2016

Bring your own device: an overview of risk assessment

Robert Ogie
University of Wollongong, rogie@uow.edu.au

Publication Details

Ogie, R. (2016). Bring your own device: an overview of risk assessment. IEEE Consumer Electronics Magazine, 5 (1), 114-119.

Bring your own device: an overview of risk assessment

Abstract

As organizations constantly strive to improve strategies for ICT management, one of the major challenges they must tackle is bring your own device (BYOD). BYOD is a term that collectively refers to the related technologies, concepts, and policies in which employees are allowed to access internal corporate IT resources, such as databases and applications, using their personal mobile devices like smartphones, laptop computers, and tablet PCs [1]. It is a side effect of the consumerization of IT, a term used to describe the growing tendency of the new information technologies to emerge first in the consumer market and then spread into business and government organizations [2]. Basically, employees want to act in an "any-devices, anywhere" work style, performing personal activities during work and working activities during personal time [2]. There are several risks associated with BYOD [3, p. 63], and the big gaps in BYOD policies adopted by today's organizations [4, p. 194] show that the solution to BYOD is not well understood. This article establishes a background to understand BYOD risks by considering conditions that increase the occurrence of these risks and the consequences of the risks occurring. It then aims to present the most commonly adopted BYOD solutions, their limitations, and remedies, as well as important policy considerations for successfully implementing them.

Disciplines

Engineering | Science and Technology Studies

Publication Details

Ogie, R. (2016). Bring your own device: an overview of risk assessment. IEEE Consumer Electronics Magazine, 5 (1), 114-119.

Bring Your Own Device: An overview of risk assessment

R.I. Ogie[*]

Smart Infrastructure Facility, University of Wollongong, Northfields Ave, Wollongong NSW 2522, Australia

[*] Corresponding Author

Email: rogie@uow.edu.au
Phone: +61 (0) 2 4239 2535

Introduction

As organizations constantly strive to improve strategies for ICT management, one of the major challenges they must tackle is bring your own device (BYOD). BYOD is a term that collectively refers to the related technologies, concepts, and policies in which employees are allowed to access internal corporate IT resources, such as databases and applications, using their personal mobile devices like smartphones, laptop computers, and tablet PCs [1]. It is a side effect of the consumerization of IT, a term used to describe the growing tendency of the new information technologies to emerge first in the consumer market and then spread into business and government organizations [2]. Basically, employees want to act in an "any-devices, anywhere" work style, performing personal activities during work and working activities during personal time [2]. There are several risks associated with BYOD [3, p. 63], and the big gaps in BYOD policies adopted by today's organizations [4, p. 194] show that the solution to BYOD is not well understood. This article establishes a background to understand BYOD risks by considering conditions that increase the occurrence of these risks and the consequences of the risks occurring. It then aims to present the most commonly adopted BYOD solutions, their limitations, and remedies, as well as important policy considerations for successfully implementing them.

BYOD has gained huge popularity and adoption. A survey conducted by Cisco in 2012 on 600 companies reveals that 95% of the surveyed companies are already permitting the use of personally owned smart devices in their work environments and assets [1], [5, p. 54], [6, p. 65]. It is predicted that about half of all businesses will introduce a BYOD environment by 2017 [1]. Research also shows that even when BYOD is not permitted, a large number of employees still use their device for work [1], with or without the knowledge of the IT department [4, p. 192]. This popularity and adoption of BYOD can be attributed to several factors, one of which is increase in convenience and efficiency of work [1]. For most companies, the reason for embracing the BYOD phenomenon is simple and always the same: it improves their productivity and reduces costs [7], [8], [9, p. 612], [10, p. 14], [11]. Other factors include the rapid development and popularization of smart devices such as tablet PCs and smartphones [12, p. 101], increase in market-based mobile apps in rich public stores [13], implementation of the wireless Internet environment [3, p. 62], increased use of desktop virtualization and cloud services, increased emphasis on real-time communication, and work continuity [1]. The growth of BYOD has even extended into other aspects like bring your own technology [5, p. 53], [14], [15, p. 1] and bring your own software, in which employees use non-corporate software and technology on their device [3, p. 62].

Despite all the hype about BYOD, there are hidden costs and security risks [6, p. 65] that must be considered before adopting BYOD. A common misconception about BYOD is that having employees purchase their own devices can save the company money, but recent data prove contrary, considering that it could actually be more expensive because of the difficulty of managing various platforms and the fact that BYOD solutions require the company to pay voice and data service charges for their employees' devices [4, p. 193]. Companies sometimes only look at the cost of the device, but, when you look at the total picture, BYOD is more expensive [6, p. 66]. A recent study found that if a company with 1,000 mobile devices adopts BYOD, the company will spend an additional US$170,000 average per year [6, p. 65].

The hype about BYOD is further watered down if we consider BYOD risks and their consequences. BYOD risks include data loss/leakage or theft [11], [16, p. 12], [17], [18]; application security [16, p. 12]; network availability [17, p. 8]; legal liability and regulatory compliance [6, p. 65], [19, p. 5], [20, p. 29]; and loss of brand identity [6, p. 68].

Conditions that Increase the Occurrence of BYOD Risks

Certain factors increase the occurrence of BYOD risks. To start, when we allow enterprise and personal data to coexist on the same device, then it becomes very problematic to find a balance between a strict security control of enterprise and privacy of personal data, particularly when the device is not a corporate issued asset [3, p. 63]. This could also lead to data leakage if enterprise information is mistakenly sent to personal contacts [21, p. 9]. These devices are also always on and connected, so the vulnerability to malicious attacks increases through different communication channels [3, p. 63]. The situation becomes even worse when we consider that wireless connection environments on a smart device can be attacked more easily than desktop computer environments [22, p. 230].

In addition, it is very difficult for IT departments to support different phone/OS version/carrier combinations [6, p. 68], which are also constantly changing with technical advancement and get outdated very quickly [1], [3, p. 63], [21, p. 9]. Worse still, the extra portability of mobile devices poses serious challenges to the security of the devices, along with the information on them, as they can be very easily lost or stolen [3, p. 63]. We should also remember that because of the increased processing power and memory of smartphones and tablet computers, increased data transmission capabilities of the mobile phone networks, and open and third-party extensible operating systems for mobile devices, they become an interesting target for attackers [7]. These attackers rely on cyberweapons such as malware, spam, phishing, and fake Wi-Fi [22, p. 230], further increasing risk to BYOD [3, p. 63]. Some disgruntled employees may also share confidential business data on personal devices with competitors, leading to a competitive disadvantage for the organization [3, p. 63].

Consequences of the Occurrence of BYOD Risks

According to an industrial report, nearly 60% of companies are vulnerable to BYOD risks [4, p. 194], and there are several consequences that abound from the occurrence of these risks. Confidential data like e-mail, documents, reports, files, applications, usernames and passwords, installed certificates, banking information, and web accounts can be accessible if a device is compromised or if it lost/stolen. Spam received from known or unknown sources can also cause waste of resources such as bandwidth and memory space [3, p. 63].

It is being reported that nearly half of enterprises that allow employee-owned devices to connect to a company's network have experienced a data breach [8]. These breaches can attract compliance liability [4, p. 196], cost enterprises millions of dollars each year, and, more importantly, result in decreased customer trust or even complete loss of customers [12, p. 100].

With the adoption of BYOD, some companies have started to notice increased work activities during holiday leave as employees are tempted to check their e-mail and other work-related information [17, p. 7]. This can result in a huge problem when we consider that the use of home smartphones leads to increased work-to-life conflict, which, in turn, creates job stress [15, p. 5] and family conflict.

Methods

A search for relevant publications was undertaken first in Google Scholar and then other databases, including IEEE Xplore, Scopus, Web of Science, and ScienceDirect. The search terms *bring your own device, BYOD, bring your own technology, BYOT, mobile devices, IT consumerization, BYOD policy,* and *BYOD solution* were used as keywords to identify articles.

Peer-reviewed journals and conferences were prioritized, and all nonscholarly articles were removed, except for articles from trade journals that are peer-reviewed. Key information was then extracted from relevant publications using coding techniques.

BYOD Technical Solutions, Limitations, and Important Policy Considerations

The best defence in response to litigation arising from a data breach is to demonstrate that the company actively attempted to mitigate threats inherent in its business model [23]. It is, therefore, important for organizations to understand the different BYOD technical solutions and their limitations before adopting BYOD. These technological solutions can hardly stand alone; there is also a need to combine them with appropriate BYOD policies [24]. While we admit that it is difficult to enforce corporate policies on personal devices [21, p. 9], the first place to start when implementing BYOD still remains to establish a BYOD policy [25, p. 118] that leaves no gaps. Several studies have noted that there are big gaps in BYOD policies adopted by today's organizations. Table 1 presents the most commonly adopted BYOD solutions in the market, their limitations, and important policy considerations for successful implementation. It is also recommended that organizations consider other standard security measures applicable to the non-BYOD environment, such as robust firewalls, antimalware software [17, p. 9], authentication, SSL and TLS encryption, an intrusion detection system, identity and access management [19, p. 5], network access control, application access control, digital rights management, data loss prevention, and secure VPN connection.

Table 1: BYOD Solutions, Limitations, and Policy Considerations

BYOD Solution	Limitations and Proposed Solutions	Important Policy Considerations
Mobile Device Management (MDM): This is a technology that gives full control over mobile devices by using software solution to lock down, control, encrypt, and enforce policies on the devices [2]. An MDM consists of two components, an MDM agent which is installed on mobile devices and an MDM server which is used to communicate and control functions on the MDM agent [26, p. 190]. MDM considers three issues when managing devices namely, device management, security management, and file synchronisation [3, p. 68].	MDM solutions suffer from coarse granularity of control [4, p. 195]. A major limitation of this solution is that it is difficult to identify terminal context information. As a result, internal data leaks can be initiated by a malicious user through abnormal terminal behaviours, such as using a stolen terminal or a spoofed account, illegal temporary private wireless AP installation, connection and removal within the company. It is also difficult to detect internal data accesses and malicious behaviours as a result of abuse and misuse of the authority [1]. System-level network layer access and behavioural analysis for network data are also impossible [1].	IT department must adhere to organisation's policies and requirements when implementing device control [26, p. 190]. In order not to incur a fine or serious reputational damage as a result of breach of applicable monitoring and data protection legislation (e.g. Data Protection Act 1998, DPA), employers who wish to monitor employees' mobile devices must have policy in place that ensures they do so lawfully. They must also take steps to inform employees that their communications and use of the mobile devices may be monitored and why [31, p. 39].
MDM is a major step towards reducing data leakage, loss of organizational control and visibility [7].	Another major limitation of this solution is users' psychological repulsion to the control of personal devices. Users are reluctant about MDM agent installation on their personal devices in demanding their privacy protection [1].	End user must be educated about specific policies that guard the control of their mobile devices. Policy should include provision for enterprise and employees to sign an End User Agreement (EUA) to create a common understanding about liability [2].
An increasing number of organisations are undertaking the implementation of MDM [16, p. 12]. MDM has certain features which make it the first BYOD solution each organization wants to implement. Some of these features include device registration, connection setup, user authentication, passcode, encryption, and compliance, restrictions based on the use of device features or applications restrictions based on platform or version. Besides being able to configure profiles, time-based profiles, certificates, accounts, MDM can also be used to monitor policies, location, alerts, rules etc. [27, p. 154]. .Some popular vendors that provide MDM services include Vmware (AirWatch), MobileIron, and FiberLink [21, p. 10]. Other MDM tools include AmTel MDM, FancyFon [27, p. 155], Maas360, Zenprise MobileManager, and a lot more [11].	In addition, MDM blocks or even reset devices by relying on security policy specified through application black- or whitelists, without behavioural analysis in place (Armando, et al. 2014, p. 49). "These lists—and hence the policy—are often based on vague concepts" [13, p. 49]. Several solutions have being proposed to address this problems, including *BYODroid*, a prototype implementation of a security framework for the Android OS that validates behavioural models from applications against security policy, and hence ensures that only applications complying with the organisation security policy can be installed [28, p. 3], [29]. Similar work include the *secure meta-market* (SMM), which is a security-enabled application that enforces BYOD security policies through analysis and monitoring of multiple mobile applications [28], [29].	BYOD policy should state what are the companies' rights to audit and monitor privately owned devices during an investigation [17, p. 9] and this must be well communicated and agreed with the employees. Policy should address how MDM may be used to remotely lock or wipe data if tablet is stolen or lost [7] and for when employee leaves the company [21, p. 10]. For instance if the stolen tablet is a private device owned by the employee, rather than wiping a personal tablet, the company can compartmentalize corporate and personal data upfront with multiple profiles, for example, and decommission the device without harming anyone's personal files [7].
MDM can be applied specifically to only applications on a device instead of on the entire device. This is called Mobile Application Management (MAM) [27, p. 155], [2]. With MAM specific corporate applications can be locked down, controlled and secured, while everything else on the mobile device is left up to the user [2]. AirWatch by Vmware, is an example of a popular MAM [21, p. 10].	In addition, Costantino et al. [8] proposes a framework to enforce on-the-fly instantiated policies inside organization using trusted BYOD technologies. It implements a role-based access control system such that each user receives a specific policy from a server, based upon her identity or role and current context. The framework uses Oauth 2.0 to confirm effective user identity and Trusted Platform Module (TPM) installed on each device to ensure integrity [8].	BYOD policy should address how and when to obtain consent, if employer wishes to monitor employee's device [31, p. 39]. BYOD policy should clearly identify which devices can be used in the company network, listing both banned and allowed and apps, and describing categories of data that shouldn't be stored locally after being used by a mobile app [21, p. 10].
Similarly, MDM can be applied specifically to only critical corporate information on a device instead of on the entire device. This is called Mobile Information Management (MIM) [26, p. 190]. MIM could roughly be described as	Still in an effort to overcome the limitation of MDM to detect abnormal access and use of terminal devices on a real-time basis, Koh et al. [1] developed Dynamic Access Control System Based on Context. The system is comprised of a collection system to collect context information of a device under agentless mode, a detection system to detect users'	Backup and recovery strategies should also be

all those “Dropbox-like” cloud-based services that allow enterprise information to be stored in a central location and securely shared between different endpoints and platforms [2].	abnormal and malicious behaviours based on known user’s profile, and a control system to implement access control according to detection results and policies [1]. Devices are isolated and agent is installed if users/devices are detected to do abnormal or malicious behaviours while using networks [1]. This builds on previous study of abnormal behaviour detection in BYOD environment [9, p. 615]. Castro et al. [30] proposes *Secured Application Framework for Enterprise (SAFE)*, a comprehensive solution that enables enterprise and consumer applications to coexist side-by-side on the same device, giving the user a seamless experience. Unlike other solutions proposed above, this solution is designed to solve security and other related issues associated with using mobile applications in BYOD context.	addressed [4, p. 194]. Policy should stipulate the mobile operating system supported by the company. It is important to note that the OS of the device determines how the device connects to the company’s data, and what types of app can be installed as well [25, p. 119]. A certain OS might also be preferred or rejected based on security ground. For instance iOS operating system for Apple devices is susceptible to *jailbreaking* and Android devices are vulnerable to *rooting* [12, p. 103]. The same iOS has a security plus in that it enforces *application sandboxing* to isolate applications from each other, such that an application cannot access files in another application’s directory [32, p. 14]. To ensure that data removed from a device cannot be read elsewhere even if it is stolen or otherwise compromised, policy must enforce that data stored on devices should be encrypted [7].
Application virtualization and desktop virtualization: With virtualization, users remotely access computing resources at a corporate facility in such a way that corporate data is not stored and corporate apps are not processed on personal devices [21, p. 10]. End users receive just an image of their environment that runs in the datacentre or server network [2]. It is a security control in which aspects like firewall, anti-X, intrusion prevention, patching, backup, data encryption and even business continuity are addressed and managed centrally without leaving some tasks to the end users. Examples include solutions from Vmware and Citrix [2].	Although virtualisation may have its own peculiar technical and implementation issues, it stands out as being privacy-friendly when compared with other BYOD solutions like MDM. This is because it is a hand-off approach, where the enterprise strives to interfere less with the worker’s device [2]. There is therefore little or no issue of privacy invasion.	In order to prevent illegal data movement or remote storage misuse, virtualization systems should implement other critical points for policies enforcement. For instance policies to: (1) Deny cut and paste data transfers between the virtual desktop and the end-user’s local clipboard running on the client device. (2) Configure client drive redirection mechanisms to deny the ability to transfer files from the datacentre to the local device or vice-versa. (3) Deny end user’s printing ability within restrictive environments [2].

Discussion

This article sheds some light on the most commonly adopted BYOD solutions, with the aim to show their limitations and remedies as well as important policy considerations for successful implementation. Two types of BYOD solutions were considered: first, MDM and its MAM and MIM variations; and, second, application and desktop virtualization. We found that MDM is the first BYOD solution most organizations want to implement, yet it has several limitations, such as users’ psychological repulsion to the control of personal devices for privacy reasons, risks of basing policy on vague concepts, coarse granularity of control, and inadequacy in detecting users’ abnormal and malicious behaviours.

Although several ground-breaking solutions have been proposed to remedy these problems, some of these solutions may also attract privacy concerns and hence suffer from poor adoption. For instance, in the detection system “dynamic access control system based on context” proposed by Koh et al. [1], users are required to be profiled, and such data will normally include privacy-invading data about users such as location data [1]. This is a concern that can affect the adoption of this technology.

On the other hand, we found that application and desktop virtualization stands out as being privacy friendly because it is a hand-off approach and the enterprise interferes less with the worker's device [2]. Yet, application and desktop virtualization is not as popular as MDM. This could be a result of the high cost and difficulties associated with implementing and supporting application and desktop virtualization. In both cases, we also found that there are certain key policy considerations to take into account to successfully implement these solutions.

Conclusion

There are several risks associated with BYOD, and the solutions are not well understood. This article guides the choice of BYOD solution by showing the limitations and remedies, as well as important policy considerations for successfully implementing some of the most commonly adopted BYOD solutions. We found that application and desktop virtualization stands out as being privacy friendly when compared to MDM, but it is not yet as popular as MDM, which has several limitations. In both cases, we also found that there are certain key policy considerations to take into account to successfully implement these solutions. Future research will delve more into understanding the reasons why privacy friendly application and desktop virtualization is not as popular as MDM and how it can be improved to make it as desirable as MDM.

References

[1] E. B. Koh, J. Oh, and C. Im, "A study on security threats and dynamic access control technology for BYOD, Smart-work environment," in Proc. Int. MultiConf., vol. II, Hong Kong, Mar. 12–14, 2014.

[2] A. Scarfò, "New security perspectives around BYOD," in Proc. 7th Int. Conf. Broadband, Wireless Computing, Communication and Applications, Victoria, BC, Canada, Nov. 12–14, 2012, pp. 446–451.

[3] P. K. Gajar, A. Ghosh, and S. Rai, "Bring your own device (byod): Security risks and mitigating strategies," J. Global Res. Comput. Sci., vol. 4, no. 4, pp. 62–70, 2013.

[4] A. M. French, C. Guo, and J. P. Shim, "Current status, issues, and future of bring your own device," Commun. Assoc. Inform. Syst., vol. 35, no. 1, article 10, pp. 191–197, 2014.

[5] K. W. Miller, J. Voas, and G. F. Hurlburt, "BYOD: Security and privacy considerations," IT Pro, vol. 14, no. 5, pp. 53–55, 2012.

[6] C. Rose, "BYOD: An examination of bring your own device in business," Rev. Business Inform. Syst.–Second Quart., vol. 17, no. 2, pp. 65–70, 2013.

[7] S. Gallotto, and W. Chen, "Security management of bring-your-owndevices," in Proc. Int. Conf. Security and Management (SAM), Las Vegas, USA, July 21–24, 2014, p. 1.

[8] G. Costantino, F. Martinelli, A. Saracino, and D. Sgandurra, "Towards enforcing on-the-fly policies in BYOD environments," in Proc. 9th Int. Conf. Information Assurance and Security, USA, Dec. 4–6, 2013, pp. 61–65.

[9] D. Kang, J. Oh, and C. Im, "A study on abnormal behavior detection in BYOD environment," Int. J. Env. Ecol. Geol. Geophys. Eng., vol. 7, no. 12, pp. 612–615, 2013.

[10]S. Marshall, "IT consumerization: A case study of BYOD in a healthcare setting," Technol. Innovat. Manage. Rev. Mar. vol. 4, no. 3, pp. 14–18, 2014.

[11]Y. Wang, J. Wei, and K. Vangury, "Bring your own device security issues and

challenges," in Proc. IEEE 11th Consumer Communications and Networking Conference (CCNC), Jan. 2014, pp. 80–85.

[12]M. A. Harris, and K. P. Patten, "Mobile device security considerations for small- and medium-sized enterprise business mobility," Inform. Manage. Comput. Security, vol. 22, no. 1, pp. 97–114, 2014.

[13]A. Armando, G. Costa, A. Verderame, and A. Merlo, "Securing the 'bring your own device' paradigm," Computer, vol. 47, no. 6, pp. 48–56, 2014.

[14]A. Sedigh, C. Campbell, and K. Radhakrishnan, "BYOT Network Solutions for Enterprise Environment," in Proc. IEEE UKSim-AMSS 16th Int. Conf. Computer Modelling and Simulation (UKSim), Mar. 2014, pp. 489–493.

[15]N. Singh, "B.Y.O.D. genie is out of the bottle—'Devil Or Angel'," J. Business Manage. Social Sci. Res., vol. 1, no. 3, pp. 1–12, 2012.

[16]B. Tokuyoshi, "The security implications of BYOD," Netw. Security, vol. 2013, no. 4, pp. 12–13, 2013.

[17]P. Beckett, "BYOD–popular and problematic," Netw. Secur., vol. 2014, no. 9, pp. 7–9, 2014.

[18]I. Woodring and M. El-Said, "An economical cluster based system for detecting data leakage from BYOD," in Proc. IEEE 11th Int. Conf. Information Technology: N ew Generations (ITNG), Apr. 2014, pp. 610–611.

[19]B. Morrow, "BYOD security challenges: Control and protect your most sensitive data," Netw. Security, vol. 2012, no. 12, pp. 5–8, 2012.

[20] A. K. Jain, and D. Shanbhag, "Addressing security and privacy risks in mobile," IT Pro, Sept./Oct. 2012, pp. 28–33.

[21] C. C. Chang, W. C. Chieh, and S. C. Chen, "The influence of bring your own device on the psychological climate at workplace," in Proc. 16th Int. Conf. Electronic Commerce, Philadelphia, PA, Aug. 5–6, 2014, pp. 9.

[22] K. Kim, and S. P. Hong, "Study on enhancing vulnerability evaluations for BYOD security," Int. J. Security Appl., vol. 8, no. 4, pp. 229–238, 2014.

[23] R. E. Crossler, J. H. Long, T. M. Loraas, and B. S. Trinkle, "Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behaviour gap," J. Inform. Syst., vol. 28, no. 1, pp. 209–226, 2014.

[24] K. Madzima, M. Moyo, and H. Abdullah, "Is bring your own device an institutional information security risk for small-scale business organisations?," in Proc. Information Security for South Africa (ISSA), Johannesburg, Aug. 13–14, 2014, pp. 1–8.

[25] C. Caldwell, S. Zeltmann, and K. Griffin, "BYOD (Bring Your Own Device)," Compet. Forum, vol. 10, no. 2, pp. 117–121, 2012.

[26] M. Eslahi, M. V. Naseri, H. Hashim, N. M. Tahir, and E. H. M. Saad, "BYOD: Current state and security challenges," in Proc. IEEE Symp. Computer Applications and Industrial Electronics (ISCAIE), Penang, Malaysia, Apr. 7–8, 2014, pp. 189–192.

[27] V. Gupta, D. Sangroha, and L. Dhiman, "An approach to implement bring your own device (BYOD) securely," Int. J. Eng. Inov. Res., vol. 2, no. 2, pp. 154–156, 2013.

[28] A. Armando, G. Costa, and A. Merlo, "Enabling BYOD through secure meta-market," in Proc. 2014 ACM Conf. Security and Privacy in Wireless & Mobile Networks, Oxford, UK, July 23–25, 2014b, pp. 219–230.

[29] A. Armando, G. Costa, and A. Merlo, "Bring your own device," in Proc. 28th Annu. ACM Symp. Applied Computing, Coimbra, Portugal, Mar. 18–22, 2013, pp. 1852–1858.

[30] 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 J. Res. Dev., vol. 57, no. 6, pp. 7.1–7.11, 2013.

[31] C. Walker-Osborn, S. Mann, and V. Mann, "to BYOD or… not to BYOD," ITNow, vol.

55, no. 1, pp. 38–39, 2013.

[32] T. Werthmann, R. Hund, L. Davi, A. R. Sadeghi, and T. Holz, “PSiOS: Bring your own privacy & security to iOS devices” in Proc. 8th ACM SIGSAC Symp. Information, Computer and Communications Security, May 2013, pp. 13–24.