The Report Committee for Nitsuh Asfaw Tesfaye
Certifies that this is the approved version of the following report:

An Analysis of BYOD Architectures in relation to Mitigating Security Risks

APPROVED BY
SUPERVISING COMMITTEE:

Suzanne Barber, Supervisor

Thomas Graser

An Analysis of BYOD Architectures in relation to Mitigating Security Risks

by

Nitsuh Asfaw Tesfaye, B.S.

Report

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Master of Science in Engineering

The University of Texas at Austin

May 2017

Abstract

An Analysis of BYOD Architectures in relation to Mitigating Security Risks

Nitsuh Asfaw Tesfaye, M.S.E.

The University of Texas at Austin, 2017

Supervisor: Suzanne Barber

As the adaptation of smartphones and tablets to conduct business activities increases, enterprise mobility becomes a rising trend in business environments providing a flexible work environment that modernizes how workers accomplish their tasks. One significant part of the current enterprise mobility movement is the adoption of the Bring Your Own Device (BYOD) strategy. BYOD allows employees to use their personal mobile devices to access corporate resources and conduct business tasks while maintaining the usage of these devices for personal activities. This underlying feature of the BYOD solution presents serious concerns for enterprises in terms of securing the storage and access of the corporate data. This report will explore the BYOD strategy and analyze the business requirements that are tied to the secure storage and management of corporate data. The report will also study existing architectural approaches as they relate to the BYOD movement, and explore how these approaches attempt to minimize the security risks and challenges associated with the BYOD strategy.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

1.1 Enterprise Mobility Management

In recent times, the use of mobile devices such as smartphones, tablets, and laptops for work-related tasks and activities has become extremely prevalent with the purpose of increasing productivity, providing flexibility for workers, shortening response time on business-related requests, fostering collaboration among workers, and increasing visibility to remote operations and sites. According to the International Data Corporation (IDC), by the year 2020, almost 75% of the US workforce will be mobile [1]. This indicates that the number of workers that will utilize mobile devices to conduct their work will cross over 105 million in the US alone [1]. In addition, a significant number of companies are now conducting their business in a 24/7 environment putting an emphasis on the need to have access to corporate data through mobile devices. As a result, many companies are investing in Enterprise Mobility Management (EMM) solutions to manage these devices as well as oversee the way employees access and store corporate owned data on those devices. According to a report published by the Global Industry Analysts (GIA), in 2014, the global EMM market was estimated to have stood at $86 billion and is anticipated to reach an estimated $218 billion by the year 2018 [2]. In the year 2022, this number is expected to increase to $510 billion worldwide [2].

Enterprise Mobility Management is an amalgamation of hardware components and software applications that allow enterprises to manage mobile devices, networks, and other services to enable employees to conduct business operations using mobile devices. EMM solutions provide corporations the ability to integrate business objectives, processes, and policies in how they manage mobile devices and provide a secure approach for accessing and storing corporate owned data. Depending on the business requirements, EMM solutions mainly provide capabilities for device management, app management, content management, email management, and security management [3]. However, based on each organization's needs, there could be overlap between these capabilities in order to fulfill all the business requirements.

EMM solutions that provide Mobile Device Management (MDM) are focused on monitoring, securing, controlling, and managing mobile devices across the enterprise. In most cases, MDM solutions have a service agent running as a daemon on the device and monitoring all underlying policies that are set by the enterprise [5]. MDM solutions usually provide features that include device configuration management, device access management, security protocol management, corporate policy enforcement, and device tracking. These features allow enterprises to perform actions such as remote data wipe, remote device wipe, remote device lock, jailbroken or rooted device detection, control access to applications by whitelisting or blacklisting specific applications, and push pre-defined network related or other service settings to the mobile device. MDM solutions also provide enterprises the capability of performing over-the-air application distribution as well as allow enterprises to push new enterprise policies or updates to existing policies to the mobile devices. Although, MDM solutions provide a variety of features and capabilities, the need for more granular, scalable, and flexible solutions has driven the market to produce mobility management solutions that provide a more specific function around a given area.

Mobile Application Management (MAM) is one of these solutions that provides features that allow enterprises to control, provision, and maintain mobile applications instead of managing the device as a whole. The focus of MAM solutions is to push as well as manage either internally developed applications unique to the organization or publically available applications used for work-related activities. These solutions provide a more granular approach to how enterprises administer mobile devices. MAM solutions allow enterprises to provide or block access to corporate applications, monitor application usage, monitor application data security, install or uninstall applications remotely, designate specific applications to be mandatory, and provide or block access to specific features of an application such as the ability to copy and paste corporate content, the ability to share corporate content, and the ability to download and store corporate data locally on the mobile device.

In addition to MDM or MAM solutions, there are also EMM solutions that provide capabilities for content management. Mobile Content Management (MCM) focuses on providing support for the secure access, storage, transmission, and sharing of corporate data using mobile devices. Among others, the data could be any file or document available on a local area network or accessible from other data repositories, encrypted or unencrypted attachments included as part of an email, and electronically archived corporate records. MCM solutions provide various features including data management, personal information management, document management, data push, data synchronization, secure web browsing, data sharing protections and policies, data version update, and location based access control [4] [5].

Mobile Email Management (MEM) is another specialized EMM solution that allows enterprises to containerize the access and storage of corporate related emails. Access to work-related emails on mobile devices is one of the most prevalent uses for EMM solutions. However, the access needs to be provided in a secure manner and provide protection for emails that may contain sensitive or confidential information or data. MEM solutions help achieve this goal by ensuring that all corporate related emails remain within a secure container and use advanced encryptions to protect the data from being compromised. In addition, MEM solutions allow enterprises to configure and enforce policies around user authentication, remote data access, secure attachment handling, and transferring or copying email content outside of the secure container [5].

Another specialized EMM solution focuses on Mobile Security Management (MSM) which allows enterprises to control the verification of mobile users as well as help enforce defined enterprise policies on registered devices. MSM solutions include features such as KIOSK mode, an approach that restricts what users can access on the mobile device while under the mode, password or passcode protection on devices and the level of protection required, device encryptions, device certificates, anti-virus support, anti-malware support, anti-phishing support, data loss protection, Single Sign-on (SSO) support, and mobile VPN.

1.2 Bring Your Own Device (BYOD)

With these range of EMM solutions available to enterprises, companies have the option to specify which device support strategy they will adopt in order to implement these solutions. The enhancement in the available technologies around this area has allowed various device support strategies to emerge. This includes initiatives such as Choose Your Own Device (CYOD), Corporate Owned Personally Enabled Device (COPE), Corporate Liable Employee Owned (CLEO), Corporate Owned Business Only (COBO), and Bring Your Own Device (BYOD).

This paper will focus on the BYOD initiative which allows employees to use their personal mobile devices for work-related activities. The BYOD concept presents employees with access to corporate owned data, corporate managed applications, corporate related records, managed networks, and web as well as other enterprise content through their own personally owned mobile devices. These business activities can include sending and receiving corporate emails, accessing and organizing their work calendar, accessing and managing their work contacts, accessing internal corporate websites and networks, managing and sharing work-related files, documents, folders, and other content, and installing and utilizing internal corporate applications.

The BYOD movement started in early 2009 at Intel where an increasing number of the company's employees started utilizing their own personal devices, including smartphones, tablets, and laptops, to connect to and access corporate network resources [8]. By early 2011, the movement had spread and achieved significant prominence allowing other companies such as Citrix and Unisys to start participating in the initiative. According to a report by Gartner, by the end of 2017 almost 90% of organizations will have adopted BYOD to some extent, while by 2018, it is predicted that employee-owned devices used for work-related activities will be twice more than corporate owned devices [8]. In addition, the BYOD market in the US is expected to increase from $24 billion to $58 billion between 2011 to 2017, while the global market for BYOD is estimated to grow from $67 billion to $181 billion during the same timeframe [8].

The significant adoption of the BYOD initiative in the enterprise environment can be attributed to several factors and advantages BYOD provides. The initiative enables enterprises to provide mobility to employees in a more cost-effective manner since the enterprise does not need to procure devices for employees. This saves money for the organization by eliminating the need to purchase and maintain hardware, software, insurance, and service agreements among others in order to provide mobility to workers [7]. In addition, employees will be more versed in the usage of a device they own versus one provided by the organization, which reduces the cost of training the company will need to provide for the employees. This also facilitates proficiency and efficiency in the usage of these devices to conduct work-related tasks as employees will usually feel more comfortable with their own personal devices than corporate issued ones. Additionally, BYOD also removes the cost of replacing devices due to loss or malfunction for the enterprise as the mobile device is owned by the employee. BYOD also benefits employees because it eliminates the need for the employee to carry and maintain two separate devices in their day-to-day activities in order to have access to company resources.

Chapter 2: Problem Formulation

2.1 Overview of BYOD Challenges

Although there are various advantages to implementing the BYOD strategy as part of an EMM solution, there are also significant challenges and issues that will need to be addressed when adopting the initiative. When implementing solutions that utilize corporate owned devices, enterprises can choose to supply their employees with a select number of mobile devices and provide support only for devices that are part of that set. These mobile devices might be chosen based on their operating system (OS), OS version, device type, device brand, or a combination thereof. With BYOD, this becomes very difficult to implement as employees are more likely to own a significant variety of device types. This will lead to the need for enterprises to provide and maintain support for a variety of hardware and software combinations. Similarly, BYOD also makes it difficult for enterprises to ensure devices are running using the latest software versions whether that applies to OS versions, firmware versions, or other applications running on the mobile devices.

Additionally, the support for the different device hardware and software combinations will cost the enterprise in terms of resources and money, since the organization will need to create and maintain applications and infrastructures that support multiple platforms. This creates an administrative overhead as it also requires setting and maintaining multiple policies and configurations to address the needs of the various device hardware and software combinations. Enterprises that adopt BYOD can also encounter scalability issues with respect to their network infrastructures. This is because today's mobile devices, such as smartphones and tablets, utilize a large amount of data and generate large quantities of network traffic. As more employees connect their personal mobile devices to the enterprise network simultaneously, there will be an increase in the usage of the enterprise's Wireless Local Area Network (WLAN) infrastructure.

Other challenges facing enterprises that adopt the BYOD strategy revolve around privacy and ownership concerns. This especially becomes an issue when enterprises attempt to monitor and collect device usage data. With corporate owned devices, enterprises can easily monitor the activities the employee is conducting on the device as a whole. This might include monitoring and collecting data about the location of the device through GPS, the applications installed on the device, what web content is being accessed using the device, and what data is being stored on the device. Additionally, the enterprise can also push remote commands to the device including commands that perform device wipe, device lock, data wipe, or even de-activation of network connections such as Wi-Fi and mobile data.

However, with the BYOD strategy this becomes much more complicated since the device is owned by the employee and also used to conduct personal related activities and tasks. This raises the issue of privacy with regards to what data can be collected about the device, what data can be collected about the employee's usage of the device, and what commands and policies administrators will be able to push to the device. This means that enterprises will have to ensure that they are only monitoring and collecting data when it relates to work-related activities and usage of corporate data. In addition, enterprises will also be limited to what type of restrictions they can enforce on the device including what public web content employees can access or what publically available applications employees can install and use on these devices.

2.2 BYOD SECURITY RISKS

Although all the previously mentioned issues and challenges are significant, one issue remains the most important challenge facing the BYOD strategy, and it is one that will be discussed throughout this paper, and that is the issue of security. The ability to conduct work-related activities on personal devices might present many benefits, but it also introduces a significant security risk for the enterprise. This is especially the case since BYOD strategies suffer from an end node problem. An end node problem refers to a device joining an untrusted network or being used to conduct riskier activities after being utilized for work-related activities under a trusted network [10] [11]. This exposes the enterprise network to security risks and can create cross contamination that can lead to security issues such as transporting malware from one network to the other, unauthorized access of sensitive data, and impersonation of trusted devices to perform malicious activities. This means that a compromised device on a corporate network can become an entry point for malicious activities as well as serve as a point of access to confidential or sensitive corporate records and data [12].

Moreover, as employees use these mobile devices for personal related activities, installations of any non-business related applications can result in inadvertently providing access to corporate data to those third-party applications. The installation of other personal related applications on the device can also pose a security risk, since some applications can introduce malicious software that compromises the integrity of the device. Jailbreaking or rooting personal devices can also lead to potential security issues as the process may introduce malicious software into the device. In addition, devices running older versions of software such as OS, firmware, or other applications can be susceptible to malicious attacks that may already have been addressed in later versions of the software. However, with BYOD, enterprises will have less say in how often employees update their device software to address these vulnerabilities.

Security risks can also be introduced when using the BYOD strategy given the portability nature of mobile devices. Mobile devices can easily be stolen or lost along with all the corporate related data and information they contain. This can lead to unauthorized entities having access to any unsecured data present on the device. In addition, the stolen or lost device can potentially be used as an entry point into the corporate network. In some instances, enterprises can also run into security risks if employees sell or give away their personal device but forget to wipe any corporate owned data or saved authentication credentials that might be present on the device. Employees can also decide to leave the company, and since their device is personally owned enterprises will not have the option of collecting back devices and ensuring all corporate data gets wiped from the device, as they commonly do with corporate owned ones. This means that enterprises run the risk of intentional or unintentional security breaches and unauthorized access of corporate data.

2.3 Security Threats

Many of the security risks associated with the BYOD strategy revolve around several well-known security threats. This section will discuss the 5 most challenging security threats associated with BYOD.

2.3.1 Malware

Malware is one of the most rapidly growing security threats associated with mobile devices and BYOD [12]. According to a report by Alcatel-Lucent, at any given time, an estimated 11.6 million mobile devices are infected with malware [12]. Mobile malware refers to malicious software targeting mobile devices that can cause the integrity of the device to collapse. Mobile malware can consist of any of the following malicious programs including Trojans, worms, spyware, viruses, botnets, and ghost push. Mobile malware can be introduced as embedded code within an application, as a link embedded in electronic communications such as emails and SMS messages that will redirect the user to a host that contains malicious content when accessed, or third-party application stores that may host malwares disguised as mobile applications. A device that is compromised with malware can be used to gain access to confidential corporate data, steal user credentials or sensitive information, or even potentially be used to ferry the malware into the corporate network.

2.3.2 Phishing and SMiShing Attacks

Phishing and SMiShing both refer to an attempt to electronically collect confidential or sensitive data by simulating another trustworthy entity. In the case of SMiShing, this is accomplished through the use of Short Message Service (SMS): the technology used for communicating through text messages. Phishing, on the other hand, is usually carried out using email spoofing: a method that involves sending email messages by forging a sender address that is trusted. Both Phishing and SMiShing usually involve sending electronic messages that direct the user to enter personal or confidential information in a webpage that mimics the look and feel of legitimate sources such as social media websites and banks or other trusted sources such as company IT administrators. These messages might also contain links that redirect users to other sites or hosts that contain malicious content including malware or hidden key-logger software.

2.3.3 Direct Attacks

With the BYOD strategy, malicious entities can also attempt to use compromised mobile devices to target and attack corporate networks and systems. The attacks could be executed as a coordinated effort to damage the availability of services tied to the enterprise's network and other infrastructures. The purpose of these types of attacks could be to access confidential information, edit or modify corporate owned data, delete or wipe enterprise records, or disseminate sensitive or confidential corporate information to a wider audience.

2.3.4 Data Leakage

In the BYOD strategy, data leakage refers to the intentional or unintentional distribution of corporate owned data to unauthorized entities. A data leakage can occur because of malicious device users, third-party application vulnerabilities, loss of device, remote access of device by malicious attackers, or installation of malicious applications. Data leakage can also occur unintentionally when employees install non-business applications on their device that might collect or access other data present on the device. Furthermore, in cases where the device is lost or stolen, sensitive or confidential corporate data that is not adequately secured might be viewed, altered, copied, transmitted, or deleted by unauthorized entities.

2.3.5 Data Interception and Network Spoofing

Another major security threat around BYOD is data interception that can occur when data sent from a mobile device is intercepted by an unauthorized entity. Attackers might initiate data interception by deploying fake network access points and luring mobile users to unknowingly connect to these access points; this is known as network spoofing [12]. Once the user has connected to the access point, the attacker can hijack the communication that transpires between the device and the corporate network. Through this method, attackers could gain access to sensitive corporate data or confidential information.

Chapter 3: Evaluation Criteria

3.1 Security Requirements

With BYOD, security vulnerabilities mainly arise from two principal sources: mobile users and mobile devices. When enterprises apply the BYOD strategy, most of the security threats discussed in the previous chapter can be connected to intentional or unintentional user activities including actions such as accessing malicious sites, links, files, or other content, installing unsafe or malicious third-party applications, connecting to vulnerable or malicious network access points, and sharing or providing access to corporate data to unauthorized entities. The other source of the security risk is the mobile device itself. These types of security risks usually arise from vulnerabilities tied to the hardware or software of the mobile device including OS vulnerabilities, firmware vulnerabilities, and security vulnerabilities around other services running on the device. Although no framework or strategy can guarantee failsafe security, many approaches attempt to minimize these risks and vulnerabilities to provide enterprises with a considerably secure infrastructure.

In this report, seven specific non-functional security requirements are created to serve as blueprints for investigating security elements that need to be addressed when implementing the BYOD strategy. Designing these security requirements provides a framework for analyzing which security challenges are addressed using a given approach. Each of these requirements tie into each of the BYOD security risks and challenges discussed in the report, and they help identify strategies that attempt to mitigate these risks. With this objective in mind, the requirements discussed below provide an outline for studying the approaches and their architectural framework.

3.1.1 Authentication and Authorization

In terms of BYOD, there are three stages of authentications and authorizations that need to be considered: device authentication, user authentication, and authentication specific to corporate services. In this case, the term *device* can refer to either the device as a whole or a section of the device such as a containerized area within the mobile device. The device authentication process should validate that only devices that can authenticate to the enterprise should be authorized to access corporate content or network. User authentication on the other hand should validate that only employees who are able to authenticate have access to the corporate data and network. User authentication should also involve authenticating a user's access to the device or any applications related to the enterprise that are installed on the device. This form of authentication might be accomplished by requiring a password, passcode, PIN, Touch ID or other forms of authentication that are applicable to the device type. The service authentication, on the other hand, should validate the identity of the device and user before granting access to specific services owned by the enterprise such as internal sites and hosts that contain content including records, folders, and files. This might be accomplished in collaboration with corporate VPNs or other enterprise authentication services.

3.1.2 Data Protection

One of the most significant concerns around BYOD is the protection of corporate owned data. BYOD involves using a mobile device for both personal and business activities, and as a result, corporate owned content will need to coexist with personal data. In this case, the partition between personal and corporate data can blur and the chance of a data breach or data leakage becomes significant. Data protection will need to encompass two main areas: security of data during transmission and security of data while stored. As mobile devices require remote connection with the enterprise through untrusted networks such as Wi-Fi and 3G/4G/LTE, there is a high potential for data interception or other security attacks on the integrity of the data during transmission. To combat these security risks, corporate data should always be encrypted during transit and should be checked for integrity and any malicious content at the corporate end-point. This might be achieved through an HTTPS session between the device and a gateway within the enterprise or by establishing an IPsec or SSL/TLS VPN connection between the device and a gateway within the enterprise. Furthermore, any at-rest corporate data should be protected while the device is online or offline through rigorous encryption. The corporate data might be stored on the device locally or on other third-party applications such as cloud services or other data backup services. Having an approach that provides considerable space isolation between the corporate and personal content provides a more secure environment for BYOD.

3.1.3 Access Control

In most enterprises, each employee is provided access to corporate data and resources based on their role within the organization. This access can include or exclude specific content based on the permission set by the enterprise. When providing access to corporate data through mobile devices, the enterprise should be able to set similar permissions and restrictions. Access control should allow enterprises to define which user can access what corporate content, which device can access what corporate content, and which device or user can access specific corporate services. Other access control should also be available to provide, limit, or block actions from being performed by specific users or devices as they relate to corporate resources and content.

3.1.4 Platform Integrity

Enterprises should also be able to ensure only mobile devices that have strong integrity have access to their corporate resources. Devices with compromised integrity will serve as potential security risks since implementing the security policies defined by the enterprise is fundamentally dependent on the ability of the device to enforce these policies. To validate the device platform integrity, there should be means of detecting whether a given mobile device is either jailbroken or rooted. There should also be support in place for detecting when a device becomes jailbroken or rooted after registration. Once these devices have been detected, enterprises should have the ability to allow or block access to their corporate resources. Furthermore, other device information such as OS type, OS version, and device brand should be detected to provide the enterprise with the option of enforcing restrictions to corporate resources based on one or a combination of these elements. This presents the enterprise with the advantage of limiting or blocking access to corporate resources if the enterprise becomes aware of any security vulnerabilities related to any of these device elements.

3.1.5 Application Control

Additionally, having the ability to allow or block specific applications from being installed on the mobile device provides a security boundary around enterprise data. Although this can be hard to fully implement on a device where complete control is not available, having the capability of whitelisting or blacklisting specific applications provides a considerable control around what applications can coexist with corporate data. Specific applications that could introduce potential security risks can be blacklisted and detection of these applications on a mobile device should result in enforcement of set enterprise security policies. Furthermore, whitelisting applications provides a security boundary for what applications can have access and share resources when it comes to corporate owned content. This might be accomplished by defining what applications are considered part of the BYOD product versus applications that are considered as running outside of the BYOD product.

3.1.6 Policy Enforcement and Compliance

With the BYOD strategy, enterprises will have less control over the management of the device as a whole and what actions can be conducted on the mobile device. As a result, effective user and security policies are necessary to minimize potential security risks. Enterprises should be able to define policies that govern the acceptable usage of personal mobile devices enrolled under BYOD. The policies can define items such as the type of authentication required to connect to and access corporate resources, the types of devices allowed to access corporate content, device management as it applies to corporate resources, application integration, and data storage management. Furthermore, policies can be created to govern a user's ability to perform actions such as copying or transferring corporate content, backing up corporate data to cloud services, accessing hyperlinks, encryption of email content, sharing of corporate data with other non-corporate applications, downloading corporate content locally to the device, storing corporate content locally on the device, and uploading content from the device to the corporate network and other services. Enterprises should have the capability to create, update, and remove these policies based on business requirements and any security vulnerabilities that may arise. Once the policies are in place, there should be an approach that provides auditing capabilities to detect any breaches of these set policies by a device or mobile user. Furthermore, enforceable device controls such as remote data wipe and remote data lock should be available to enterprises to combat any security risks that arise from devices that do not comply with these policies.

3.1.7 Monitoring and Data Collection

With BYOD, data collection and monitoring mobile device usage habits can be difficult as the device is used to conduct both private and business activities. Unlike corporate owned devices, collecting information around items such as device location, network usage, or even locally stored device content can raise concerns around employee privacy. As a result, event and data collection under BYOD should be geared towards monitoring activities that can lead to security vulnerabilities around corporate owned content. Monitoring activities such as any unauthorized access of corporate information on a device, downloading of corporate content without authorization, storing corporate data under non-corporate containers, inappropriate use of corporate email, inappropriate web usage related to corporate resources, and sharing of corporate data with unauthorized entities will allow enterprises to quickly respond to any potential security threats. Enabling the monitoring of these scenarios leads to detections of any intentional or unintentional activities that can result in security attacks. Additionally, exploring the collected data can reveal any security attacks, breaches, or suspicious activities that might have already occurred without detection. This provides the opportunity for the enterprise to evaluate the existing security measures that are already in place and investigate any additional policies or procedures that need to be implemented to strengthen these measures.

Security Requirements	**Features**
Authentication and Authorization	Device Authentication
	User Authentication
	Application Authentication
	Service Authentication
Data Protection	Encryption of Data during Transmission
	Data Integrity Check at End-point

Table 1: Features Associated with Each of the Security Requirements

	Encryption of Stored Data
Access Control	Access Level of Corporate Content per Group
	Access Level of Corporate Content per User
	Access Level of Corporate Content per Device
	Access Control Based on Device Status
	Access Control Based on Device Type
Platform Integrity	Detection of Jailbroken or Rooted Devices
	Detection of Device Type
	Detection of Device OS
	Detection of Device OS Version
	Detection of Other Device Information
Application Control	Whitelist Applications
	Blacklist Applications
	Manage Installation of Applications on Device
	Manage Access of Corporate Data by Application
	Manage Access of Corporate Services by Application
Policy Enforcement and Compliance	Define and Manage Group Level Security Policies
	Define and Manage User Level Security Policies
	Define and Manage Device Level Security Policies
	Enforce Defined Security Policies on Device
	Remote Data Wipe
	Remote Device Wipe
	Remote Data Lock
Monitoring and Data Collection	Monitor User Level Corporate Network and Content Access
	Monitor Device Level Corporate Network and Content Access
	Monitor and Collect Unauthorized Access of Corporate Infrastructures
	Monitor User Security Policy Compliance
	Monitor Device Security Policy Compliance
	Monitor for Suspicious or Malicious Activities on Corporate Network

Table 1, cont.

Chapter 4: Analysis

To study whether a given approach meets the defined security requirements, examining its high-level structure that serves as a blueprint for the overall system is a key aspect. The architecture of a system provides an abstraction or a structured framework that can be utilized to conceptualize elements and properties of the system and the relationship among these entities. In this paper, the system architecture is used to examine the approach and study how it relates to the seven requirements put forth in this report. Examining how well the given software architecture satisfies the defined security requirements will provide a constructive approach for analyzing a given strategy as it relates to BYOD security challenges. This chapter will study three specific BYOD approaches and it will examine their system framework in relation to the security requirements defined in the previous chapter.

4.1 Cisco BYOD Smart Solution

4.1.1 Overview

The Cisco BYOD Smart Solution is an approach that is based on combining elements across the network to provide secure device access, device policy control, and visibility to enterprises [14]. In terms of network structure, the Cisco BYOD solution builds on the Cisco Borderless Network Architecture and provides support for a variety of network connections including wired, Wi-Fi, and mobile networks such as 3G and 4G connections. In addition, the solution supports mobile devices as they move from one form of network connection to another. This includes switching from trusted corporate networks to other untrusted network access points. The solution also provides support for a wide range of device types, but available functionalities and features vary depending on the device type or its operating system. To provide its many features, the solution is not deployed as a single product, instead it is an amalgamation of different Cisco products, components, and services integrated to provide support for the strategy.

4.1.2 Solution Architecture

The high-level architecture of the Cisco BYOD Smart solution, as provided in [14, Fig. 2], contains five main components that interact with each other. These components include the BYOD mobile devices, supported network access types, the overall access infrastructure, off-premise gateways, and the security and policy infrastructure. Each of these architectural components utilize various Cisco services and components to provide the overall secure environment. For BYOD mobile devices, Cisco AnyConnect Secure Mobile Client is utilized to provide 802.1x supplicant capability while on trusted networks. This means that any mobile device that attempts to connect to the corporate network will be required to provide valid credentials and will need to authenticate before attaching to the corporate network and accessing any corporate resources. Furthermore, Cisco AnyConnect will provide VPN connectivity when mobile devices access the corporate network from other untrusted networks. The untrusted network could be a public internet access point, a public Wi-Fi hotspot, or a mobile data network such as 3G or 4G connection [14]. The VPN connectivity secures any traffic that flows between the mobile devices and the corporate network. Cisco AnyConnect will run in the background and automatically route network traffic as well as encrypt the data using Datagram Transport Layer Security (DTLS) over SSL or over Transport Layer Security (TLS). Additionally, the Cisco AnyConnect client can provide posture assessment of the mobile device and can be leveraged for some policy enforcements around device usage provisions [15].

Another core component of the Cisco BYOD solution architecture is the Cisco Identity Services Engine (ISE). This component provides several services including authentication, authorization, device profiling, certificate enrollment, posture assessment, policy definition and enforcement, and serves as an interface to identity stores [15]. These identity stores include other services such as Active Directory (AD), RSA SecurID, or other Certificate Authority (CA) servers. The service engine also presents an easier approach for registering devices under the BYOD solution and enrolling mobile device users. Furthermore, Cisco ISE serves as a policy-based service enablement that ensures mobile devices connected to the corporate network comply with any policies set by the enterprise. The service supplies device intelligence to the enterprise by performing device profiling of any endpoints connected to the corporate network. This allows enterprises to make proactive decisions around policy enforcement based on a posture assessment of the mobile device or the mobile user. During device profiling, a multitude of data is collected including the identity of the device, the identity of the user attempting to access the corporate network, the type of access being requested, the location of the requester, and the device type requesting the access [15]. Additionally, in conjunction with ISE, Cisco Prime Network Control System (NCS) provides visibility to endpoint connectivity so that enterprises might be able to troubleshoot any network problems that might arise. Cisco Prime can also be used for auditing and monitoring user activities while on the corporate network.

Cisco TrustSec Secure Group Access (SGA) is another component that is part of the solution architecture and provides the capability of defining logical policy groupings and assigning users to these groups to consistently maintain secure access of corporate content. TrustSec SGA allows enterprises to set access levels and permissions based on these groupings. As shown in Figure 1, specific users will be assigned to defined security groups and each group is provided access to specific corporate resources based on the policies defined by the enterprise. This approach decouples resource access control and management from being tied to specific IP addresses and allows enterprises to maintain large scale or granular policies based on the enterprise's needs.

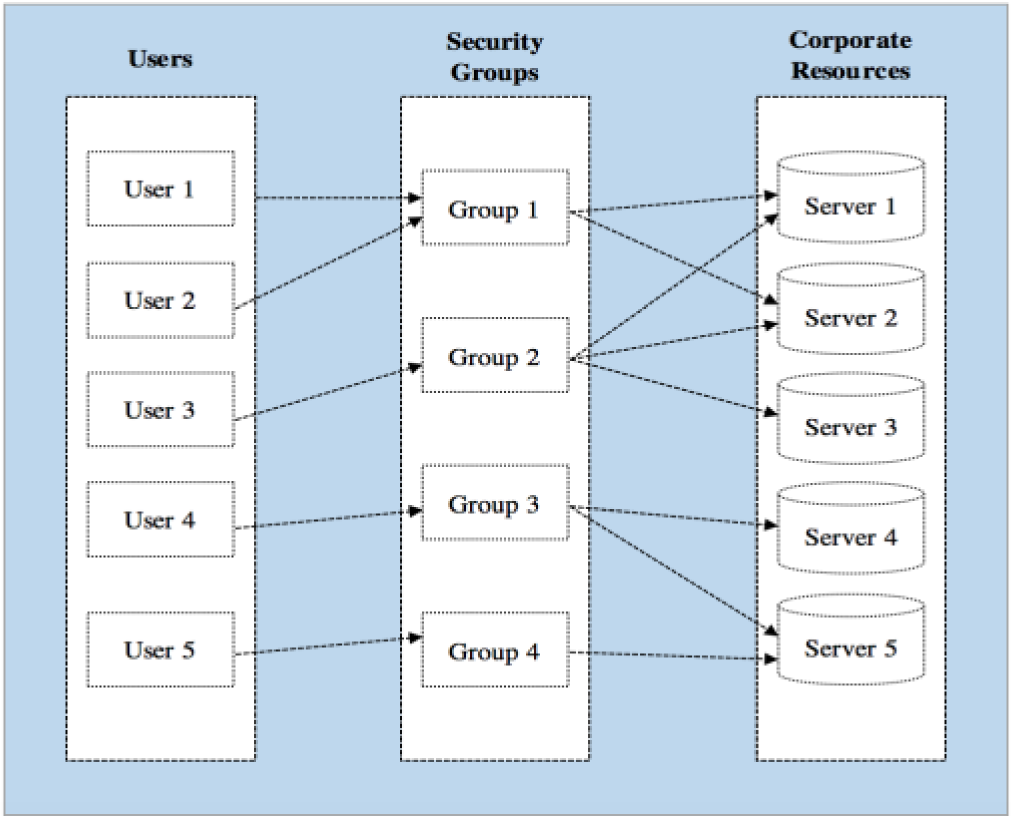

Figure 1: Secure Group Access Architecture

The Cisco Solution also relies on other connectivity and wireless configuration products to manage the enterprise network infrastructure and provide secure wired, wireless, and VPN connections. These products include the Cisco Catalyst Switches designed to provide wired network access and manage authentication requests with 802.1x, and Cisco Wireless LAN Access Points used to provide Wi-Fi connectivity for the corporate network as well as handle authentication requests via 802.1x. Cisco Integrated Services Routers (ISR) are also used to provide Wireless Access Network (WAN) connectivity, direct connectivity to the internet and cloud services, and serve as termination points for mobile device VPN connections [15]. Additionally, Cisco Wireless LAN Controller (WLC) is utilized for automating the configuration and management of wireless connection and interacts with the ISE to enforce the authorization and authentication policies defined by the enterprise across the different mobile devices [15].

To provide security threat protection, the Cisco BYOD Smart Solution implements Cisco Adaptive Security Appliance (ASA) that includes conventional firewall and Intrusion Prevention System (IPS) functionalities. The ASA solution contains capabilities for intrusion prevention, VPN and remote access, and some anti-virus, anti-phishing, anti-spam, URL blocking and filtering, and content control features [14] [15]. Additionally, the IPS solution provides protection for security threats such as worms, directed attacks, botnets, and SQL injection attacks [14]. For web security concerns, the solution includes Cisco ScanSafe Cloud Web Security (CWS) services which provides protection when accessing non-corporate web pages through untrusted network connections.

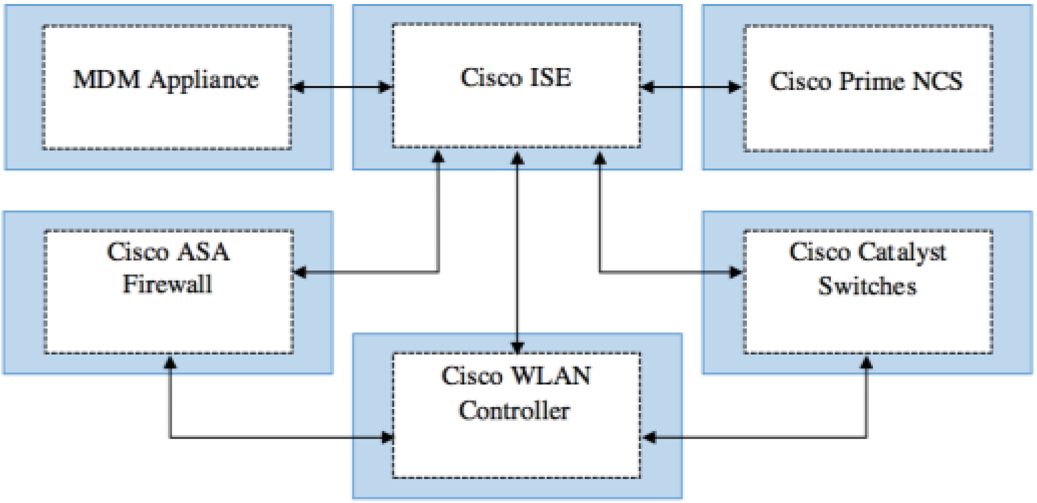

Figure 2: Products and their Relationships in the Solution Architecture.

4.1.3 Analysis Per Security Requirements

4.1.3.1 Authentication and Authorization

The Cisco BYOD solution fulfills the authentication and authorization security requirements as defined in Chapter 3. The Cisco ISE component provides the ability to register mobile devices to the BYOD solution. The service allows devices to be automatically registered and fingerprinted the first time they attach to the corporate network. After registration, the combination of ISE and Cisco AnyConnect Client validate that only authorized devices and users gain access to corporate network resources. Furthermore, third-party authentication services such as RSA SecurID can be integrated into the solution to provide two-factor authentication for a more stringent security. Additionally, Cisco AnyConnect can be utilized to authenticate with and have access to corporate contents and services such as internal corporate web pages, files, and documents to minimize the risk of unauthorized access.

4.1.3.2 Data Protection

When it comes to data protection, the solution as is does not provide any space isolation between personal data and enterprise data, and it does not implement containerization on the mobile device. Additionally, the solution by itself does not provide encryption of any at-rest data stored on the mobile device. However, other third-party MDM solutions can be integrated with the Cisco solution to address these limitations. Conversely, the Cisco solution does provide data protection during transmission on untrusted networks. This is achieved through the use of the Cisco AnyConnect client and the variety of wired and wireless network infrastructure components that are part of the solution.

4.1.3.3 Access Control

Access control is provided by the solution through the use of the TrustSec Secure Group Access component. This service allows enterprises to exercise access management and control through the creation of security groups. Enterprises will be able to define groups, assign users to these groups, and control what content each group can access through the solution. However, without integrating with other third-party MDM solutions enterprises will not be able to push down these policies to the mobile devices and enforce policies related to managing content on mobile devices or managing actions that can be performed on these devices when it comes to corporate content.

4.1.3.4 Platform Integrity

The Cisco solution allows enterprises to perform platform integrity inspections on mobile devices and provide or block access based on these inspections. Using the Cisco ISE component, enterprises can gather device profiles including device type, device OS version, and whether the device is jailbroken or rooted. Using these profiles the enterprise can set policies on what resources these devices can access based on one or a combination of elements from the device profile.

4.1.3.5 Application Control

The Cisco solution, as is, does not provide application control on mobile devices. Enterprises will need to integrate with other third-party MDM solutions to be able to manage or enforce policies around specific application installations or access on the BYOD device. Enterprises will also need to integrate with other MDM solutions to enforce policies regarding what corporate content could be shared with which application, and to be able to whitelist or blacklist applications to restrict access on the device.

4.1.3.6 Policy Enforcement and Compliance

The Cisco BYOD Smart solution allows enterprises to set, update, and remove policies that govern the access level to corporate resources and define the acceptable usage of the mobile devices while accessing corporate content. The Cisco ISE component provides functionalities for a centralized policy management resource and allows custom policies to be set based on a variety of elements. However, enforcing certain policies on the mobile device including those related to the user's ability to perform actions such as copy and paste, accessing hyperlinks, sharing corporate data, among others will require integration with other MDM solutions. The Smart solution by itself does not support the ability to manage, control, and enforce policies on the BYOD devices themselves.

4.1.3.7 Monitoring and Data Collection

The Cisco solution provides the ability to collect data and monitor access to corporate resources. This is achieved by Cisco ISE and Cisco Prime which allow enterprises to have visibility into device and user activity while using corporate network resources. Cisco Prime provides functionalities that allow enterprises to monitor any endpoint connectivity and endpoint security policy compliance. This includes real-time information collection from mobile devices, mobile users, and network activities across the corporate network infrastructure. Using this information, enterprises can monitor for network related issues, security vulnerabilities, and security attacks in real-time.

4.2 CITRIX MOBILE SOLUTION

4.2.1 Overview

The Citrix BYOD solution contains components for mobility management, file sharing, remote support and collaboration, desktop virtualization, and data isolation among others [16] [18]. The solution is an amalgamation of several entities that provide functionalities for device provisioning, web and SaaS application delivery, native application delivery, SharePoint integration, mobile application management, and mobile policy configuration and enforcement [17]. The approach combines two main elements to deliver these functionalities: XenMobile MDM and CloudGateway. XenMobile MDM provides the ability to configure, manage, and monitor mobile devices and validates that devices accessing corporate resources comply with the policies and provisions set by the enterprise. CloudGateway, on the other hand, serves as an enterprise application store and is used to deliver web, mobile, Windows, and SaaS applications to mobile devices. CloudGateway also provides capabilities for controlling access to corporate applications and data only to authorized users and devices.

4.2.2 Solution Architecture

The solution architecture, as shown in [17, Fig. 1], contains components for network and security infrastructure, app and data access control, device access control, support for enterprise application store, public as well as private cloud access, and secure data access and sharing. The main components of this solution architecture are XenMobile MDM and CloudGateway. XenMobile includes the following infrastructures to provide management and control of mobile end-points: XenMobile Device Manager, XenMobile Secure Mobile Gateway (SMG), and XenMobile SharePoint Data Leak Prevention (DLP). The second component of this architecture, CloudGateway, contains infrastructures for providing a self-service application store which include AppController, NetScaler Access Gateway, StoreFront, and ShareFile.

The XenMobile Device Manager component in the architecture provides device management capabilities that include provisioning and controlling mobile devices, access management for applications and corporate data, decommissioning devices that do not comply with set policies, and wiping corporate content from decommissioned devices. The Device Manager runs on a Windows server and allows devices to connect to it over pre-defined ports. Devices will enroll and connect to the server using the Citrix Mobile Enroll or Citrix Mobile Connect applications installed on the mobile devices. After enrollment, the Citrix Mobile Connect application will monitor and report security and policy compliance data from the mobile device. Furthermore, the MDM server connects to other infrastructures such as Active Directory, DNS, certificate authorities, SQL servers, and SMTPs for security and data access purposes. The MDM server also requires a Public Key Infrastructure (PKI) service to be present for data encryption and secure data transmission functions. If an external PKI service is not available, the MDM server contains its own PKI service that could be utilized with the Device Manager [16].

The XenMobile Secure Mobile Gateway component provides functionalities for protecting email access on mobile devices through MDM policies. SMG allows the viewing of corporate emails and encrypted email attachments on iOS and Android devices. The gateway can be installed on Microsoft Forefront Threat Management (TMG) server or on Exchange Client Access Server (CAS) and requires access to devices over HTTPS [16]. The gateway will also communicate with the MDM server to establish the MDM policies that need to be applied for a specific device or user.

The XenMobile SharePoint Data Leak Prevention (DLP) is an optional component within the architecture and allows access to SharePoint content on mobile devices. It also provides capabilities for managing access to the SharePoint data including providing, limiting, and blocking access to corporate data through the use of MDM policies. Furthermore, the Mobile Connect application servers as an interface to view and manage the SharePoint content on mobile devices.

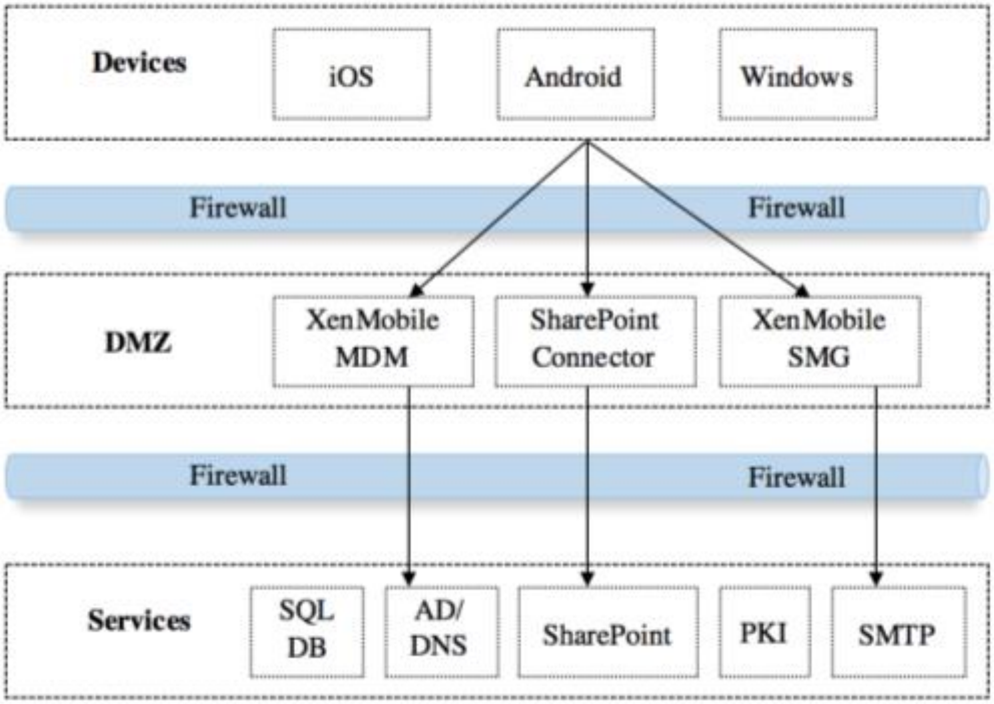

Figure 3: Architecture of XenMobile MDM (adapted from [16]).

AppController is another component of the architecture and is used to provide access to a variety of applications including web, SaaS, mobile, and Windows. AppController is deployed as a VPX appliance using a server and requires connections to NTP, LDAP, SMPT, and DNS servers [16]. AppController integrates with Citrix Receiver, a client used to access data and applications from mobile devices, in order for users to have access to applications without the enterprise setting up another peripheral server. Moreover, AppController provides support for single-factor authentication, verifying that a valid credential mapping is in place for a given user and application before granting access to a request. After a successful authentication, a direct connection is established between the device and the requested service. AppController also allows an SSO connector, such as Formfill and SAML, to be set up for a given application and provides capabilities for provisioning these connectors. This allows for creating, updating, and deleting user accounts as well as pushing remote commands such as resetting passwords, locking and unlocking accounts, and disabling and enabling accounts [17]. Moreover, AppController provides functionalities for publishing and managing access to mobile applications including corporate or other third-party applications. Application wrapping is implemented on these applications to allow for policy enforcement once the applications are running on mobile devices. Additionally, the CloudGateway MDX component along with the AppController allows for business applications and corporate data to be containerized and provides space isolation between personal and business contents residing on a device. This provides the ability to create and enforce policies specific to only the content within the business container. It also allows for encryption measures to be enabled for the business content as well as provide the ability to push remote commands such as data wipes and data locks to the containerized content.

Within the CloudGateway component, NetScaler Access Gateway is used to provide remote access to corporate resources while outside of the corporate network [17]. The Access Gateway is part of the De-Militarized Zone (DMZ) and serves as the main access point to the corporate network. StoreFront, on the other hand, is an optional component in the architecture and serves as a web interface that aggregates the list of available applications for a specific user. The last component within the CloudGateway is ShareFile, which is a cloud solution that provides storage, synchronization, and sharing of data within or outside of the enterprise. ShareFile serves as a data storage solution and provides access to the data based on the set provisions and policies.

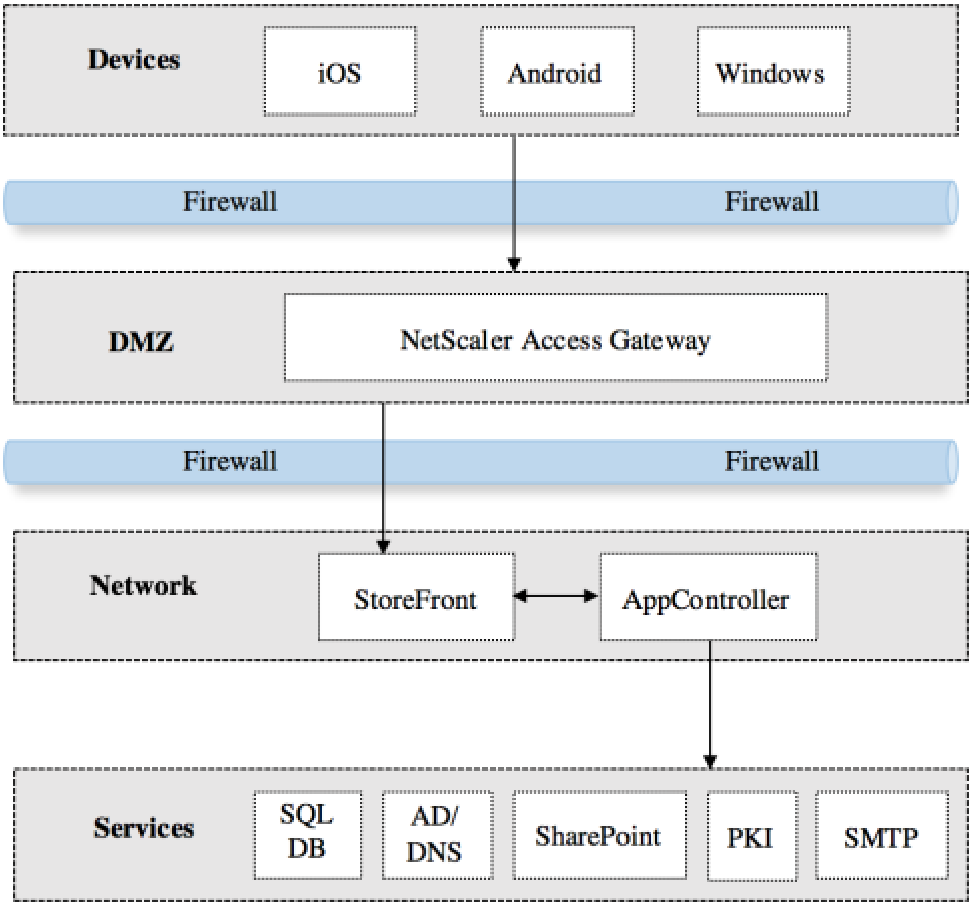

Figure 4: CloudGateway Component Architecture (adapted from [17]).

4.2.3 Analysis Per Security Requirements

4.2.3.1 Authentication and Authorization

Authentication and authorization services are provided through a combination of components comprising Device Manager, NetScaler Access Gateway, and AppController. The Device Manager uses a PKI service to deploy client certificates to mobile devices during enrollment. These certificates are used for client authentication to the MDM component. Once the device is enrolled, NetScaler Access Gateway is used to provide authentication to access the corporate network without the device joining the network as an end-point. For a more stringent security, a Remote Authentication Dial-In User Service (RADIUS) can be integrated into the architecture to perform two-factor authentication. Furthermore, after the device is enrolled, AppController provides a single-factor authentication in order for the device to have access to business applications. A credential mapping is used to transparently authenticate a given user's request to access a specific application and create a direct connection once the authentication is successful. This provides a Single-Sign On (SSO) experience to a user when requesting authorization to access a particular application. On the device side, the Citrix Receiver application is used as an authorization interface to provide authentication prior to opening any business application on a mobile device.

4.2.3.2 Data Protection

For data protection, the AppController component provides an application wrapping approach for space isolation between business and personal content on the device. The mobile applications deployed through the CloudGateway are wrapped before distribution and run within a container on the mobile device. This allows for control of the data within the container including being able to remotely wipe the data and revoke access after employees leave or a device is lost or stolen. The AppController component also provides data encryption for content that resides inside the container and allows applications within the container to interact and share content. Furthermore, enterprises can restrict or allow data access and application interaction between content inside the container versus outside the container. Additionally, the architecture contains the ShareFile component to encrypt and store corporate files and documents and provides cloud-based access to the data to authorized mobile devices. For data protection during transmission, the NetScaler Access Gateway provides encryption capabilities for network traffic outside of the corporate network.

4.2.3.3 Access Control

For access control, as defined in the requirements presented in Chapter 3, the solution utilizes the MDM and CloudGateway components to control user group creation and management, although both components do not allow the creation of nested groups. Based on the group the user is allocated to, access to specific corporate resources and applications can be controlled by the enterprise. Additionally, with these components in place, access to corporate data and applications can be limited based on user or device status, location, or other policy provisions set by the enterprise.

4.2.3.4 Platform Integrity

With this architecture, platform integrity can be detected through the MDX technologies integrated into the solution. These technologies allow for detection of jailbroken or rooted devices. They also provide capabilities for setting policies that govern how these devices are managed once identified and whether these devices can access corporate resources. The architecture supports iOS, Android, and Windows devices and provides the ability to collect device status information including OS version, OS type, and other data that could be utilized to measure the required platform integrity level by the enterprise.

4.2.3.5 Application Control

The AppController component within the architecture allows for controlling access to mobile applications distributed by the enterprise or other third-party entities. Any applications available for a given user are displayed within Citrix Receiver and users will be able to install these applications on their devices. The applications available to a given user can be defined and controlled by the enterprise through the use of application tunnels or blacklisting and whitelisting applications using provisions and policies. Additionally, polices can be established through the solution for accessing applications while the device is offline, the amount of time applications and corporate data will be accessible after a device goes offline, whether an application can be installed on devices that have been jailbroken or rooted, and application lock and data wipe when access is revoked. Moreover, the solution allows enterprises to remotely push application updates and mark updates as mandatory or define a given timeframe for when these updates need to be installed. This allows enterprises to control the business-related application versions running on the BYOD devices.

4.2.3.6 Policy Enforcement and Compliance

Policy enforcement and monitoring device compliance, as defined in the Chapter 3 requirements, is accomplished through a combination of MDM and CloudGateway components. As discussed in this Chapter, the architecture allows for an assortment of policies to be defined that govern and manage several areas. These policies might include disabling and enabling device camera access, allowing or blocking cloud usage, restricting copying and pasting corporate content outside of the business container, or restricting corporate data storage on the device, among many others. Other policies that govern which applications a user can access and what environmental conditions are necessary for the user to access these applications can also be defined by the enterprise. Once these policies are pushed to the mobile devices, Mobile Connect which will be installed on these devices will be used to enforce the set policies and monitor for any compliance failures. When a compliance failure is detected, the set conditional actions are applied on the device including data wipe or data lock.

4.2.3.7 Monitoring and Data Collection

Monitoring and data collection functionalities are handled by the MDM component with support from other CloudGateway elements. The MDM component allows enterprises to log information related to device and user activities around corporate data, network resources, and applications, and view the collected data for any security risks and vulnerabilities. It also allows for monitoring of mobile devices in conjunction with the Mobile Connect application around policy compliance and corporate resource usage activities.

4.3 SAMSUNG KNOX

4.3.1 Overview

Samsung KNOX is an Android specific solution designed as a suite of security features that allow personal data to coexist with secure content on the mobile device [19] [20]. KNOX implements a containerization technique to provide space isolation between enterprise and personal content and allows enterprise content to be deployed in an isolated environment that could be controlled through MDM platforms. On compatible Android devices, the solution creates a virtual partition that would divide corporate content such as applications and data from other personal content on the device. This is achieved by splitting the CPU of the Android device into two environments: a secure environment and a personal environment. The secure environment will run inside a TrustZone-based Trusted Execution Environment (TEE) and hosts a secure operating system that runs parallel to the personal one and stores and processes protected content. Each environment utilizes its own set of system resources and while the secure environment can access resources from the personal environment, the personal environment will not be able to access resources from the secure environment.

4.3.2 Solution Architecture

The solution architecture is composed of elements that focus on three main attributes: platform security, application security, and mobile device management. To provide platform security, the architecture contains three main strategies that include Secure Boot and Trusted Boot, Security Enhancements for Android (SE for Android), and TrustZone-based Integrity Measurement Architecture (TIMA). The application security component contains TIMA-based security services, KNOX Container, Virtual Private Network (VPN) support, and SmartCard framework. The mobile device management component contains strategies for enhanced management policies and unified enrollment.

Secure Boot is an approach used to validate the integrity of the device OS by cryptographically verifying each bootloader in the sequence during the Android start-up process. The loading of the Android OS starts by loading the primary bootloader and sequentially loading other secondary bootloaders until the final bootloader, aboot, is loaded. To prevent other unauthorized bootloaders and OSs from being loaded during this process, Secure Boot uses a certificate chain with a root-of-trust located in the hardware to validate each bootloader in the sequence [20]. If the validation fails during any step, then the overall boot process is terminated as this might indicate an altering to the device OS. However, Secure Boot only validates the start-up process until the final bootloader, aboot, is loaded and does not validate the integrity of the OS at the end. This creates a loophole where users can install and boot other OS kernels allowing them to run customized versions of the OS [20]. To combat this, Trust Boot was introduced to the architecture and it records measurements of each bootloader in secure memory and uses the recordings to make security decisions. Furthermore, if an unidentified kernel is present, the instance is recorded and the creation of the KNOX container is prevented while any existing data in the container remains protected.

SE for Android is used to isolate any data or application residing on the device into two separate environments based on security requirements. Using Mandatory Access Control (MAC) policies, SE for Android divides data and applications into two different domains and minimizes the risk of security compromises such as malwares and malicious applications from propagating from the personal environment to the secure one. Additionally, the mechanism reduces the risk of other third-party applications bypassing the security provisions set by the enterprise. This is achieved by using security configuration files that define what resources each application can access within the system. However, enforcing these security policies set by the enterprise depends on the OS kernel integrity; if the kernel integrity is compromised, then these security mechanisms might potential become disabled. To address this, the TIMA strategy was introduced into the architecture.

The TIMA strategy utilizes the ARM TrustZone hardware component on the Android devices to ensure the integrity of the Android kernel is not compromised during runtime [21]. TrustZone is a security extension included in processors that are ARMv6 or higher and is able to run two separate OSs simultaneously on a single core. This allows for the secure and personal environments to run separately but in parallel on the Android device. SE for Android runs in the personal environment and TIMA runs in the secure environment, but cannot be disabled. Additionally, the TIMA strategy contains techniques that include Periodic Kernel Monitoring (PKM), Real-Time Kernel Protection (RKP), and Attestation. PKM monitors the OS kernel to ensure no kernel code has been modified by malicious code, and checks the data structure of SE for Android to validate that it has not been corrupted by malicious content. RKP monitors that no kernel has been altered at runtime from within TrustZone. Attestation, on the other hand, validates the bootloaders and kernels at runtime using the measurements recorded by Trusted Boot. Using these measurements, Attestation provides a verdict on whether any altering has occurred on the device bootloaders or kernel. The combination of TIMA, Secure Boot, Trusted Boot, and SE for Android provides a defense against malicious security attacks on the bootstrap processes or OS kernels and can be used to notify enterprises about any security vulnerabilities or attacks.

For application security purposes, TIMA-based security services are integrated into the architecture including TIMA Client Certificate Management (CCM), TIMA KeyStore, and TrustZone-based On Device Encryption. TIMA CCM provides functionalities for creating, storing, retrieving, and installing digital certificates. These certificates and their corresponding keys are encrypted using a device specific key and can only be decrypted from within TrustZone [20]. TIMA CCM also allows for other operations to be performed using the certificates including encryptions, decryptions, and signings among others. Another component of the architecture, TIMA KeyStore, provides functionalities for creating and maintaining cryptographic keys. These keys are encrypted using a device specific hardware key which can only be decrypted from TrustZone. Both TIMA CCM and TIMA KeyStore allow operations to be performed, if the integrity of the system can be verified through Trusted Boot. If the system integrity is suspected to be compromised, then both TIMA CCM and KeyStore will disable these operations from being performed. The third element in the architecture is TrustZone-based On Device Encryption which is used to strengthen the solution’s device encryption abilities by validating the system integrity through Trusted Boot along with password authentication before any data is ever decrypted.

Another component in the architecture for application security is KNOX Container. It provides space isolation between business and personal content by creating a separate OS environment on the device that contains its own user interface. With the KNOX

Container, business related applications and data will reside inside the container and all personal related content will reside outside the container. While applications inside the container can interact with each other, applications outside of the container will not be able to interact with applications inside the container or vice versa. Enterprises can integrate with other MDM solutions to create and manage policies that govern the usage of the content inside the container.

Additionally, the KNOX solution provides support for enterprise VPN connections. The solution offers support for the assorted IPsec protocol suites including Internet Key Exchange (IKE and IKEv2), Triple DES (56/168-bit) and AES (128/256-bit) encryption, split tunneling mode, and Suite B Cryptography [20]. Furthermore, the solution also offers support for SSL VPNs and allows enterprises to configure a VPN client from other third-party SSL vendors. The support for VPN connection also allows for a per-application VPN setup that enforces VPN use only on specific applications. This means that enterprises can apply the VPN support to either the entire KNOX container or to one or a group of applications within the container. In addition to enterprise VPN, the solution architecture also contains support for smartcards. Common Access Card (CAC) smartcards store PKI certificates that can be used to digitally sign documents, establish secure online connections, and encrypt and decrypt email messages [20]. The architecture allows other third-party smartcards and readers to integrate into the solution using Public Key Cryptography Standards (PKCS).

4.3.3 Analysis Per Security Requirements

4.3.3.1 Authentication and Authorization

For authentication purposes, the solution supports several authentication approaches including Single-Sign On (SSO) and digital certificates. The SSO approach includes support for SAML 2.0 and on premise services with HTTP Negotiate authentication. With the SSO solution, infrastructure for Active Directory support as well as a SAML 2.0 compliant Identity Provider (IdP) is necessary. With digital certificate authentication, all Kerberos based applications can use these certificates to authenticate without the user having to enter a password.

4.3.3.2 Data Protection

For at-rest data protection, the solution provides stringent encryption algorithms such as AES-256 to secure all content within the business container. The TrustZone-based On Device Encryption strategy enhances this capability by requiring that the system integrity be verified before any data is decrypted. The TIMA CCM and TIMA KeyStore capabilities allow enterprises to generate cryptographic keys that are encrypted using a device specific hardware key that can be decrypted only from within TrustZone. This means that any operations on the secure content requires a system integrity verification from Trusted Boot and the decryption of the content using the device specific hardware key. Additionally, the solution provides data protection during transit by offering support for the IPsec protocol as well as SSL VPNs. This allows enterprises to integrate VPN requirements when accessing corporate content outside of their secure network infrastructure. Moreover, enterprises can set the VPN requirement for communications that arise from the KNOX container as a whole or from specific applications inside the container. This allows employees to user their devices for personal activities without overtaxing the corporate VPN, but will preserve the security of any network traffic that is initiated from the business container.

4.3.3.3 Access Control

For access control purposes, as defined in the requirements in Chapter 3, the solution can be integrated with other MDM solutions to set provisions and policies that govern the corporate content users will be able to access from their mobile devices. In conjunction with the KNOX container, other MDM solutions can be incorporated to define security groupings and assigning users to these groups in order to provide, limit, or block access to specific corporate content.

4.3.3.4 Platform Integrity

In the solution architecture, platform integrity is verified through a combination of elements including Secure Boot, Trusted Boot, and TIMA. As described in the previous section, Secure Boot and Trusted Boot are utilized to validate the integrity of the Android kernel as the system goes through its start-up process. The combination of these two elements validates that no unauthorized OS kernel is used to run customized or altered versions of the Android operating system. The process also provides protection to corporate content if a device's OS is altered after the device is already enrolled into the BYOD solution, by preventing the KNOX container from being created during boot-up if any tampering is detected. Moreover, the TIMA solution ensures that the platform integrity check cannot be disabled by malicious content running on the device by implementing the ARM TrustZone approach. The periodic monitoring performed by the TIMA PKM and RKP components allow enterprises to detect any tampering of the device's kernel. Additionally, the attestation approach can be utilized to inform enterprises about the tampering, and the enterprise can choose to enforce certain security procedures including data wipes and data locks to protect the corporate content on the device.

4.3.3.5 Application Control

Application control is implemented through the use of the KNOX container. The container provides space isolation by allowing two separate Android environments to run on the mobile device. The corporate content including applications and data will be isolated in the secure KNOX container, and will have its own user interface separate from the personal environment. The KNOX container includes its own home screen, application icons, widgets, and launchers and allows enterprises to push applications into the secure environment. This allows enterprises to set policies that define which corporate applications a given user can access. Moreover, enterprises can integrate the KNOX container with other MDM solutions to set and enforce policies around whitelisting and blacklisting specific applications for a given user. Since, the KNOX container restricts content interaction between applications outside the container and those inside the container, enterprises can minimize the risk of data leakage between the two domains.

4.3.3.6 Policy Enforcement and Compliance

Policy management is accomplished through integration with other MDM solutions. The KNOX architecture provides support for MDM policies that include limiting features and functionalities of specific applications, requiring secure access protocols such as VPN to remotely access corporate resources, geo-fencing, and managing corporate application and data usage on the mobile devices, among many others. The MDM solutions provide a centralized hub for creating and managing these policies. Additionally, the solution also offers APIs for managing the KNOX container, the TIMA KeyStore, client certificates, smartcards, Single-Sign On options, and setting device restrictions.

4.3.3.7 Monitoring and Data Collection

The solution allows enterprises to monitor the integrity of the Android operating system of a given device through the use of the TIMA components in the architecture. The attestation component also allows other corporate applications to validate a device's security condition before providing access to sensitive data. For monitoring or event logging around activities performed on the mobile device or access to corporate network resources, other MDM solutions can be integrated into the architecture. These MDM solutions provide enterprises with the ability to monitor activities inside the secure container as well as collect and log information about a device's corporate data usage.

Chapter 5: Conclusion

The recent rise in using mobile devices such as smartphones, laptops, and tablets to conduct business activities has generated a significant interest in Enterprise Mobility Management solutions. One strategy tied to enterprise mobility is the Bring Your Own Device initiative which allows employees to use their personal mobile devices to conduct both business and personal activities. The BYOD strategy presents several significant advantages to enterprises including eliminating the cost of purchasing and maintaining mobile devices, eliminating the need for purchasing and maintaining service agreements, eliminating the cost of replacing lost or malfunctioning devices, and reducing the cost of training enterprises will need to offer to employees regarding the usage of these mobile devices. However, the BYOD strategy presents several challenges to enterprises including the need for an infrastructure that supports a significant variety of device hardware and software combinations, scalability issues with respect to corporate network infrastructures, and concerns around employee privacy and device content ownership. Nonetheless, one of the most significant concerns when adopting the BYOD strategy is the issue of security. Since employees use a single device to conduct both personal and business activities, BYOD presents security risks around the storage of corporate data on the device, space isolation between personal and corporate data, corporate data transmission using untrusted networks, and access of third-party applications and web content on mobile devices that could introduce security threats. These security threats can range from malwares, phishing and SMiShing attacks, direct attacks, and data leaks to data interceptions and network spoofing. This report presented seven all-purpose security business requirements that identify elements that help minimize these security risks. These business requirements are as follows: authentication and authorization, at-rest and in-transit data protection, content access control, platform integrity, application control, policy enforcement and compliance, and monitoring and event collection. Additionally, the report presented a detailed examination of three different BYOD solutions and their architectures, and how the approaches attempt to address the security challenges presented by the BYOD strategy. Furthermore, the three solutions were explored with respect to the defined seven security business requirements and how the relationship between the solution architectural strategies align with these requirements.

References

[1] J. Street, *The Secrets to Succeeding in Network Marketing Offline and Online*. Ocala, Florida: Atlantic Publishing Group, 2008.

[2] Global Industry Analysts, Inc., “Enterprise Mobility: A Global Strategic Business Report”, Global Industry Analysts, Inc., 2015.

[3] R. Basole, *Enterprise Mobility: Applications, Technologies and Strategies*. Amsterdam: IOS Press, 2008.

[4] M. Pierer, *Mobile Device Management: Mobility Evaluation in Small and Medium-Sized Enterprises*. Vienna, Austria: Springer Nature, 2016.

[5] S. David, R. Dikhit, J. Shrivastava and T. Sawlani, “Enterprise Mobility Management: An Overview”, *International Journal of Engineering Sciences & Research Technology*, vol. 6, no. 2, pp. 111-116, 2017.

[6] C. Sørensen, *Enterprise Mobility: Tiny Technology with Global Impact on Work*. Houndmills, Basingstoke, Hampshire: Palgrave Macmillan, 2011.

[7] N. Zahadat, P. Blessner, T. Blackburn and B. Olson, “BYOD security engineering: A framework and its analysis”, *Computers & Security*, vol. 55, pp. 81-99, 2015.

[8] D. Tse, L. Wang and Y. Li, “Mobility Management for Enterprises in BYOD Deployment”, in *IEEE TrustCom/BigDataSE/ISPA*, 2016, pp. 23-26.

[9] M. Olalere, M. Abdullah, R. Mahmod and A. Abdullah, “A Review of Bring Your Own Device on Security Issues”, *SAGE Open*, vol. 5, no. 2, 2015.

[10] P. Gajar, A. Ghosh and S. Rai, “Bring your own device (BYOD): Security risks and mitigating strategies”, *Journal of Global Research in Computer Science*, vol. 4, no. 4, pp. 62-70, 2013.

[11] E. Yeboah-Boateng and F. Boaten, “Bring-Your-Own-Device (BYOD): An Evaluation of Associated Risks to Corporate Information Security”, *International Journal in IT and Engineering*, vol. 4, no. 8, pp. 12 - 30, 2016.

[12] A. Garba, J. Armarego and D. Murray, “Bring Your Own Device Organizational Information Security and Privacy”, *ARPN Journal of Engineering and Applied Sciences*, vol. 10, no. 3, pp. 1279 - 1287, 2015.

[13] A. Yautsiukhin, R. Scandariato, T. Heyman, F. Massacci and W. Joosen, “Towards a quantitative assessment of security in software architectures”, in *13th Nordic Workshop on Secure IT Systems*, Copenhagen, Denmark, 2008.

[14] “Cisco Bring Your Own Device”, *Cisco*, 2012. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byodwp.html#pgfId-436060.

[15] N. Anderson, “Cisco Bring Your Own Device Device: Freedom Without Compromising the IT Network”, Cisco Systems, Inc., San Jose, California, 2012.

[16] “Reference Architecture for Mobile Device and App Management”, *Citrix*, 2013. [Online]. Available: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/reference-architecture-for-mobile-device-and-app-management.pdf.

[17] “Guidelines for deploying Citrix BYOD solutions”, *Citrix*, 2013. [Online]. Available: http://davidhoglund.typepad.com/files/guidelines-for-deploying-byod.pdf.

[18] “Best practices to make BYOD simple and secure”, *Citrix*, 2013. [Online]. Available: https://www.sharefile.com/content/dam/sf/pdf/en/byod-best-practices.pdf.

[19] “White Paper: An Overview of Samsung KNOX”, *Samsung*, 2013. [Online]. Available: http://www.samsung.com/global/business/business-images/resource/white-paper/2013/06/Samsung_KNOX_whitepaper_June-0.pdf.

[20] “White Paper: An Overview of Samsung KNOX 2.0”, *Samsung*, 2014. [Online]. Available: http://www.samsung.com/ca/business-images/resource/white-paper/2014/03/Samsung_KNOX_tech_whitepaper_Final_140220-0.pdf.

[21] U. Kanonov and A. Wool, “Secure Containers in Android: the Samsung KNOX Case Study”, in *the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices*, 2016.