Securing BYOD Networks:

Inherent Vulnerabilities and Emerging Feasible Technologies

Arthur B. Herenandez, Young B. Choi*
Department of Business, Leadership, and Information Systems
College of Arts & Science
Regent University
1000 Regent University Drive
Virginia Beach, VA 23464
USA
*E-mail: ychoi {at} regent.edu

Abstract — **The security of Bring Your Own Device (BYOD) networking is evaluated. Mobile Device Management (MDM) software as the primary means of securely implementing BYOD functionality into networks is found insufficient. Best practices, both in terms of policy and technology, are presented to those intending to upgrade, or to those who have already upgraded networks to support BYOD.**

Keywords-Bring Your Own Device (BYOD); Mobile Device Management (MDM); Mobile Device Acceptable Use Policy

I. INTRODUCTION

The popularity of Bring Your Own Device (BYOD) networking is on the rise for enterprises. From 2013 to 2014, there was a 46% increase in companies who plan to support BYOD functionality in 2014, or 84% of all companies polled [1]. However, most of these companies intend to only implement a Mobile Device Management (MDM) to secure their BYOD network, or nothing at all. While MDM systems are designed to manage smartphones and tablet devices remotely, according to Clarke [1], a MDM system will not be enough to secure one's network. It requires a layered defense consisting of good practices, effective policies, and better technological solutions than what is currently available.

Therefore, we will discuss BYOD networking's inherent weaknesses, general guidelines to address these weaknesses including technological and policy-based solutions, we will evaluate current technologies utilized for this purpose, and provide a look into the future for BYOD networking including solutions that may be available in coming years. Weintend to provide network engineers and management with a primer in BYOD networking in order to empower them to move their enterprise into the future in a way that does not compromise their budget or their data's security.

II. BACKGROUND

Before Intelligent Operating System (iOS) and Android devices became so popular, the majority of employees privileged enough to enjoy a company-issued mobile device, were issued a laptop or a Blackberry device, or both. Laptops could be easily managed through Virtual Private Networks (VPNs), firewalls, and other commonplace network security architecture. To use Blackberry devices with one's network required only that the organization deploy a BlackBerry Enterprise Server (BES), which allowed network managers to control which devices connected to the network and what activities they could perform. The BES allowed the employees to synchronize their work calendar, contacts, and email with their mobile device and it provided limited access to certain applications and work files outside of the office. Network managers were satisfied with this configuration as BES servers supported both Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) "to protect and ensure the integrity of wireless data that is transmitted between the BlackBerry Enterprise Server components and devices [2]." Employees were satisfied because we didn't know how much better it could get.

Alas, the age of tablets and consumer-oriented smart phones are upon us, each ripe with its own unique vulnerabilities and threats waiting to spread to our network like a virulent sexually transmitted disease. Worst of all, the employees themselves purchase and manage these devices. Ever since most of tore apart our first Personal Computer (PC) at home, did we know that employees are our greatest threat, and now they have so much more power for ill. And so, we with hands tied behind our back, are now being asked by our management to secure the insecure and protect those that do not want to be protected. So, really…nothing has changed.

III. POLICY-BASED SOLUTIONS

The first step in implementing a BYOD network is effective planning. How will it affect your network? What are the new and/or elevated risks, and how can they be mitigated? Who will "own" the mobile devices? What services/files will you allow employees to access? Will you, and how could you go about, holding employees' accountable for issued and non-issued devices? What is your/their liability given someone committing a computer crime? These are a just a few of many

questions that swim in the minds of network engineers when proposed with the task of adding mobile device access to their network. Thus, these individuals should define or at least inform an enterprise-wide MDM (Mobile Device Management) policy, also known as a Mobile Device Acceptable Use Policy (MAUP).

According to Speed, Nykamp, Anderson, Nampalli, and Heiser a MAUP "is a formal agreement between an organization and the employees…[that] document[s] acceptable rules for mobile device usage…[and] review[s] any penalties that could be applied resulting from the rule violation from incorrect use of mobile devices" [3]. The MAUP should incorporate the concepts of the Security Systems Development Life Cycle (SecSDLC) including defining the procedures for implementing the BYOD network, the people who will manage this implementation, eligibility criteria to include one's device(s), hardware and software requirements necessary to implement the MDM policy, and what data will be accessible, and in what ways [4].

Also, as with other issue-specific security policies, it should include, at a minimum,1) a statement of purpose and the scope of the policy, 2) the philosophy of the organization concerning the implementation of the MDM policy, 3) fair and reasonable use as it applies to the data owned by the company, 4) liability on both sides, 5) unauthorized or prohibited use including context and repercussions, 6) employee monitoring policies (if applicable), 6) device management protocols (software updates, antivirus, back up procedures, and MDM agent requirements), 7) physical security requirements, 8) a statement about the importance of following the policy including any applicable legal or ethical regulations which are applicable, 9) the responsibilities of device owners, network managers, organizational leadership, and policy enforcers, if they are separate, 9) the policy review schedule, and 10) limitations of liability or any disclaimers that are applicable [4].

According to Midgley, an effective MDM policy, or MAUP, is built on three key pillars. Together these pillar "offer comprehensive visibility and control over all IT endpoints, anywhere, anytime" [5]. These pillars include: 1) framing the organization's mobility needs, 2) to defining the organization's security policy, and 3) offering and implementing device management and support solutions [5]. Midgley continued that by incorporating these three pillars into one's MAUP, the organization would reap the following benefits: 1) reduce risks and costs associated with elevated risk levels, 2) define a clear roadmap for the technological roll-out of the BYOD network topology, 3) enable an increased employee productivity, 4) potentially make new services and processes possible in the future, and/or 5) make existing services and/or processes more efficient [5].

IV. Technological Solutions

A. Mobile Device Management Systems

Network World reviewed six of the most popular MDM solutions AirWatch, Apperian EASE, BlackBerry Enterprise Server 10 (BES10), Divide, Fixmo, and Good Technology's Good for Enterprise [6]. Each of these six systems support a different configuration of supported devices including Android, iOS, BlackBerry, Windows, and a variety of other MAC products. Some support servers being placed on a Cloud, some on the premises of the organization, and some support both. They range in price. Network World did not rank any product higher than the others, but pointed out that they all have their strengths and weaknesses and should be chosen based on the needs of the network on which they would be installed.

B. Features of MDM Technologies

Some additional features of these MDM systems are offering a secure container, device control, application control, and file control. Creating a secure container overcomes the inherent weaknesses present in Android operating systems, which offer no inherent encryption or automatic access control devices, in of themselves. Creating a secure container means creating an encrypted and manageable data store restricted by an access control mechanism on the mobile device. Device control protects against unauthorized data transfers by allowing network managers to monitor and control which data are allowed to be transferred from servers to mobile devices. Application control, or app control, is the ability of a MDM to host and distribute Applications (apps) over-the-air, which have been approved and/or are required by network managers for mobile devices to connect to enterprise resources. File control is the ability to access network shares and to edit files from these shares from the mobile device, which then synchronizes to save edits on the network resource as well as the mobile device.

V. Implementing One of These MDMs on Your Network

There are many different ways to configure a MDM on to your network. However, as Strom pointed out, "assembling the various bits and pieces of a typical MDM solution isn't easy: in between the server and client components there is a lot of other stuff that interacts with a great portion of your network infrastructure [6]." He was referring to infrastructures such as Active Directory, Web proxies, servers, and firewalls [6]. For instance, connecting Fixmo's MDM to one's cloud server requires a supplemental VPN. Good Technology's product has a strong secure container and is fast and easy to deploy, but it has weak app and file control [6]. Divide is the best in terms of deployment ease and features, but it only supports iOS and Android devices [6]. Finally, AirWatch seems to be the most complete product with a separate MDM, a mobile content or file management, and mobile application control service, each managed by a single, integrated console delivered from a cloud or on the premises [6]. However, it is by far the hardest to deploy, though Strom stated that Airwatch offers a great deal of assistance in terms of video tutorials and comprehensive FAQs [6]. For these reasons, many equate MDM systems to a band aide to a much bigger problem.

VI. MDMs are not Enough

As Clarke pointed out, MDMs alone are not enough [1]. Rather, it needs to be incorporated within a strong forward-looking MAUP, and along with network tools that allow network managers to control bandwidth utilized by these devices in order of their priority, securing the network, controlling who gets access through automated device recognition, and recognizing when devices have been jail broken or rooted so that these devices are denied access. Some of these additional network tools include devices that perform fingerprinting, or inspecting a device's characteristics such as the device type, OS, and browser version to determine if it meets pre-determined metrics, and then allows the device to connect or not connect without having to address access privilege for each new device. Another network tool to accompany a MDM is Network Access Control (NAC) devices, or devices that automatically manage network access for mobile devices by determining the security posture of each mobile device. "NAC provides a deep inspection of the device to validate security apps, such as intrusion prevention, antivirus, anti-spam, anti-spyware, and anti-malware…if the device isn't equipped with …[them] NAC can limit access to corporate resources based on preset rules" [1]. After a device has been fingerprinted, and confirmed to have required security apps using NAC, then it can use 802.1x to authenticate users.

VII. Future solutions

Should we have to figure out how to make all of these technologies work together on our network in that pie-in-the-sky configuration that evenly balances network accessibility, efficiency, and security, all while navigating each vendor's updates and interfaces? No. That is not the world we live in. What we need is an integrated system that combines these network tools with a MDM and our Wireless Local Area Network (WLAN) security framework from one interface, and this system should come from a vetted, respectable vendor who we've worked with in the past. Do such systems exist?

Cisco's Secure Unified Access System is one such system. It combines an MDM with 802.1x, fingerprinting (profiling), posture assessments, device onboarding, and Guest Lifecycle management including network utilization tools that allow network managers to know who and what is connected to their network at all times and even the location of the devices [7]. This is all controlled with one interface and one set of updates to deal with. Fortunately, Cisco is not the only vendor to pick up on this need, and other vendors such as Brocade and Aruba Networks are collaborating to make a competitive product, but it will not be able available till 2017 [8].

VIII. Is a BYOD-Enabled Network Really More Risky?

Bergman et al. [9] stated that while statistics from IT vendors would have us believe that mobile networking is uniquely perilous, that in reality, it is merely a new variation on an old and known concept, securing a client-server model. That is not to say that mobile computing is safe. For instance, McAffee's Quarterly Threat Report showed a 1,200 percent in mobile malware in the first quarter of 2012 over the last quarter of 2011, Apple had six times more Common Vulnerabilities and Exposures (CVEs) for Code Execution in iOS from 2011 to 2012, and Android accounting for 98.5% of all mobile malware according to Kaspersky's Security Bulletin for 2013 [9, 10].

Bergman et al. [9] continued, the main difference between traditional threat architecture and that which is has become prevalent in mobile malware is that mobile malware is written in native code that is inherently insecure such as Objective C (iOS). Another key difference is the way in which mobile devices access our networks (through public WiFi mostly) which opens users up to Man-in-the-Middle Attacks (MiTM). In fact, most malware threats are variations of MiTM attacks [9]. Bergman et al. [9] also stated that the conglomeration of vendors (apps, OS, hardware, tele-carriers) that ends in the creation of a cell phone, means many, many hands in the cookie jar. Finally, the size and mobility of these devices make them easy to steal physically, and without authentication standards in place for each login, and perhaps with them, a company will be opened up to increased risks.

Therefore, some basic recommendations Bergman et al. [9] made, 1) do not store sensitive information on a mobile device if it is not completely necessary, 2) use a strong authentication method, 3) only allow users to connect certain apps which have been developed using best practices, and 4) do not rely only on a MDM system.

Two options Bergman mentioned for storing sensitive information on the phone itself, outside of creating an encrypted secure container, is to store sensitive information on a trusted cloud such as Apple's KeyChain. Another option is to use a Secure Element (SE) or a tamper resistant element that is embedded in the devices' Subscriber Identification Module (SIM) or a Secure Digital card (SD) card [9]. Bergman et al. [9] recommended two authentication methods Simple Security Assertion Markup Language Hypertext Preprocessor (SimpleSAMLphp) and Windows Identity Foundation which were not vulnerable to exploits that were easily bypassed using the other authentication methods tested.

IX. Best Practices for Securing BYOD Network

Along with these recommendations, the following are also some general best practices that should be implemented in order to ensure that your BYOD network does not open up your company to non-acceptable risks. These include:

- Doing third party penetration testing on your mobile networks using common vulnerabilities for mobile devices.
- Analyzing your WLAN logs for devices which are unrecognized.
- Base lining average app usage and running tests periodically to keep this information up-to-date.

- Be forward-looking with any new technological acquisition, ensuring that each device will be able to be integrated into your network and/or unified management system.
- Determine statistics about the number of employees that telecommute, use mobile devices on-premises, and current WLAN usage for upgrading purposes.
- Inventory each new piece of equipment and devices that connect including version, operation systems and systems testing notes on app development and keep this information up-to-date as part of your disaster recovery/business continuity plan as well as being prepared for emerging intrusions.

X. CONCLUSION

We discussed BYOD networking, how it is accomplished, policy and technological solutions, and an evaluation of the security and effectiveness of these technologies to accomplish BYOD networking. Some inherent vulnerabilities present in BYOD networking were discussed. Finally, We suggested some general best practices for BYOD networking.

REFERENCES

[1] P. Clarke, "Networking for the BYOD enterprise," Nemertes Research. 2013. http://www.hp.com/hpinfo/newsroom/press_kits/2013/GPC2013/BYOD_Business_Issues_Nemertes_Whitepaper.pdf

[2] Blackberry, Overview: BlackBerry Enterprise Server. 2014. http://docs.blackberry.com/en/admin/deliverables/25768/BES_overview_1275732_11.jsp

[3] T. Speed, D. Nykamp, J. Nampalli, and M. Heiser, Mobile security: How to decure, privatize, and recover your devices. 2013. [E-book]

[4] M. E. Whitman and H. J.Mattord, Principles of information security. Boston, MA; Course Cengage Learning. 2012. [4th ed.]

[5] S. Midgley, Navigating the consumerisation of the IT storm. In Bring Your Own Device: The mobile computing challenge. BCS Learning & Development Limited. 2013. [E-book]

[6] D. Strom, Review: Best tools for mobile device management. Network World.Dec,2013. http://www.networkworld.com/reviews/2013/120913-mobile-device-management-test-276534.html?page=1

[7] J. Heary and A. Woland, Cisco ISE for BYOD and Secure Unified Access. Cisco Press. 2013. [E-Book].

[8] J. Duffy, Cisco's Unified Access plan challenged. Network World. Sept, 2013.http://www.networkworld.com/community/blog/ciscos-unified-access-plan-challenged

[9] N. Bergman, M. Stanfield, J. Rouse, J. Scambray, S. Geethakumar, S. Deshmukh, S. Matsumoto, J. Steven and M. Price, Hacking exposed mobile: Security secrets & solutions, McGraw-Hill. 2013. [E-book]

[10] A. Funk and M. Garnaeva, Kaspersky Security Bulletin 2013: Overall statistics for 2013. Dec, 2013 . https://www.securelist.com/en/analysis/204792318/Kaspersky_Security_Bulletin_2013_Overall_statistics_for_2013

[11] A. Hernandez and Y. Choi, Securing BYOD Networks: Inherent Vulnerabilities and Emerging Technologies, CyberSecurity 2014, Stanford University, Stanford, California, USA, May 27-31, 2014.

.