Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 72 (2015) 129 – 136

Procedia Computer Science

The Third Information Systems International Conference

Trusted Security Policies for Tackling Advanced Persistent Threat via Spear Phishing in BYOD Environment

Lau Lap Bann[a], Manmeet Mahinderjit Singh[b]*, Azman Samsudin[c]

[a,b,c]*School of Computer Sciences , Universiti Sains Malaysia, 11800, Penang, Malaysia.*

Abstract

With the advent of pervasive and ubiquitous mobile devices, Bring Your Own Device (BYOD) trend is steadily gaining traction amongst many corporations, in allowing the extensive utilization of mobile devices in handling work-related data. However, there are several drawbacks to this approach, one of which is the risks resulted from the occurrence of Advanced Persistent Threat (APT). The goal of APT is to exfiltrate and leak important and sensitive corporate information through exploitation of vulnerabilities within BYOD environment. This paper addresses the APT issue via spear phishing attacks within BYOD environment, through the mediation provided by security policies. The devising of Mandatory Access Control (MAC) security policies using ACPT includes the implementation of environment attributes along with the specification of proposed policy rules for organizations is proven to be the most suitable policy mechanism for BYOD environment. Guidelines in mitigating APT via spear phishing are briefly discussed as well.

Peer-review under responsibility of organizing committee of Information Systems International Conference (ISICO2015)

Keywords: Security policy; Spear Phishing, Access Control Policy Tool (ACPT); OWASP risk rating methodology

1. Introduction

Bring Your Own Device (BYOD) is a rather well known approach implemented in most organizations where mobile devices and other portable devices like laptops and tablets are utilized in handling work-related data and applications. It is forecasted that 200 million out of 350 million mobile device users will be utilizing them in conjunction with the BYOD approach by the year 2016 [1].There are numerous benefits from enforcing BYOD approach in corporate organizations, in which few of them include an increase in employees' productivity and reduced hardware cost. However, there are drawbacks to the implementation, such as the invasion of location privacy, security vulnerabilities from the constraints of limiting resources within mobile devices and others that may belong. The lack of proper and standardized establishment of security policies in terms of safeguarding BYOD environment from malware attacks are another major drawback of BYOD approach. One of the major exploits in BYOD environment is the advanced persistent threat (APT).

APT is an intelligent and stealthy threat utilized by a group of highly motivated and resourceful perpetrators in order to extricate and leak important confidential data from the targeted political or

Peer-review under responsibility of organizing committee of Information Systems International Conference (ISICO2015)
doi:10.1016/j.procs.2015.12.113

business organizations. APT usually involves prolonged duration of covert monitoring approach in detecting vulnerabilities within targeted network, in order to infiltrate the network through the exploitation of the weak points from the vulnerabilities. APT is often hard to detect due to its capability to bypass traditional security defenses like host firewall, intrusion detection system and other security systems. There are several challenges with BYOD approaches [14]; 1) distinction of isolation between privacy of mobile users and work related data; 2) lack of security policies to safeguard BYOD environment from multiple security attacks; 3) vague definition of access control within mobile devices in conjunction with BYOD environment and 4) proneness of BYOD mobile devices to insider attacks

This paper addresses the issues of BYOD environment vulnerabilities resulting from APT via spear phishing attacks, through mediation of security policies in mitigating spear phishing attacks. Among the research objectives are i) to investigate and explore in depth on security policies and their correlation with multilevel security and access controls focusing in alleviating APT attacks; ii) to identify vulnerabilities and tactics most commonly employed by APT and to quantify the risks accordingly; iii) to propose and formulate multilevel security and access control policies that can mitigate APT via Spear Phishing efficiently and to evaluate the proposed security policies and record the result by benchmarking it against other security policies. The security policies proposed in this paper are to comply with MAC, Clark Wilson, LOMAC and ABAC.

The organization of the paper is as the following: Section 2 cover the background study of BYOD and APT attack. Section 3 and 4 are the methodology and security policy implementation sections. Section 5 presents the evaluation result and its discussion. Finally, a section on Conclusion is shared.

2. Background of BYOD and Advanced Persistent Threat (APT)

There are several notable security issues in BYOD environment. This is due to the fact that the mobile devices are lacking in terms of computational power and resources required to enforce security features in guarding against malware attacks. Direct threat like tampering and lost or theft of portable mobile devices are also becoming an issue in BYOD environment. Other indirect threats like interception of communication in BYOD environment is also another troublesome matter. Communication interception is often resulted from unprotected and unregulated transmission of corporate data involving insecure cloud-based services. Apart from that, employees are contributing factors in the occurrence of security issues within BYOD environment. The lack of security awareness amongst the employees has led to extensive abuse of organization data [2]. APT is a systematic and complex attack used by coordinated and highly skilled perpetrators to compromise machines and network over a prolonged time span in stealthy manner [3,14]. APT is first coined in US Air Force circa 2006 as it originally referred to nation-states stealing of data and defaming others for strategic gain [4]. APT exfiltrates data like customer records, source code, sensitive and confidential information to be stolen and leaked for sabotaging purposes. There are several key features of APT:

- **Targeted.** APT is highly intricate and targeted in selecting victims. Unlike common malware which are opportunistic and random in targeting victims, APT is focused and driven to exploit corporate or political bodies which contain sensitive and confidential information.
- **Advanced.** APT employs multitude of attack and intrusion techniques, such as social engineering and spear phishing emails with malicious payloads. Other than that, custom malicious codes and tools are used to exploit zero-day vulnerabilities in order to gain an advantage over the control of vulnerable network or machines prior to the knowledge of such vulnerabilities by the vendor or the security community.
- **Persistent.** APT is resilient in covert operations, in investigating and conducting a thorough background check on would-be victims, for example, APT operations can be time consuming as it may take months or even years to exfiltrate sensitive data from the targeted network without

triggering any risk of detection. This is to maximize the rate of success of APT operations in achieving the objective of leaking and stealing important data.

- **Evasive.** APT is generally elusive to traditional security defense mechanisms like firewall and intrusion prevention system which are often signature-based and thus hardly effective against zero-day vulnerabilities. Besides, APT also abuses commonly allowed protocols such as SMTP, HTTP and HTTPS. APT is often successful in operation due to the over dependent of business organizations on traditional security systems instead of a more multilayered security systems better at safeguarding BYOD environment against APT attack [5].

Access control models can be used to regulate controls through their capabilities of supporting segregations and integrity of different levels of information belonging to multiple parties [8]. The most basic and fundamental access control models are discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC) and attribute-based access control (ABAC). In general, security models provide access authorization based on the specification and enforcing of security policies. The common security models are Bell-La Padula model, BIBA model, Clark Wilson Integrity Model and Chinese Wall Model. Muthukumaran.et al. [10] proposed a multilevel security (MLS) system comprised of both MAC and Clark Wilson model. Low Water Mark access control (LOMAC) is introduced into the proposed solution.

3. Security Policy Methodology

There are five primary steps in this research methodology, namely, problem statement, identification of common APT vectors along with their probable risks, proposition and implementation of security policies, result analysis based on devised security policies and the evaluation and benchmarking of these policies. The problem statement addresses the first research objective in investigating security policies in alleviating APT via spear phishing attack. The hypothesis postulated is that the formulated security policies in this research will be more efficient in mitigating APT via spear phishing within BYOD environment. The identification of common APT vectors with risk quantifications conforms to the second research objective of identifying vulnerabilities and quantifying risks accordingly.

The next step is the proposition of security policies in mitigating APT via spear phishing attack, followed by the evaluation and benchmarking of these policies in accordance to quality metrics such as degree of least privilege support, degree of duty separation support and other metrics [11]. The most feasible security policy will be selected based on these metrics.The security policies proposed and to be formulated in this research are MAC, Clark Wilson integrity model, LOMAC and ABAC. MAC is selected for its scalability to a large population of users and strict implementation in preventing unauthorized disclosure of data at all cost [8]. Clark Wilson integrity model is well known for its practicality and commercially oriented features aside from its integrity protection through enforcement and certification. LOMAC is reliable and secure in terms of preventing movement of data from lower level to higher level objects. ABAC is context-aware as it captures real-time environment attributes to better enforce access control, for example, in sharing and managing information between organizations or departments.

4. Implementation of Security PolicyModels for APT threat in BYOD Environment

In this section, two phases employed in producing the benchmark result of the best security policy in thwarting spear –phishing in BYOD is presented. Phase 1 is the step in which risk quantification of the severity of sub-attack which leads to spear phishing is done. Overall, based on literature, APT sub-attacks method are social engineering, Pass-the-Hash (PtH) attack, SQL injection, waterhole attack and spear

phishing [11]. The attack with the highest severity is then used as an input to for preventive security rules in different security models discussed above. This is done in phase 2.

4.1 Phase 1: Risk Quantification Of APT Common Vectors

The common vectors employed in APT are social engineering, pass-the-hash (PtH) attack, SQL injection, waterhole attack and spear phishing [11]. The risks of each of these vectors are calculated using OWASP assessment calculator, which apply the OWASP risk rating methodology [12]. The factors are distinctly made up of 2 major factors comprising of likelihood factors and impact factors. Likelihood factors consist of threat agent factors and vulnerability factors, whereas the impact factors consist of technical impact and business impact. Table 1 shows the relationship of the likelihood and impact factors with the risk of APT vectors. According to Table 1, the vector with the highest risk is spear phishing, followed by waterhole attack and SQL injection. Pass-the-hash attack involves the least risk among the other vectors in comparison.

Table 1. Likelihood, Impact and Risk Factors of APT Common Vectors

Attack Vectors	Likelihood	Impact	Risk
Social Engineering	High (6.125)	Medium (3.625)	High
Pass-the-hash attack	Medium (4.25)	Medium (3.375)	Medium
SQL Injection	High (6.25)	Medium (4.875)	High
Waterhole Attack	High (6.75)	Medium (4.875)	High
Spear Phishing	High (7.125)	Medium (4.75)	High

Overall, spear phishing likelihood is the highest with 7.125 followed by waterhole and SQL injection when it comes to occurrence of APT. As the risk of spear phishing is high, the impact is at a medium rate in contrast to waterhole attack and SQL injection. As a result, spear phishing attack is further used to generate security policies as a preventive measurement.

4.2 Security Policies Specification Using Access Control Policy Tool (ACPT)

The security policies consisting of MAC, Clark Wilson, LOMAC and ABAC, as proposed in this research, are implemented and devised using ACPT by specifying the attributes for subject, resource, actions, environmental attributes and the associated permission. Access Control Policy Tool (ACPT) is a policy specification tool developed by National Institute of Standards and Technology (NIST) and North Carolina University [13]. ACPT is used to reduce human error and inaccuracy found in security policies crafted by administrators, through the rigorous verification of the security policies. As there is a limitation in term of space, only result of MAC is displayed here. The disclosure of other result is upon request.

A. Mandatory Access Control (MAC) for APT threat in BYOD environment

MAC security policy employs the multilevel approach through the definition of subject clearance level and object classification level, in which all subject and object are categorized into levels. Subject and

objects interact only within their respective categories, namely management, department and project. MAC security policy enforces no read up and no write down approach, along with several environment attributes. There are four environment attributes which checks and validates if an object is accessed during working hours, the condition in which the maximum number of access of an object within a day is specified, the guarantee of trusted and secure environment and verification of mail authenticity. Table 2 lists the properties and attributes of MAC security policy.The no read up approach is to prevent from unauthorized disclosure of highly sensitive data, in which only a subject with equal or higher level can read an object with a lower level. No write down approach is implemented as well.

B. Clark Wilson for APT threat in BYOD environment

Clark Wilson security policy is concerned with data integrity protection, especially in terms of the separation of duty among users. Subjects consist of employee, supervisor, security officer and system administrator, whereas objects are divided into corporate files, authorization list files, audit log files and email log files. The actions available are create, view, modify and delete. The environment attributes are defined in such a way that they ensure the certification and enforcement of integrity rules conforming to Clark Wilson policy, access within working hours, access within maximum number of access limit and the guarantee of trusted and secure environment. Employee and supervisor can only access corporate files and e- mail log files, whereas the security officer and system administrator can only access authorization list files and audit log files. The email log files and audit log files are created in automation, thus modify and delete access are prohibited for all users.

C. LOMAC for APT threat in BYOD environment

LOMAC is one of the MAC variant, which is similar but more integrity oriented compared to its counterpart. LOMAC emphasizes more on write operation rather than on read operation. No write up approach is implemented to protect data integrity, and that the level of subject is permanently demoted to that of the object accessed to prevent corruption of data by the subject after accessing previous object. The environmental attribute is to govern the permission of read up access, which is adjunct to the LOMAC security policy. Under any given circumstances, after accessing a lower level object, the subject is demoted to the same level as the previous object. A subject cannot write to an object with a higher level, in order to preserve the integrity of the confidential data from unauthorized modification or deletion.

D. ABAC for APT threat in BYOD environment

One of the key features of ABAC is its capability to regulate sharing of information between two organizations, and also the use of real-time environmental conditions to determine the access control. The subjects are distinguished based on department, organization and position, whereas objects are on department and organization.Subjects can either create, view, edit or delete an object. The environment attributes validate if access is done within the compound of the work premise, if an object is accessed within working hours, if other organization is allowed to create or edit objects from another organization.

There are three departments, namely human resources (HR), IT and Finance. Access to objects under these departments within the same organization are governed by the environment attributes which ensure conditions like access within work place and within working hours. Files from HR department can only be accessed by employee during working hours, whereas files from IT must be accessed within work compound. Finance department with sensitive files, must fulfill both requirement of within workplace and within working hours to ensure its integrity.As for supervisor within the same organization, all actions are

permitted for supervisors according to respective departments. However there is an exception in which supervisor from HR department can only view files from finance department. As for file access in between different organizations, environment attributes especiallyisOtherOrgCreate and isOtherOrgEdit are extensively applied to dictate policy for supervisors only, as employee are forbade from accessing files from other organisation.isOtherOrgCreate dictates if supervisor has the right to create or delete files from other organization, whereas isOtherOrgEdit dictates the right of supervisor to edit these files.

5.Summary of Quality Metrics Evaluation and Discussion

Every security policies devised are evaluated according to a series of quality metrics in order to gauge the performance of security policies in mitigating APT attacks via spear phishing. Table 2 summarizes the quality metrics with respect to MAC, Clark Wilson, LOMAC and ABAC security policies. Result obtained are based on various quality metrics evaluated using ACPT tool. Different scenarios on how spear phishing could impact the organization that employ different types of access control model are observed.

Table 2. Summary of Quality Metrics Evaluation

Quality Metrics	MAC	Clark Wilson	LOMAC	ABAC
Size of organisation	Large	Medium	Small	Large
Administrative Cost	High	Moderate	Low	High
Completeness	Stable	Stable	Less stable	Less stable
Complexity	Not complex	Moderate	Complex	Complex
Steps to assign and reassign User capabilities and Object Access Control Entries into Systems	More steps required	Moderate steps required	More steps required	Least steps required
Degree of Least Privilege Support	Least	More	Moderate	More
Support of Separation of Duty	Least	Most	Less	Significant
Number of Relationships Required to Create AC Policies	Most	Moderate	Moderate	Least
AC Coverage Across Platforms and Applications	Less	Less	Moderate	Most
Support for Safety	Highest	High	High	Lowest
Policy Conflicts that AC Systems can Resolve or Prevent	Occasional	Occasional	Probable	Less likely
Flexibilities of Configurations into Existing Systems	Least	Moderate	Moderate	Most
Integrity versus Confidentiality	Confidentiality	Integrity	Integrity	Least of both

The best security policy in terms of mitigating APT attacks conducted via spear phishing is MAC. This is due to the justification in which MAC is much more rigid and strict in implementation, as well as putting more focus on confidentiality. Both APT and spear phishing is carried out with the purpose of exhilarating sensitive data, which violates and exploits the aspect of data confidentiality. Both Clark Wilson and LOMAC security policies are more integrity oriented, which make them less suitable in the case of alleviating spear phishing issue. The information sharing feature facilitated in ABAC may expose the corporate system to adverse malicious exploits by the APT perpetrators. Thus, MAC security policy is deemed the best among other policies in mitigating APT especially induced by spear phishing.

One of the many guidelines in mitigating APT attack via spear phishing is the implementation of a well-defined security policy that clearly specifies and dictates the users' responsibilities and rights within BYOD environment, in order to achieve a proper balance between the privacy aspect of mobile device users and the security aspect of the corporate data. It is also vital to maintain and update the security policy from time to time to ensure its optimum regulation. Apart from that, monitoring of all network traffic through ports are recommended to mitigate APT attack. Numerous audition tools or log analyzer scan be utilized to keep track of inbound, outbound and internal network traffic for any potential unusual behavior. For instance, Database Activity Monitoring (DAM) monitors the access of sensitive data, and it can identify access attempts by an individual, which in turn triggers alert and block the access if the attempted access is unauthorized. The business or political corporations which are exposed to the risks of spear phishing and APT occurrences, should be vigilant and steadfast by constantly keep up with reliable trusted sources of global intelligence on the latest trends of targeted attacks and possible APT exploitations. Regular patching of security vulnerabilities within corporation environment is essential in guarding against APT via spear phishing attacks.

6. Conclusion& Future Work

As a conclusion, current BYOD approach is vulnerable to APT attacks, especially in the case of spear phishing exploitations. In this paper, the issue of spear phishing is thoroughly addressed by a series of objectives in order to mitigate APT via spear phishing. Different models of security policies are investigated by observing their features and characteristics by using security modesl such as ACPT. Prior step involve using risk rating model to study of the common vectors of APT attack. The reason of selecting spear phishing attack is due to the high risk and likelihood result obtained from the evaluation done. The MAC security policy is the most appropriate one for mitigating APT via spear phishing attacks. Reason being is because the nature of MAC security policy which is scalable to large user group, and it is strict in terms of enforcing data confidentiality, which is an important criteria in tackling the issue of spear phishing. As the recommendation for future work, the issues of multiple stakeholders in the implementation of access control within mobile devices as well as the standardization of these access control policies. The application of ACPT in coping with other APT-related attacks other than spear phishing is also listed as a possible expansion of the future work. In addition, the fine-tuning of security policies devised in this paper can be proposed and carried out in the future as well.

References

[1]Manmeet Mahinderjit Singh et al. (2014), "Security Attacks Taxonomy on Bring Your Own Devices (BYOD) Model", International Journal of Mobile, Network, Communication and Telematics (IJMNCT), ISSN : 1839-5678

[2]A. Pillay, H. Diaki, E. Nham, S. Senanayake, G. Tan, S. Deshpande, Does BYOD Increase Risks or Drive Benefits?, Melbourne, The University of Melbourne.

[3]Frankie Li, A Detailed Analysis of an Advanced Persistent Threat Malware, the SANS Institute, October 2011, [online] :http://www.sans.org/reading-room/whitepapers/malicious/detailed-analysis-advanced-persistent-threat-malware-33814

[4]Websense, "Advanced Persistent Threats And Other Advanced Attacks White Paper", 2011

[5]N. Leavitt (2013),"Todays Mobile Security Requires a New Approach", IEEE Computer Society Press Los Alamitos, CA, USA, Volume 46 Issue 11, November 2013, pp 16-19, doi:10.1109/MC.2013.400

[6]Advanced Persistence Threats : A Decade in Review, Command Five Pty Ltd., June 2011, [online] : http://www.commandfive.com/papers/C5_APT_ADecadeInReview.pdf

[7]S. Kim, D. Cho and S. Yeo, "Secure Model against APT in m-Connected SCADA Network," International Journal of Distributed Sensor Networks, vol. 2014, Article ID 594652, 8 pages, 2014. doi:10.1155/2014/594652

[8]V.J.R Wrinkler, Data Security in Cloud Computing – Part 3 Cloud Data Protection Methods. (August 8, 2011) [Online] : http://www.eetimes.com/document.asp?doc_id=1278993&page_number=2

[9]E. Coyne, &T. R. Weil (2013). ABAC and RBAC: Scalable, flexible, and auditable access management. IT Professional, 15(3), 0014-16

[10]D. Muthukumaran, J. Schiffman, M. Hassanm, A. Sawani, V. Rao, T. Jaeger (2009) Protecting the Integrity of Trusted Applications in Mobile Phone Systems, Security and Communication Networks, Security Comm. Networks, 4/6, pp 633 -650, doi : http://dx.doi.org/10.1002/sec.194

[11]ISACA, Advanced Persistent Threat Awareness Study Results, [online] : http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/wp_apt-survey-report.pdf

[12]OWASP Risk Rating Methodology, OWASP, (February 2015), [online] :https://www.owasp.org/index.php/How_to_value_the_real_risk_AoC#Informal_Method

[13]J. Hwang, T. Xie, V. C. Hu, M. Altunay, (July 2010), ACPT: A Tool for Modeling and Verifying Access Control Policies. In Policy(pp. 40 - 43)

[14] Zakiah Zulkefli, Manmeet Mahinderjit Singh , Nurul Hashimah Ahamed Hassain Malim; Advanced Persistent Threat Mitigation Using Multi Level Security – Access Control Framework; Computational Science and Its Applications -- ICCSA 2015 Volume 9158 of the series Lecture Notes in Computer Science pp 90-105