Awareness of BYOD Security Concerns

Benjamin Tillett-Wakeley

East Carolina University

Abstract

This paper will address security concerns relating to the Bring Your Own Device (BYOD) phenomena. BYOD is the ever-increasing trend of employees using mobile devices such as smart phones and tablets to perform work related tasks and access an organization's resources. This paper will explain the risks associated with mobile devices including mobile malware and a lack of inherent security. It will explain the risks associated with the fact that these devices often roam between wireless networks using cellular, WiFi, and Bluetooth antennas. It will also illustrate how users lack awareness about these potential security risks despite many of them using mobile devices for work every day. It will then emphasize how setting policies and using Mobile Device Management (MDM) to help enforce those policies is an important step in creating a safe BYOD environment.

Awareness of BYOD Security Concerns

Today's enterprise environment is continually facing changes as technology grows exponentially. Today, we have a slew of new phone and tablet devices that run on mobile operating systems much different from their desktop and laptop counterparts. Functions of these devices are increasingly used in place of functions that would normally be done on a PC. Workers want to take their email, word processing, and much more on the go. On one hand there are great benefits to be seen from this. Communication is quicker and easier than ever, and workers are more productive because they can work on the go and they can choose the device that they're most comfortable with. On the other hand, from a security standpoint, these new devices can be a can of worms. Not only are there now a number of new devices on your network that create new security vulnerabilities, but potentially confidential data is being downloaded to these devices that roam from network to network, and the devices themselves are easily lost or stolen due to their small form factor.

BYOD is the trend of enterprise environments to allow network users to connect their own devices such as smart phones, tablets, or laptops to the enterprise network and access resources and information on that network through these devices. These devices can be both personally owned and corporate owned devices, but even if they are corporate owned, this often means a mixture of personal and enterprise data resides on these devices as the devices will travel with the user between work, home, and often to public spaces. According to a study performed by Cisco partners in 2013, 92% of bring your own device (BYOD) workers use a

smartphone for work every week, and 62% use one every day. Only 42% of workers felt their employers were prepared for problems that could arise from their smartphone use (Cisco mConcierge, 2013).

In this paper we will take a look at the security risks that mobile devices bring to the enterprise environment. Such as the concern for malware that can be unknowingly downloaded, the potential for physical loss or theft of the device, and the potential for network based attacks with devices that so often roam and connect to many different networks. We will talk about best practices for mitigating these risks, and see what tools are available to help us do this.

Mobile Malware

Mobile malware is a concern for an enterprise environment because of the difference in control the enterprise has over these devices. Desktop software can easily be monitored and controlled when it comes to users downloading and installing software, but with smartphone and tablet devices an enterprise may have less knowledge of what is being downloaded on the device. Additionally these mobile devices invite users to browse app markets and download the plethora of free apps available to them. The majority of these apps are harmless, but some of them contain malicious or unwanted effects.

In a Q1 2014 report from the antivirus company F-Secure, they identified 275 new, so-called, “families” of malware on android devices (only 1 was found on iOS devices) (F-Secure, 2014). It should be noted that F-Secure found only 0.1% of apps from Google Play Store to be infected, while third party app stores that are mainly prevalent in china had a higher rate of infection (F-Secure, 2014). What do these

malware apps do once they infect devices? There is a variety of malicious activity performed by these malware apps such as: SMS sending that causes premium rate charges to the user's cellular plan. Downloading unsolicited apps in the background. Banking fraud that diverts banking related SMS messages. Stealing personal data such as pictures, documents, and contacts. Running the microphone, camera, and GPS in the background to spy on users. Creating a botnet of mobile devices to perform Distributed Denial of Service (DDoS) attacks, and even botnet malware that mines crypto-currency using CPU power from the mobile device (F-Secure, 2014).

Mitigating Malware

How do we avoid getting malware on our mobile devices? As noted, malware was much more prevalent on third party app markets. Downloading apps only from trusted markets such as Google Play and the iOS App Store will greatly decrease your chances of getting malware. This means that jailbroken iOS devices are more likely to download malware since they have access to third party app markets. In fact, malware for iOS is almost exclusively found on jailbroken phones (Felt, Finifter, Chin, Hanna, & Wagner, 2011). To mitigate against mobile malware it is best to avoid rooting or jailbreaking your phone, and to always update to the latest operating system version when possible. When downloading apps it is important to be cautious of apps that request unnecessary privileges. Interestingly however, malware apps tend to request only slightly more permissions than non-malicious apps (Felt, Finifter, Chin, Hanna, & Wagner, 2011), so it is important to note that this is not a fool proof way of knowing whether or not an app is malicious.

Inherent Vulnerabilities

Malware is an obvious risk, but it requires installing an app on the device to allow the device to be infected. So what risks are associated with mobile devices out of the box? One doesn't have to download a malicious app to be vulnerable to attacks on their mobile device. There are a number of security concerns that an average user is susceptible to from the moment they boot up their phone. These concerns include password protection and file encryption in the event of device theft or tampering, and the multiple wireless networks enabled on these devices that could all be used as a vector of attack.

Passwords and File Encryption

On average, 40% of smartphone users do not have password protection enabled (Cisco mConcierge, 2013). According to Consumer Reports, 3.1 million smartphones were stolen in 2013 (Tapellini, 2013). It should go without saying that a simple task such as setting a password goes a long way to protect confidential data with smartphone theft being so prevalent. There should be no reason not to set a password on a device that you carry with you everywhere. However, even with a password set, it's important to consider that the data on your phone will not be protected unless it is encrypted. For iOS devices, encryption is enabled by default and should protect your data if you have a password set on the device. Unfortunately for Android, encryption is not enabled by default on most devices, and even the latest version 5.0 does not require encryption to be enabled (Seppala, 2015). This means to protect confidential data on a mobile device, android users

need to go a step further and verify that encryption is enabled rather than simply setting a password.

Wireless Attacks

The wireless nature of these devices causes them to be susceptible to more network based attacks than a typical PC. As users connect to unsecure WiFi sources, such as ones at coffee shops or business conferences, they easily open themselves up to man in the middle attacks that allow for eavesdropping of unencrypted communications. It's simple enough to advise users against this practice, however because of the multiple wireless antennas embedded in these devices, we also need to consider that wireless attacks can be performed on these devices without a user connecting them to unscrupulous hotspots.

Bluetooth. Smartphone users often overlook Bluetooth as a network attack. Bluetooth creates a personal area network (PAN) with a typical range of 10-30 meters. Bluetooth can be used to connect to peripheral devices such as headsets and speakers. This is something that may either be enabled by default on mobile devices, or accidentally left on after connecting to a peripheral device. When Bluetooth is on it leaves devices open to a number of attacks. Some of the most notable Bluetooth attacks include bluesnarfing, bluejacking, and bluebugging. Bluesnarfing is an attack that uses exploits in the firmware of older devices to gain access to the device and even steal the International Mobile Station Equipment Identity (IMEI), allowing calls and messages going to a user's phone to be routed to an attacker's device instead. Bluejacking is an attack that sends unsolicited messages to a device via Bluetooth, and can result in phishing attacks that will allow an attacker to gain access to the

device. Bluebugging exploits a flaw in the firmware of peripheral devices, which allows an attacker to take control of the device and retrieve information from a paired phone or eavesdrop on messages and phone calls (Padgette, Scarfone, & Chen, 2012). To avoid the risks associated with Bluetooth, users should check to ensure that Bluetooth is turned off when not in use, and remember to toggle it off again after they are done connecting to a peripheral device. Cisco partners found that many users "don't even consider that their phones' Bluetooth discoverable modes may still be on" with 48% responding either "no" or "I don't know" when asked if Bluetooth discoverable mode is disabled (Cisco mConcierge, 2013).

Rogue cell towers. So far we've seen that we can mitigate most network attacks with very basic device settings and user awareness. When it comes to cellular networks however, this may not be entirely possible. In July 2014, ESD America, a company that produces the CryptoPhone (which encrypts calls and messages), reported finding more than a dozen rogue cell phone towers around the US. These rogue towers, also known as interceptors or IMSI catchers, are capable of eavesdropping on cell phone calls and text messaging, as well as pushing spyware data to devices that connect to them (Ragan, 2014). Protecting against this threat in a BYOD environment is not easy. One possibility is to use an app that provides encrypted messaging and encrypted Voice over IP (VoIP) calls. For example, Open Whisper Systems provides this with their RedPhone and Signal apps. Allowing both Android and iOS users to make calls and send messages with end-to-end encryption (Open Whisper Systems, 2014). Their app is both free and open source. The downside to this app is that your contacts need to also install the app on their device

for it to be useful, and the experience may not be as seamless as using the built-in apps on your smartphone.

Policies and MDM

Most of these security concerns can be effectively mitigated with proper security policies and user awareness. Having a policy that outlines things like password settings, encryption options, Bluetooth, and WiFi for mobile devices is a basic step toward having a more secure BYOD environment. Policies should define what devices are acceptable if the employee is using a personally owned device. For example, you may want to have version requirements on the operating system of the device, and disallow jailbroken or rooted phones. Policies should also outline appropriate usage of confidential information on mobile devices, and how that information should be stored. After creating a solid security policy that includes mobile devices, an administrator can implement Mobile Device Management (MDM) software to help ensure that policies are enforced. MDM software provides central management of all mobile devices to enforce policies such as requiring passwords and detecting rooted phones. An MDM profile is installed to a device whether it's a personal or corporate owned device. If it's a personal device, the profile can be deleted if the person leaves the company and corporate data associated with that profile would be removed with it. If the device is lost or stolen it can be remotely wiped, and an MDM interface allows for easy monitoring of all devices (AirWatch, 2013).

Conclusion

BYOD is here to stay, and organizations need to acknowledge that fact while making changes to mitigate the security concerns that come along with it. Employees are carrying around devices that potentially contain access to confidential information everywhere they go, often without a password, and often connecting to 3 separate types of wireless networks at a time. Organizations have tools at their disposal to help them manage these devices and mitigate the risk associated with them. Thus, the real problem with BYOD is not that it's unmanageable, it's that organizations either aren't aware of the risks associated with it, or are aware and are negligent in taking action to mitigate these risks. BYOD security policy and Mobile Device Management should become standard security tools to help mitigate potential risks that have come with the age of mobile devices.

References

AirWatch. (2013). *Bring Your Own Device (BYOD).* Retrieved from airwatch by vmware: http://www.air-watch.com/downloads/brochures/AirWatch_brochure_BYOD.pdf

Cisco mConcierge. (2013, March). *BYOD Insights 2013: A Cisco Partner Network Study.* Retrieved from Privacy Association: https://privacyassociation.org/media/pdf/knowledge_center/Cisco_BYOD_Insights_2013.pdf

Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011). A survey of mobile malware in the wild. *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices (SPSM '11)* (pp. 3-14). New York: ACM. *

F-Secure. (2014, March). *Mobile Threat Report.* Retrieved from F-Secure: https://www.f-secure.com/documents/996508/1030743/Mobile_Threat_Report_Q1_2014.pdf

Open Whisper Systems. (2014, July 29). *Free, Worldwide, Encrypted Phone Calls for iPhone.* Retrieved from Open Whisper Systems: https://whispersystems.org/blog/signal/

Padgette, J., Scarfone, K., & Chen, L. (2012, June). *Special Publication 800-121 Guide to Bluetooth Security.* Retrieved from National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf *

Ragan, S. (2014, September 17). *Rogue cell towers discovered in Washington, D.C.* Retrieved from CSO: http://www.csoonline.com/article/2684064/mobile-security/rogue-cell-towers-discovered-in-washington-dc.html

Seppala, T. J. (2015, March 2). *Google won't force Android encryption by default (update)*. Retrieved from engadget: http://www.engadget.com/2015/03/02/android-lollipop-automatic-encryption/

Tapellini, D. (2013, May 28). *Smart phone thefts rose to 3.1 million last year, Consumer Reports finds*. Retrieved from ConsumerReports.org: http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm