shown in the Table 1 below.

Table 1: Taxonomy of BYOD attacks

Components	**Security Attacks**		
	Active Attacks	**Passive Attacks**	**Privacy Attacks**
User	Man-in-the-mobile Social engineering	Eavesdrop-ping	Data privacy for company and client
Network	SSL attack		
Software	Malware APT		
Physical		Lost or stolen mobile devices	
Web	SQL injection		

3.0 RELATED WORKS

The related works cover an overview of mobile security reference architecture, security attacks of BYOD and existing proposed solutions to mitigate the problems in BYOD. Further details on each issue are covered in the next three sections.

3.1 Mobile Security Reference Architecture

The MSRA document provides reference architecture for mobile computing, released by the Federal CIO Council and the Department of Homeland Security (DHS) to assist Federal Departments and Agencies (D/As) in the secure implementation of mobile solutions through their enterprise architectures. One important assumption pointed out by the council is that this reference only applicable to mobile devices including mobile phone and tablet, but not laptops and other technology gadgets. The main components of MSRA are discussed in Table 2 along with some brief explanations.

Table 2 : 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 raises 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

3.2 Security Attacks of BYOD

BYOD could bring a lot of security attacks against the companies and organization. One of the common attacks is an Advanced Persistent Threat (APT). Johannes de Vries and his team have presented that APT is a form of multistep attack that is executed with more stealth and is targeted specifically to achieve a specific goal [14]. Social engineering and targeted emails to direct users to websites to install malware are common traits of APTs. Besides that, Tarique Mustafa stated that the advent of APT against Information Security Systems, "Purposeful Evasion Attacks" have assumed even more serious significance [15]. In fact, the "Purposeful Evasion Attacks" are difficult to address and pose unparalleled challenges at the basic algorithmic level. Moreover, Websense and his team discussed that the APT process is divided into a few phases which are reconnaissance, preparation, targeting, further access, data gathering and maintenance [16]. The data gathering is where the attacker extracts data from target network and takes action, such as sell the company or client data to third parties.

The other common concern of BYOD is the unauthorized access to company data and system. One of the biggest challenges for the organization is that corporate data is being delivered to devices that are not managed by the IT department, which has security implications for data leakage, data theft and regulatory compliance. With unmanaged devices, enterprise has less control and visibility towards them. One of the most notable examples is the infections of malware on the unmanaged devices. Malware writers might attempt to corrupt or modify data without the permission of the data's owner. For example, SMS can be hijacked or deleted. Malware can manipulate files inside the victim's device. Files can be downloaded from the victim's device and also uploaded to the device without user's intervention and permission. For example, the LuckyCat [18] can manipulate the file in the victim's device. User credentials are also the targets of malware writers.

4.0 ATTACK 1: ADVANCED PERSISTENT THREATS (APT ATTACK)

In this section, a detailed study will be done on the APT attacks. The proposed solution will also be presented, followed by the evaluation of the proposed solution based on x.800 security services.

4.1 Overview of APT Attack

Mobile devices have added a new threat to the corporate landscape as they have introduced the concept of Bring Your Own Device (BYOD). The information accessed through the device means that theft or loss of a mobile device has immediate consequences. Additionally, weak password access, no passwords and no encryption can lead to data leakage on the devices. Advanced Persistent Threats (APTs) are a cybercrime category directed at business [16]. APT requires a high degree of stealth over a prolonged duration of operation in order to be successful [17]. This attack's objective is extending beyond immediate financial gain and compromised systems continue to be of service even after systems have been breached.

APTs can be summarized by the names requirements [23]:

- *Advanced*

Criminal operators behind the threat utilize the computer intrusion technologies and techniques. The operators can access and develop more advanced tools as required and they combine multiple attack methodologies and tools in order to compromise their target system/ device.

- *Persistent*

Criminal operators give priority to a specific task, rather than opportunity seeking immediate financial gain. The attack is conducted through continuous monitoring and interaction in order to achieve the defined objectives.

- *Threat*

There is a level of coordinated human involvement in the attack, rather than a mindless and automated piece of code. The criminal operators have specific objective and are skilled, motivated and organized.

4.1.1 The APT process

The APT process includes a few major phases that occur over a period of months. The APT process consists of six phases which is reconnaissance, preparation, targeting, further access, data gathering and maintenance. Table 3 shows the explanation of each of the APT process phases. Figure 3 illustrates the APT attack.

Table 3 The phases of APT Attack [15]

Phase	Description
Phase 1: Reconnaissance	The attacker passively gathers information about their target to identify the best targeting method. This may include research into the location of the target's office, the location of their own devices and their contact information
Phase 2: Preparation	The attacker actively prepares for the attack, developing and testing appropriate tools and techniques to target their intended victim.
Phase 3: Targeting	The attacker launches their attack and monitors for signs of compromise or failure.
Phase 4: Further Access	The attacker successfully gained access to a device and they will try to identify where in the network and they are and move literally within the network to access data of interest and to install a backdoor.
Phase 5: Data Gathering	The attacker will try to gather the company information or client data and exfiltrate it. They will to exfiltrate the desired data before it is detected.
Phase 6: Maintenance	The attacker will attempt to maintain their access. This may involve minimizing the amount of malicious activity they generate on the network to avoid detection.

Figure 3: The example of APT attack [24]

4.1.2 APT security functional requirements

By analyzing the characteristics and phases in conducting the APT attacks as described above, the functional requirements of an effective security solution can be described. There are several functional requirements, access control, trusted path, cryptography and separate private information and company data. These functional requirements can be used to enhance the security on the mobile computing and mitigate the APT attack [25].

4.2 Proposed Solution

In recent years, mobile devices have replaced desktop personal computers as the primary computing platform for many users. This trend brings to the workplace where nowadays the employees use their personal owned mobile devices to access company's data. BYOD causes a

lot of cyber attacks towards the users and the organization. The proposed solution for BYOD model attack precisley the APT attack is to provide the Trusted Execution Environment Applications (TEEA) for the employee's personal mobile devices. Hence, this section is discussed about the proposed solution to mitigate APT attack of BYOD.

4.2.1 Trusted Execution Environment (TEE)

Nowadays, no method can provide trusted computing support for both kinds of the devices for multi-platform property. This is because desktop machines and mobile devices have different CPU architectures which x86 and ARM [30]. Besides that, limitation in resources and spaces which caused the secure chips is not suitable for mobile devices. If using the security chips, users cannot customize their own security features to meet some experimental demands. Mobile trusted module provides Traffic Control API by software and had been proven to be faster than Trusted Platform Module (TPM). TEE is a secure area that resides in the application processor on a mobile device [27]. Separated with hardware from the main operating system, a TEE ensures the secure storage and processing of sensitive data and trusted applications. So it can protect the integrity and confidentiality of key resources, such as the user interface and service provider assets. There are several important components in the TEE which is platform integrity, secure storage, isolated execution, device identification and device authentication. Figure 4 illustrates the overview of the TEE architecture diagram.

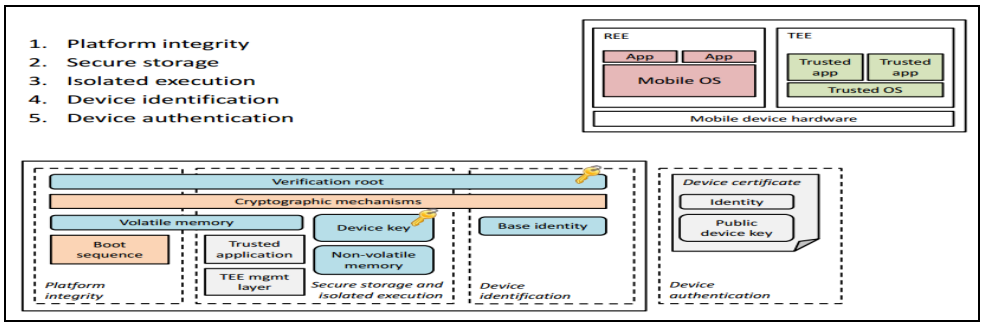

Figure 4: Overview of TEE architecture diagram [27]

4.2.2 Architecture of Trusted Execution Environment Application (TEEA)

The proposed solution for trusts is a user oriented trusted computing system based on the portable trusted module (PTM). PTM is a TPM-like portable device built on a USB key. PTM binds to a user and is the root of trust for users of security applications. PTM is to achieve multiple platform property and the PTM solution is built based on mobile devices rather than USB devices. PTM acts as a trustworthy device which is used to provide TC services instead of TPM to propagate the trust in the computing system to the end user.

The TEEA provides multiple traffic control (TC) modules in the secure world (SW) of mobile device. The multiple TC modules are TPM modules, Transmission Control module (TCM) and Mobile Trusted Module (MTM). The cryptographic library contains SHA256 and Elliptic Curve Cryptography (ECC) [28]. The advantages of SHA-256 over SHA-1 are the SHA-256 has the larger hash size, which is 256 bits long. Even with the advent of multi-core CPUs, multi-threading and distributed computing over the Internet, SHA-256 has remained unbroken [28]. On the other hand, On the other hand, compared to RSA, ECC offers smaller key sizes, faster computation, as

well as memory and energy savings. A new authorization protocol for the TEE is proposed which is Session Key Authorization Protocol (SKAP) [28]. It generalizes and replaces the exiting authorization protocols (OISP and OSAP) [29].

4.2.3 Evaluation of Proposed Solution-TEEA

The X.800 security architecture is used to evaluate the proposed solution, TEEA. Below are the main components of X.800 with the mappings of the features offered by TEEA.

Table 4 The key ebaluation of TEEA based on the X.800 security services

X.800 security services	Achieved	Key evaluation
Authentication	x	None
Access control	✓	SKAP authorization protocol. Trusted execution environment for multiple platform. PTM module used for multiple platform.
Data confidentiality	✓	Cryptography library of SHA-256 and ECC.
Data integrity	✓	Cryptography library of SHA-256 and ECC.
Non-repudiation	x	None

The summary of the evaluation is presented in Table 4.

5.0 ATTACK 2: MALICIOUS APPLICATIONS

In this section, a detailed study will be done on the categorization of malicious applications in BYOD environment. The proposed solution will also be presented, followed by the evaluation of the proposed solution based on x.800 security services.

5.1 Categorization of Malicious Applications

The focus of this section will be largely placed on malicious mobile applications as the growth of malicious mobile application hit a new high recently in the year 2013 in the overall malware identification [32]. Cisco's annual security report claimed that 99% of the mobile malware were built to target Android users [31]. As Android mobile device is having a market share of 79.3% of all mobile operating systems [31], this clearly implies that most of the Android devices are most likely to be used in an organization BYOD environment.

5.1.1 Profit Driven

Most of the malware applications are created for profit purposes. More than 50 percent of the existing malware is profit driven [33]. To further understand how the malware writers earn money through malware applications, they are classified based on their revenue generate method and the payloads.

5.1.1.1 Selling user information

Mobile operating system such as Android has many capabilities. For example, through the usage of APIs of Android, an application can obtain a large amount of information which includes user's location, contact lists and user's preferences based on internet browsing history and installed applications. One of the examples is the GGtracker. This information can be sold to advertising and marketing companies as they can make use of this information to improve their marketing strategies such as selecting a good target market. Information such as contact lists in

the corporate email account can also be sold to phishers and spammers to conduct targeted attack, for example spear phishing [34].

5.1.1.2 Stealing user credentials

People use mobile phones not only for calling purpose but also for many other purposes such as log in to their corporate emails, social networking site, and online banking account. These activities normally require the authentication of username or password. Username and password have been always the popular target of malware writers. As an example, Zitmo (Zeus Trojan for smartphone) has been introduced as mobile Transaction Authentication Number (mTAN) stealing tools. The bank account credential can be easily captured by Zitmo. In addition, user credentials could also be captured by malware distributors through hacking and scanning tools. DroimDream.G collects International Mobile Station Equipment (IMEI) and International Mobile Subscriber Identity (IMSI) number of the compromised device and sends to a remote server [33]. Also, a recent vulnerability attack on the OpenSSL, named Heartbleed, which focused on stealing user credentials, has cost the business e commerce world millions of money. It is also reported that about 50 million of 4.1.1 Jellybean Android users are vulnerable to Heartbleed [35]. On the other hand, popular e-commerce site, E-bay, reported that the company database that contained encrypted username and password was hacked at the end of March 2014 and urge a total number of 145 million users to change their password immediately [36]. A recent released of powerful premium android malware created by the powerful Russion cybercrime gang was named iBanking. iBanking can intercept SMS, steal IMEI , access file, prevention of removal, record audio and etc. iBanking also has a business model of Saas that allows anyone to pay a rental fee and make use of the malware to conduct unethical cybercrime [37].

5.1.1.3 Premium Rate Call and SMS Charges

Legitimate premium rate call and Short Message Service (SMS) provide useful information such as latest news update, technical support for a certain brand of product, or oversea services. Premium rate calls and premium rate SMS can cost several dollars per minutes or per message. Android applications can request permissions to send SMS messages and call at installation. These SMS messages can be sent without the user confirmation. Therefore, malware writers take the advantages of the flaws of user permission scheme and include the SMS services into their malware. FakePlayer and Boxer.G [38] are the malware programs that use this technique and send multiple messages to the premium rate numbers. As a result, this greatly increases the expenses and wasting the company recourses without user knowing.

5.1.2 Non- Profit Driven

Although most of the malware programs are profit driven, there are still a number of them that are not. Most of the malware in this group is focused on bringing destruction and achieving their non-profit purpose and motive. For example, an attacker might want to sabotage the reputation of a specific rival company to achieve their business or corporate objective. Stuxnet is one of the recent examples that can be categorized into this category. It is a sophisticated malware that created by US government to sabotage the Iraq nuclear plant.

5.1.2.1 Data integrity threat

Malware writers might attempt to corrupt or modify data without the permission of the data's owner. For example, SMS can be hijacked or deleted. Malware can manipulate files inside the victim's device. Files can be downloaded from the victim's device and also uploaded to the device without user's intervention and permission. This can be very costly to enterprise, as company data is one of the important assets. For example, the LuckyCat [33] can manipulate the file in the victim's device. KabStamper deletes the entire image found in the Secure Digital (SD) card / Data Center Infrastructure Management (DCIM) / camera folder that stores images taken

with the device's camera. This malware also checks this folder and modifies the images by overwriting them with a predefined image.

5.1.2.2 Privacy exploitation

Hacking tools and monitoring tools are common tools that are used by the attackers when they are trying to exploit the victim's network or device. In addition, sensitive information such as SMS content and current Global Positioning System (GPS) location can be easily obtained. Although some malware is not malicious in itself, but it introduces potential risks for misuse with malicious intent. For example, Penthos.A is a penetration testing application that can assist the attackers to penetrate a network. It generates password for WIFI routers that use Service Set Identification (SSID) and Wired Equivalent Privacy (WEP). Another interesting malware is the Whapsnl. A. It is one of the new families of hacking tools that appears during the third quarter of 2012 [33]. It can sniff and intercept WhatsApp packets.

5.1.2.3 Denial-of-Service Attack

Similar to Denial-of-Service attack on PC desktop, an attacker can use malware and deny the availability of a service or even a device of the victim. Specific DoS could quickly drain the batteries. Placms [29] and Ksapp [38] have the capabilities to remote access connection handling and perform DoS or DDoS. Mobile botnets are also another rising trend in mobile security. The less-monitored devices with high capabilities such as university servers and SOHOs (small office and home office) are always preferred by Botmasters [34].

5.3 Proposed Solution

To mitigate the likeliness of the consequences of the malware attacks mentioned above, a propose solutions named BlueBoxEx is proposed [37] [39] [40] [41]. BlueBoxEx focus on 4 main areas which are i) Mobile Device Management, ii) Mobile Device Security, iii) Application management and iv) Data protection. Each of the area will be discussed in detail in the following section.

5.3.1 Mobile Device Management

The main focus of this area is to take control of the device, but not the other way round. With BlueBoxEx, users can go to legitimate Google App store, iOS play store, or Windows store to download the BlueBoxEx mobile app. The mobile application that sits on the device will perform the task below:

i. **Device enrollment**
The installation of the device will also mean that the device will register a new unique APIs key on the central server. This unique APIs key is essential for the mobile device security. The user will need to register an account and login to the application whenever they try to connect to the VPN gateway.

ii. **Security functions**
The installation will also allow the central remote management to take place. For example, device provisioning, remote locking, feature lock, monitoring and alerting can play their role in securing the device.

iii. **Employee privacy control**
There are two modes of privacy control that are available in BlueBoxEx, which are: working mode and private mode. The approach is similar to how Windows handle different user account on the same device. Working mode is automatically activated once the user requests to connect to the VPN gateway. Restriction and implication will take place to harden the security of the device. Certain privileges will be disabled to prevent unwanted risks taking place.

5.3.2 Mobile Device Security

The main focus of this area is to secure the devices from all possible sources of attack vectors. BlueBoxEx focus on providing secure network and strong authentication method to prevent unauthorized access to the corporate resources. Antivirus application and loss of device protocol are also available in BlueBoxEx in order to secure the mobile device in BYOD environment.

i. Authorization & Authentication

Two factors biometrics will be used in BlueBoxEx. The employee will need to provide their username, password and a token to log in the VPN through the mobile app. The token will be the fingerprint of the user. A token mentioning which fingerprint for users to put will be sent to the user device whenever they request to log in into the VPN gateway [40]. Instead of usual mTan that only ask for 4-6 digits of pass code, fingerprints are unique, more complex and difficult to replicate. With biometric authentication, employees no longer have to worry about remembering complex passwords or losing their authentication tokens.

ii. Secure networ

As mentioned in MSRA, VPN and IDS are essential components of mobile security. As shown in the figure IDS is employed to detect unusual patterns of network patterns before the user is relayed to the VPN gateway. IDS, central server and VPN gateway sit in the DMZ area. With a secure network and monitoring tools, malware will not be able to deploy its payload easily.

iii. Mobile Antivirus

A light weight mobile antivirus is installed together with BlueBoxEx mobile app. The lightweight antivirus will scan the device and send useful information to the central server for monitoring and auditing. If any virus or malware is detected, it will trigger the central server to perform remote virus wiping, or even remote phone locking to secure the device.

iv. Lose of device handling protocol

With the usage of APIs service as the layer of transmitting data between the mobile device and central data server, administrators can remotely deactivate or delete the unique APIs key in order to prevent the device from accessing the VPN gateway. Upon deactivating, GPS location and essential data will be sent back to the central server for filing police report purposes.

5.3.3 Application management

With tons and millions of mobile applications available in the market, whether it is from the legitimate or black market, a good management system for these applications need to be done especially on BYOD environment. This section will present about how BlueBoxEx help the corporation or organization in application management.

i. Application Whitelisting and Blacklisting

As a non-legitimate mobile application is the main source of method for malware writers to deploy their malware onto the victim, application whitelisting and blacklisting need to be done. BlueBoxEx will automatically search the latest report of malware from trusted sources for example F-secure, Trend Micro, Symantec, and Google News to periodically update the list of suggestions for admin to whitelist and blacklist the mobile application.

ii. Remote wipe and lock

If any unwanted or potentially high risk application is found, the admin will have the rights to remotely remove the application. Phone locking will be also take place if remote wiping is unable to perform the require task. Security administrator will collect the locked device and remove the application before unlocking the phone.

iii. Application inventory tracking

The application APIs data usage of each of every apps that installed in the particular device will be monitored in the working mode.

iv. Jail breaking/rooting detection

BlueBoxEx will perform scanning of the device to detect jail breaking / rooting device. If the device is jail broken, it will activate its defense mechanism that will be discussed in the next section.

5.3.4 Data protection

By securing the device is not the sole solution. Data is the main assets of the company and should also be one of the focus in securing BYOD environment. BlueBoxEx focus on providing an end to end data traffic encryption in order to secure the data.

i. Data traffic end to end encryption

BlueBoxEX identifies and dynamically encrypts corporate data on the device and in apps, and only allows files to be decrypted by BlueBoxEx-secured apps. BlueboxEx also provide secure corporate data traffic end-to-end from devices as well as cloud based and internal applications. With configurable, context-aware policies across devices, apps and networks, Bluebox further allows user to dynamically safeguard the corporate data and prevent data leakage.

ii. Defense mechanism on platform level vulnerabilities

BlueBoxEx will activate the defense mechanism to prevent privileges rooting. One step backward, the defense mechanism will lock down potentially unwanted applications from functioning during the working mode. Without the usage of potentially unwanted applications, potential attacking vectors can be stopped one step ahead. However, this solution might not be able to function properly in jail broken device. A password mechanism will be implemented when any privilege access is activated.

iii. Monitoring APIs usage to provide data analytics [41]

Behavioral tracking can be done by analyzing the pattern of API access operations of the user. An organization can detect and immediately report on any unusual usage patterns. Take a mobile device user that typically accesses certain API operations in a particular pattern. If their behavior suddenly changes, for example, as the result of theft, then an alert will be sent to the IT security team.

5.4 Evaluation of Proposed Solution

Similar to what have been done in the section where ATP was discussed, an evaluation of the proposed solution, BlueBoxEx has been done based on X.800 security services.

Table 5: The key evaluation of BlueBoxEx on the X.800 Security Services

X.800 security services	Achieved	Key evaluation
Authentication	✓	Two factor authentication including biometric The usage of unique API key
Access control	✓	VPN gateway Controlling file access based on the current mode Require password to access to certain phone module
Data confidentiality	✓	Secure network architecture Lost of device handling protocol Tracking of API usage
Data integrity	✓	End to end data traffic encryption
Non-repudiation	✓	Unique APIs key

The main components of X.800 along with the mapping of the features offered by BlueBoxEx. The summary of this section will be presented in a tabular form in Table 5.

6.0 CONCLUSION

In this paper, we have presented a survey of security challenges of BYOD environment in corporate and organizational. The possible attacks that might occur in a BYOD environment are identified and discussed, followed by the classification on top of it. Two main attacks were chosen and discussed in detail. The two main attacks are ATP and malware attack. We have also proposed some solutions to overcome the mentioned attack. Among them are BlueBoxEx. These proposed solutions are then evaluated based on X.800 security services. However, the proposed solutions in this paper are presented based on the literature review and survey that we have performed. Therefore, the proposed solutions in this paper lack of implementation through the real BYOD environment. In the near future, we will implement the proposed solution and evaluate it in a real BYOD environment to evaluate the performance of our proposed solutions.

REFERENCES

[1] Osterman Research by Dell, "The Need for IT to Get in Front of the BYOD Problem White Paper", January, 2013.
[2] Georg Disterer, Carsten Kleiner, BYOD Bring Your Own Device,CENTERIS 2013 - Conference on ENTERprise Information Systems / ProjMAN 2013 -International Conference on Project MANagement / HCIST 2013 - International Conference on Health and Social Care Information Systems and Technologies, May 2013
[3] Check Point Software Technologies Dimensional Research, "The Impact of Mobile Devices on Information Security", June, 2013.
[4] Lumension Information Security, "2013 Survey Results of BYOD & Mobile Security", 2013.
[5] iBanking: Exploiting the Full Potential of Android Malware [Online] http://www.symantec.com/connect/blogs/ibanking-exploiting-full-potential-android-malware Accessed date: 20/5/2014
[6] Owasp Mobile Security project https://www.owasp.org/index.php/ OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks Accessed Date : 20/5/2014
[7] SYBASE, "Mobility Advantage: Why Secure Your Mobile Devices? White Paper", February 2013.
[8] Jessica Keyes, "Bring Your Own Devices (BYOD) Survival Guide", CRC Press Taylor & Francis Group, Boca Raton, 2013
[9] Brian Prince (16th April 2014), SQL Injection Breaches Take Months to Uncover and Fix: Survey, [Online] Available: http://www.securityweek.com/sql-injection-breaches-take-months-uncover-and-fix-survey, Last Accessed Date: 23 May 2014.
[10] Dell Secure Works, "Anatomy of an Advanced Persistent Threat (APT)", 31 March, 2011.
[11] Command Five Pty Ltd, "Advanced Persistent Threats: A Decade in Review", June 2011.
[12] Why heartbleed could be much worse for android user [Online] http://bgr.com/2014/04/16/heartbleed-android-4-1-1-jelly-bean/ Accessed date: 17/5/2014
[13] Mobile Security Reference Architecture v1.0, CIO council, 23 May 2013
[14] Antonio Scarfo, Maticimind Spa, "New Security Perspectives Around BYOD, Wireless Computing", Communication and Applications, 2012.
[15] Johannes de Vries & Hans Hoogstraaten, "Systems for Detecting Advanced Persistent Threats", International Conference on Cyber Security, 2012.
[16] Tarique, Mustafa, "Malicious Data Leak Prevention and Purposeful Evasion Attacks: An Approach to Advanced Persistent Threat (APT) Management", Conference at IEEE, 2013.
[17] Websense, "Advanced Persistent Threats And Other Advanced Attacks White Paper", 2011
[18] iGR, "The Trusted Computing Group Mobile Specification: Securing Mobile Devices on Converged Networks White Paper", September, 2006.
[19] T. Andrew, Radu Vlas, Alan Yang & Cristina Vlas, "Risk Management in Era of BYOD", IEEE Computer Society, 2013.

[20] Sean Chung, Barbara & Yan Bai, "2TAC: Distributed Access Control Architecture for "Bring Your Own Device" Security", IEEE International Conference on BioMedical Computng, 2012.
[21] T. Ruesbsamen, and C. Reich, "Enhancing Mobile Devices Security by Security Level Integration in a Cloud Proxy", The Third International Conference on Cloud Computing, GRIDs, and Virtualization, Furtwangen, Germany, pp. 159-168, July 2012.
[22] R.G. Lenon, "Changing User Attitudes to Security in Bring Your Own Device (BYOD) & the Cloud", Computing Department, Ireland, 2012.
[23] Antonio Scarfo, Maticimind Spa, "New Security Perspectives Around BYOD, Wireless Computing", Communication and Applications, 2012.
[24] J.A, de Vries, "Towards a roadmap for development of intelligent data analysis based cyber attack detection systems", Delft University of Technology, 5th July 2012.
[25] iGR, "The Trusted Computing Group Mobile Specification: Securing Mobile Devices on Converged Networks White Paper", September, 2006.
[26] Wei Feng, "TEEM: A User Oriented Trusted Mobile Device for Multi-platform Security Applications", Institute of Software Academy of Sciences, 2013.
[27] Zhang Dawei and Han Zhen, "Protocol for Trusted Channel Based on Portable Trusted Module", Trusted Computing and Information Security, 2012.
[28] Kathleen N. McGill, "Trusted Mobile Devices: Requirements for a Mobile Trusted Platform Module", Johns Hopkins APL Technical Digest, vol. 32, 2013.
[29]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.
[30] Liqun Chen and Mark Ryan, "Attack, solution and verification for shared authorization data in TCG TPM", University of Birningham, UK, 2011.
[31] International Data Corporation; Apple Cedes Market Share in Smartphone Operating System Market as Android Surges and Windows Phone Gains, According to IDC; published 7 August 2013; http://www.idc.com/getdoc.jsp?containerId=prUS24257413.
[32] Cisco Security Threat Report 2014 [Online] https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf accessed date: 18/5/2014.
[33] F-Secure, "Mobile Threat Report Q3 2013", F-Secure Corporation, Helsinki, 5 November, 2013.
[34] Trend Micro, "Implementing BYOD plan" , Trend Micro Corporation [Online] http://www.trendmicro.com/cloud-content/us/pdfs/businessrep orts/rpt_implementing_byod_plans.pdf Accessed date : 17/5/2014
[35] Why heartbleed could be much worse for android user [Online] http://bgr.com/2014/04/16/heartbleed-android-4-1-1-jelly-bean/ Accessed date: 17/5/2014
[36] Ebay ask 145 million user to change their password after cyber attack [Online] http://uk.reuters.com/article/2014/05/21/uk-ebay-password-idUKKBN0E10ZL20140521 Accessed date: 20/5/2014
[37] BlueBox, "A New Era Dawns in Mobile Data Security", whitepaper, August 2013
[38] F-Secure, "Mobile Threat Report Q1 2013", F-Secure Corporation, Helsinki, 11 May, 2013.
[39] Mark Shepherdson, Trustmarque, "BYOD – the biometric implications" Volume 2013, Issue 4, Pages 5–7, April 2013
[40] John Thielens, "Why APIs are central to a BYOD security strategy", ScienceDirect network security Volume 2013, Issue 8, Pages 5–6 August 2013
[41] 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