Improving Security in Bring Your Own Device (BYOD) Environment by Controlling Access

Musa Abubakar Muhammad, Aladdin Ayesh & Pooneh Bagheri Zadeh
School of Computer Science and Informatics
De Montfort University, The Gateway,
Leicester, LE1 9BH
Email: masmob@yahoo.com, aayesh@dmu.ac.uk, pooneh.bagherizadeh@dmu.ac.uk

***Abstract*—With the rapid increase in smartphones and tablets, Bring Your Own Devices (BYOD) has simplified computing by introducing the use of personally owned devices. These devices will help to ease access to business enterprise contents and networks. The effectiveness of BYOD offers several business benefits like employee job satisfaction, increased job efficiency and flexibility. However, allowing employees to bring their own devices could lead to a plethora of security issues; like data theft, unauthorized access, data leakage among others. This paper investigates current security approaches, and how organisations can leverage on these techniques regarding policies, risks, existing technologies, awareness and training to mitigate or halt potential security challenges. The research aimed to fill up the access control gap(s) in the existing Bring Your Own Device Environment by developing an adaptive security policy model.**

I. INTRODUCTION

Bring Your Own Device (BYOD) has tremendously changed the landscape of enterprise working environments especially at large organizations, where it increases employees flexibility, job satisfaction and reduce cost. Most commonly used mobile devices are smartphones and tablets. These devices are mostly relied upon for daily tasks such as shopping, listening to the news and chatting with friends, etc. BYOD exerts significant impact not only on daily activities but also saves cost for organizations; whereby IT related task are performed by the employees using their own devices [1],[2],[3],[4]. Employees find it desirable to use their personal devices in the workplace and make no distinction between their carrier services and that of their organisation. It is also an essential part of a corporate network that necessary measures need to be taken to protect organisational networks from threats [5]. As BYOD is acceptable, it is also a point of entry for attackers. Therefore, security policies need to be adopted to overcome the new security challenges posed by BYOD. Some of these difficulties included; loss of companys intellectual property, unauthorized or illegal access, application with embedded exploits downloaded by a user, malware infection and lost or stolen devices [3],[6]. The paper emphasizes a research intent that focuses on developing an adaptive security technique with an intelligent filter that will address prevailing access control issues based on user(employee) behaviour. Some of these user-based issues include: ability to detect new devices, analyse their security threat potentials and provide means to ameliorate the threats identified. However, this paper starts with a review of discussion of current BYOD security issues, threats, vulnerabilities and other related limitations. It further explains how the study will try to tackle access control related issues. The remaining part of the paper is arranged as follows: section II gives a background of the study, work done in the area along with their limitations, section III presents the proposed work, discussess the technique to be applied in answering the question and section IV concludes the paper.

II. BACKGROUND

The term Bring Your Own Device (BYOD) started in 2009. Intel recognized it earlier by allowing their employees to bring their devices to work and connect them to the corporate network. However, it took up to 2011 for other organizations to recognise it as a trend. Software vendors like CITRIX and Internet Service Providers like UNISYS popularized the trend. BYOD features a consumer enterprise [7], where mobility plays a significant role in business markets with high growth as technologies evolve [8]. Furthermore, there were some partnerships around enterprise mobility between Apple and IBM. In July 2014, Apple announced its partnership with IBM to push IOS 8 devices further into enterprise mobility management(EMM). IBM released hundreds of applications for IOS 8 aimed at industry sector together with analytics to exploit backend data generated by Apple devices. It believes that this kind of partnership could yield to operational savings, better security and productivity in the era of BYOD technology[7]. The use of personally owned devices will be of more benefit both to the employee and employers in conducting their daily tasks. In the next decade, IT enterprises operational costs will fall tremendously due to the diversity of BYOD technology [8],[9],[10]. Mobile devices and business environments are one of the fastest evolving trends in the computing landscape [4]. However, a failure to manage the proper configuration of policy servers by administrators could lead to widespread security problems in companys policies and controls, which will undoubtedly introduce privacy concerns. Apple mobile devices prevent applications from accessing users' personal pieces of information without permission. Users can only preview information they are allowed to access at given periods such as calendar, reminders photos, etc. Movement of data between the application and account installed by mobile device management and those by a user are restricted by the IOS Plat-

form [11],[12]. Multi-Platform Usable End Solution (MUSES) is an Open-source solution user-centric framework based on machine learning and computational intelligence techniques developed to improve the security and user policies on BYOD. The framework has a limitation in the rule enhancement due to its inability to generate the set of standards to deal with unknown or unexpected events; which could yield to security issues [13]. Mobile Device Management (MDM) focuses more on management rather than securing devices. Mobile Application Management (MAM) secures information residing on i.e. secure the mobile application, and accessed on the devices including policies. Mobile Information Management (MIM) emerges as an add-on to maintain the integrity of the enterprise information by encrypting the data in a secured container and in a centralized location[3],[4],[6],[14]. These solutions come up with strict policies that restrict users (employees') privilege(s) while protecting the organization. Existing solutions such as the integration of MDM with Network Access Control (NAC) for better access to the enterprise, purpotedly providing additional authentication and device authorization controls do not yield adequate security to BYOD environments[4]. Kernel Modification model allow MDM to modify the operating system of Android devices and create a profile that isolates company data from that of users. This model could make employees feel uncomfortable regarding the privacy of data on their devices. Virtual Private Network (VPN), access control model, protects the channel of communication while data on the device are left unprotected [15]. A remote mobile screen is an efficient approach whereby the user (employee) will access virtual mobile operating system to perform the task on their mobile devices. This approach has weaknesses in latency and connectivity, and data can be captured using screen shots [16]. Apparently, BYOD as a mobile technology; is also vulnerable to attacks like prior to mobile trends. The use of access control mechanisms to give permission based on user identity (ID) and roles are not sufficient due to their mobility nature. Existing security frameworks do not provide adequate ways to identify users (employee) behaviour on how they connect to the platform and threats on their mobile,etc. They mostly focus on monitoring and controlling the devices with strict policies [17]. The threats on BYOD are majorly of malware infections, unauthorised or illegal access, privilege escalation and disgruntled employees actions. Since they are mobile devices, they are also vulnerable to attack over the air, denial of service and mobile botnets. The limitations on the current mobile device management executions lead to unpredictable environments [18]. As mobile devices offer a near always connectivity to work environments, attackers employ lots of tricks to fool users into downloading malware with data theft capabilities, email interception and capturing[19]. Another concern arises from network access whereby the devices were connecting via external access points to public or unprotected wireless networks [20]. They may contain threats such as malware that can install itself when establishing a connection, which could result in mobile threats such as malware, spyware, attack over the air, denial of service and mobile botnets (Mobots)[3],[4].

III. PROPOSED MODEL

This research will adopt quantitative methods which would go a long way in resolving imminent research problems. It is noted that literature review alone would not be enough to resolve research gaps, since user pattern behaviours are going to be observed, and their potential threats analysed. . Using the quantitative methods may result in capturing the greatest outcome. For the data collection approach, user behaviour is going to be observed from captured and available datasets. It is expected that the collection process would adopt experimental analysis with matlab or any suitable tool, and the discrete values collected would be used to transform the data and formulate the facts in the research pattern. Thus, this study endeavor to close-up the gaps in access control on BYOD environments. Focus will be more on enhancing security using an adaptive security technique like the multi-level security approach within the platform and the device. An intelligent adaptive filter with the features of; identifying the behaviour of different users connecting to the platform based on their keystrokes, detect potential threats, and enabling a tougher access control. It is hoped that such ventures will bring about greater security and assurances of safety of personnel, and security of data in the contexts of confidentiality, integrity, availability, and non-repudiation in the BYOD environment.

A. Adaptive Security Technique

The adaptive security technique will be able to help in mitigating security breaches with capability for continuous tracking for potential security threats on devices. Also, preventing users (employees) from advanced attacks like phishing, and social engineering among others; by balancing the approaches organizations could apply to their business processes. The technique will improve access control on devices by patterning user (employee) behaviour and context to restore trust. These features will include the predictive measures to be taken, immediate response to any suspicious behaviour, monitoring capabilities for activities, and ways to anticipate them.

B. Intelligent Filter

This work conceptualizes ways to improve access control by authenticating users (employee) based on patterns and context information, and detecting abnormal employee behaviours based on the analysis of patternscontexts generated. Once, a new user tries to access the platform, user behavioural contexts will be recorded and added to the employee policy manager. This could be achieved by setting up the value to allow access to a limit, and denying access for contextual value less than the limit. In case of existing users (employees), the system checks the policies, compare the behavioural context for correspondence to known context before determining if or not to grant access. when access is denied due to lack of correspondence to existing context information, such device is registered suspicious, and profiled for potential threats before transiting to a subsequent system information safeguard stage in line with organisational requirement. User contextual information such as accessed date, time, location etc., will be

collected from the dataset sample from which comparisons of behaviours would be evaluated, and conclusions formulated. Figure 1 shows the proposed user profile creation process.

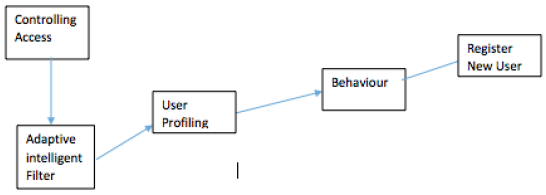

Fig. 1. User Profile Creation

Figure 1 is a stage where we generate a user profile. The adaptive intelligent filter plays a significant role in creating a new user by context analysis which involves; registering keystrokes, as well as monitoring and identifying user typing speed and accuracy. It then compares this user behavioural profile with existing registered profiles. This is further expounded in Figure 2

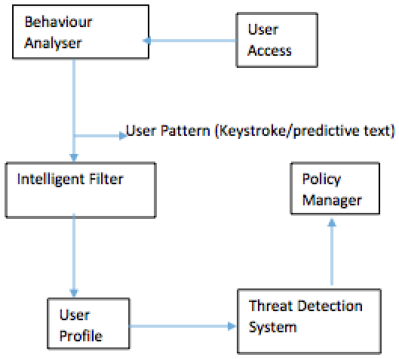

Fig. 2. Policy Creation

Figure 2 presents the behaviour Analyser, which uses a keystroke dynamic technique to process, record and monitor user related operations such as keys pressed, speed, and timing information to observe a user pattern. Also, it will help set a threshold to benchmark False Acceptance Rate (FAR) and False Rejection Rate (FRR) at an individual level; thus making a significant impact in monitoring and recording user behaviours (how the keys are pressed from left to right or vice versa etc.). The intelligent filter will use machine learning technique to learn and store behaviour of the user using the values identified by the behaviour analyser. The user Profile will compare the existing values with the new ones on the system, and allow transition to threat detection stage if the values correspond, or mark it as suspicious if values did not match. The threat detection will register the user as suspicious or not suspicious on the profile. The policy manager will create new and manage the existing systems to allow access (see figure 3), or register the user as suspicious.

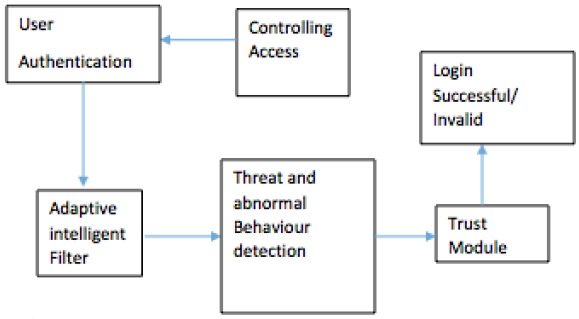

Fig. 3. User Access

Figure 3 Once a user tries authentication using their credential, the intelligent filter will perform its function in order to protect data theft, unauthorized or illegal access. This will be achieved by verifying installed policies on the policy manager, if the policy exist it will proceed then pass the authorization request to threat and abnormal detection system where it will verify correspondence before proceeding to the next stage.

IV. CONCLUSION

This paper discusses related BYOD security issues, highlighting the existing security frameworks as well as their limitations, likely threats and vulnerabilities therein. It aims to develop an adaptive access control security technique through the exploitation of behaviour profiling for user access by patterning user behaviour and monitoring their keystrokes in term of speed, time, etc, and using such context details to enable the protection of data, devices and users on Bring Your Own Device (BYOD) environments. This will explore validation means through experimental analysis in order to test and compare the result for a proof of concept.

REFERENCES

[1] C. Cascaval, "Special issue on mobile systems," *IEEE Micro*, vol. 35, no. 1, pp. 4–5, Jan. 2015.

[2] G. Costantino, F. Martinelli, A. Saracino, and D. Sgandurra, "Towards enforcing on-the-fly policies in byod environments," in *Information Assurance and Security (IAS), 2013 9th International Conference on*, Dec. 2013, pp. 61–65.

[3] M. Eslahi, M. V. Naseri, H. Hashim, N. M. Tahir, and E. H. M. Saad, "Byod: Current state and security challenges," in *Computer Applications and Industrial Electronics (ISCAIE), 2014 IEEE Symposium on*, Apr. 2014, pp. 189–192.

[4] M. Ketel and T. Shumate, "Bring your own device: Security technologies," in *SoutheastCon 2015*, Apr. 2015, pp. 1–7.

[5] N. Zahadat, P. Blessner, T. Blackburn, and B. A. Olson, "Byod security engineering: A framework and its analysis," *Computers & Security*, vol. 55, pp. 81–99, 2015.

[6] B. Morrow, "Byod security challenges: control and protect your most sensitive data," *Network Security*, vol. 2012, no. 12, pp. 5–8, 2012.

[7] P. Hunter, "Business in the wild," *Engineering Technology*, vol. 9, no. 11, pp. 60–62, Dec. 2014.

[8] R. Copeland and N. Crespi, "Analyzing consumerization - should enterprise business context determine session policy?" in *Intelligence in Next Generation Networks (ICIN), 2012 16th International Conference on*, Oct. 2012, pp. 187–193.

[9] A. Scarfo, "New security perspectives around byod," in *Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012 Seventh International Conference on*, Nov. 2012, pp. 446–451.

[10] P. C. Castro, J. W. Ligman, M. Pistoia, J. Ponzo, G. S. Thomas, S. P. Wood, and M. Baluda, "Enabling bring-your-own-device using mobile application instrumentation," *IBM Journal of Research and Development*, vol. 57, no. 6, pp. 7:1–7:11, Nov. 2013.

[11] S. Furnell, "Managing privacy settings: lots of options, but beyond control?" *Computer Fraud & Security*, vol. 2015, no. 4, pp. 8–13, 2015.

[12] Apple Inc., "iOS Security," no. September, p. 21, 2015. [Online]. Available: https://www.apple.com/business/docs/iOS{_}Security{_}Guide.pdf

[13] P. de las Cuevas, A. Mora, J. Merelo, P. Castillo, P. García-Sánchez, and A. Fernández-Ares, "Corporate security solutions for byod: A novel user-centric and self-adaptive system," *Computer Communications*, vol. 68, pp. 83–95, 2015.

[14] D. Jaramillo, R. Newhook, and N. Nassar, "Techniques and real world experiences in mobile device security," in *SOUTHEASTCON 2014, IEEE*, Mar. 2014, pp. 1–6.

[15] S. Ali, M. N. Qureshi, and A. G. Abbasi, "Analysis of BYOD Security Frameworks," pp. 56–61, 2015.

[16] S. G. Ocano, B. Ramamurthy, and Y. Wang, "Remote mobile screen (RMS): An approach for secure BYOD environments," *2015 International Conference on Computing, Networking and Communications, ICNC 2015*, pp. 52–56, 2015.

[17] Y. Wang, J. Wei, and K. Vangury, "Bring your own device security issues and challenges," in *Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th*, Jan. 2014, pp. 80–85.

[18] M. Ji, S. Kim, Y. Park, and J. H. Yi, "Mobile device management system with portable devices," in *Consumer Electronics (ISCE), 2015 IEEE International Symposium on*, Jun. 2015, pp. 1–2.

[19] M. Shaulov, "Bridging mobile security gaps," *Network Security*, vol. 2016, no. 1, pp. 5–8, 2016.

[20] G. Disterer and C. Kleiner, "Byodbring your own device," *HMD Praxis der Wirtschaftsinformatik*, vol. 50, no. 2, pp. 92–100, 2013.

[21] J. W. Creswell, *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications, 2013.