cloud security alliance℠

Mobile Working Group

Security Guidance for Critical Areas of Mobile Computing

November 2012

Contents

Foreword

Welcome to the first version of the Cloud Security Alliance's "Security Guidance for Critical Areas of Mobile Computing." As the mobile marketplace continues to mature and businesses continue to adopt mobile technologies as part of their standard technology, managing the myriad devices, operating systems, applications and security challenges becomes a crucial component to the acceptance and development of this technology. This document intends to provide you with both guidance and inspiration to support your business needs while managing new risks.

This initial guidance is intended to describe the current state of mobile computing as well as detail the top threats to mobile computing. This guidance also intends to describe various components of mobile computing which will each require business decisions on how it should be implemented. Each component of mobile computing will give guidance to implementing best practices as well as potentials risks. Some of these risks are similar to risks associated with other end user devices, while others are unique and new to the mobile workspace.

Mobile computing is quickly changing and maturing, and as such, our intention is to continue updating this guidance to ensure that readers stay informed of changes and advancements in the mobile technology as well as the accompanying management components that come along with mobile computing.

Please stay engaged on this topic and work with us to continue with this important mission. We encourage you to download and review all of our flagship research at http://www.cloudsecurityalliance.org.

Best regards,

Jerry Archer	Alan Boehme	Dave Cullinane
Nils Puhlmann	Paul Kurtz	Jim Reavis

The Cloud Security Alliance Board of Directors

Letter of Introduction

Today, all organizations to some degree are mobile—in the work they do, the products they sell, the services they deliver. Mobility enables people to take their business with them wherever they go – including proprietary company information, intellectual capital, and sensitive customer data.

Mobile devices empower employees to do what they need to do — whenever and wherever. People can work and collaborate "in the field" with customers, partners, patients or students and each other. But they need to be supported with always current operational processes and information, whether from apps, the Internet, or documents from other people. Let's face it: mobile devices today "house" the company just as much as an office building does.

Two million added work hours. This isn't hyperbole or some throwback to Draconian labor practices. This is the total sum of increased work hours achieved by Intel's mobile strategy. Of course, with any positive Ying is the inevitable negative Yang. The path to mobile success in business is not an open sieve of information, but rather a well-guarded gate that grants entry once proper authentications have been validated.

Sadly, many companies have yet to learn this seemingly simple truism. With the consumerization of IT has come the tsunami of bring your own device (BYOD), the perception by employees that just because they can access corporate systems they should access these systems. And who can blame them? Information security is not their job—they simply want to meet the intense work hour demands of the modern global economy while still being able to see their children and spouse before the day ends. Network access becomes simpler for the layman with each new mobile OS release. Some will say the time for IT to act is now; I say that the time for IT to act has already passed. Now IT must make up for the mistakes of the past and plan today for the inevitability of tomorrow.

Dave Lingenfelter
CSA Mobile Working Group Co-Chair

Letter from the Co-Chairs

Mobile computing is not necessarily a new addition to the computer landscape, but with the increase in speed, accessibility, and adoption, smartphones and tablets are quickly becoming an important piece of consumers' lives, both personally and professionally. Corporations are adopting mobile technology as new means of accessing corporate resources in many areas.

The explosive growth of smartphone and tablet devices in the consumer space has led to an overwhelming, and unprecedented, demand by end users to bring their consumer-level technology into the corporate environment. This has led to an entirely new area of security concern for the enterprise administrators.

Devices designed for consumer use, along with the availability of applications and resources readily available through cloud service providers, has come together in a sort of perfect storm for IT and Security administrators. This document is meant to help identify different components involved in mobile computing in an effort to educate IT professionals and consumers alike, as well as strengthen and secure the mobile working environment.

We want to thank all of the many contributors worldwide who have worked so hard to produce these areas of focus providing guidance for best practices in mobile computing. Many have been with the mobile working group since the beginning; others have recently joined this effort. Each has spent countless hours considering, clarifying, writing, and editing these papers. We anticipate much more work in this area of research as the mobile landscape continues to morph.

Sincerely,

Mobile Working Group Co-Chairs

An Editorial Note on Risk

Throughout this Guidance, we make extensive recommendations on understanding and reducing your risk when adopting mobile computing, but not all the recommendations are necessary or even realistic for all deployments. As we compiled information during the editorial process, we quickly realized there simply wasn't enough space to provide fully nuanced recommendations for all possible risk scenarios.

With so many different mobile deployment options, no list of security controls can cover all circumstances. As with any security area, organizations should adopt a risk-based approach to adopting mobile devices and selecting security options.

Acknowledgments

Co-Chairs

Cesare Garlati, Trend Micro
David Lingenfelter, Fiberlink Communications

Contributors

Top Threats to Mobile Computing

Lead: Dan Hubbard, OTS; Jon-Michael Brook, Symantec; Alice Decker, Trend Micro; Eric Fisher, FishNet Security; Bernd Jaeger, Colt Technolgy; Freddy Kasprzykowski; Allen Lum, Control Solutions; Steven Michalove; Guido Sanchidrian, Symantec; Sam Wilke

Mobile Maturity Questionnaire

Lead: Nadeem Bhukari, Kinnamik; Alice Decker, Trend Micro; Steve Dotson, Travelport; Giles Hogben, CSA

Bring Your Own Device (BYOD) Policy Guidance

Lead: Jay Munsterman, Cox Communications; Yvette Agostini; Andrea Berther, Lutech S.p.A.; Megan Bell, Kivu Consulting; Randy Cadenhead, Cox Communications; Harish Chaihan, Cognizant; Robert de Monts, de Monts & Associates; Alice Decker, Trend Micro; Steve Dotson, Travelport; Eric Fisher, FishNet Security; Mushegh Hakhinian, Intralinks; Naveed Hamid, Cisco; Subber Iyer, Zscaler; Sachin Jain, JainSys, Inc; Vladimir Jirasek, CSA UK; Matt Leipnik, Tata Communications; Sandeep Mahajan, Avaya; Steven Michalove; Sandeep Mittal; Somanath NG, Infosys; Dale Nacke, Cox Communications; Guido Sanchidrian, Symantec; Eiji Sasahara, IDC; Glenn Schoonover, KoolSpan; Sam Wilke; Mason White, Symform

Mobile Authentication

Lead: Mark Cunningham, Altimetrik; Megan Bell, Kivu Consulting; Matt Broda, Qualys; Randy Bunnell; William Corrington, Stony Point Enterprises; Chris Garrett; Giles Hogben, CSA; Vladimir Jirasek, CSA UK; Daniel Miessler; Mats Naslund, Ericsson; Jeff Shaffer, Kivu Consulting; Glenn Schoonover, KoolSpan; Said Tabet, EMC; Govind Tatachari, Augmente LLC; Sam Wilke

App Store Security

Lead: James Hunter, Net Effects; Alice Decker, Trend Micro; Tom Jones; Ionnis Kounelis, Joint Research Centre - European Commission; Sandeep Mahajan, Avaya; Somanath NG, Infosys; Henry St. Andre, InContact; Morey Straus, mFoundry; Satheesh Sudarsan, Samsung

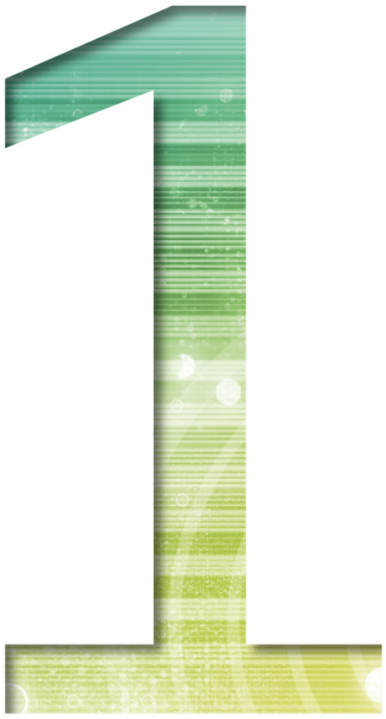
Mobile Device Management

Lead: Guido Sanchidrian, Symantec; Jane Cosnowsky, Dell; Alice Decker, Trend Micro; Pamela Fusco, Virtuosi Group; Nader Henein, RIM; Subbu Iyer, Zscaler; Allen Lum, Control Solutions; Paul Madsen, Ping Identity; Jay

Musterman, Cox Communications; Somanath NG, Infosys; Eiji Sasahara, Healthcare Cloud Initiative, NPO; Tyler Shields, Veracode; Sam Wilke

CSA Global Staff

Aaron Alva, Graduate Research Intern
Luciano JR Santos, Research Director
Kendall Scoboria, Graphic Designer
Evan Scoboria, Webmaster
John Yeoh, Research Analyst



SECTION 1 //

Mobile Definition

1.0 Mobile Computing Definition

This domain on mobile computing provides a framework for how mobile computing can become an integral part of a company's environment. The contents of this domain focus on a description of mobile computing that is specifically tailored to the unique perspective of IT security professionals.

The first section of this document discusses home mobile computing has been defined and framed for the purposes of the rest of the document.

The second section of the document talks about the current state of maturity of mobile technology in the corporate environments. It also addresses the threats and concerns of IT professionals in regards to mobile computing.

The final section of this document provides an introduction to each of the major components of mobile computing, including **Bring Your Own Device (BYOD)**, **Authentication**, **App Stores**, **Mobile Device Management (MDM)**, and **Security**. These subsections talk about areas to be considered within each of these components, as well as possible ways to implement and support each component.

1.1 What Is Mobile Computing?

Mobile computing is a very broad term which can be used to define any means of using a computer while outside of the corporate office. This could include working from home or on the road at an airport or hotel. The means to perform mobile computing could include kiosks used to remotely connect to the corporate office, home computers, laptops, tablets or smartphones. Specialized or integrated devices could also be considered as mobile computing devices.

For the purposes of this guidance, we've limited our scope of mobile devices to smartphones and tablets. The decision was based in part on the current market demand and widespread use of these types of devices. The consumer-centric nature of these devices was also a major factor as these devices are widely used by consumers and are quickly being introduced into corporate environments.

1.2 What Comprises Mobile Computing?

Mobile computing is comprised of several different components. While similar to components of other technologies, when dealing with mobile technology, many of these components take on a more critical role in terms of making decisions on how to manage these devices.

BYOD – The concept of allowing employees to bring personally-owned devices to the office is not new to mobile technology. While previous generations of computing technology could be more closely controlled and monitored, mobile devices lend themselves very easily to the concept of bring your own device (BYOD). These devices were designed with the consumer in mind, allowing consumers, and not the enterprise, to drive demand for them. The devices have quickly become part of the consumer culture, and with the computing power, ease of use, and ability to connect virtually anywhere, they have also quickly become the desired means for consumers to do their work while outside the office.

This document covers the topic of BYOD and helps lay out a path for both end users and enterprise IT, which will aid in defining how BYOD can work in a corporate environment.

Authentication – Authentication is another concept that is not new or unique to mobile computing, but how it is handled in regards to mobile can be quite different from previous technologies. The focus with mobile devices is not necessarily to protect just the device, but to also protect the data stored on and accessed by the device. With this in mind, authentication takes on a different role.

This document outlines several scenarios for authentication as well as several methods of authentication that can work for different components of mobile computing.

App Stores – The management and distribution of applications has traditionally been the role of IT. Licensing, centralized management and controlled distribution have helped ensure uniformity across systems. Mobile devices take a different approach to applications, and, like many aspects of mobile computing, put the end user in control.

This document covers the different types of app stores and how each can be utilized as part of a complete mobile solution.

Device Management – Mobile devices are designed for consumers, meaning they are designed to be managed by the end user. While this is convenient as a consumer device, it does not lend itself to a sustainable model for enterprises to adopt mobile devices across their entire user population. Mobile device management (MDM) is an important component of any successful enterprise deployment of mobile devices. Central management of mobile devices allows IT and security departments to ensure a level of uniformity and compliance with corporate policies. In many industries, central management also helps companies meet their regulatory commitments when dealing with mobile devices.

This document covers the various aspects of MDM that should be considered by enterprises when looking at a solution.

Security – While security affects all areas of mobile computing, it is still necessary to call it out separately. Mobile devices have quickly become the preferred method of people accessing email and other services when they are not in the office.

1.3 The Characteristics of Mobile Computing

There are several characteristics to mobile devices and mobile computing. Many of these are shared with other technologies but have unique significance when it comes to mobile computing.

Portability – As the name “mobile” implies, the devices have to be able to easily move to different locations, while remaining functional.

Connectivity – The ease of being able to connect to the Internet and receive or transmit data is an essential component to mobile computing. Connectivity through mobile carriers over a 3G- or 4G-type network, as well as WiFi capabilities, are basic requirements for mobile devices.

Interactivity – This could almost go without saying, but like most other computing technologies, the ability for a mobile device is critical. The interactivity becomes more significant with mobile devices, as they typically have less computing power than other types of technology.

Individuality – Individuality may sometimes be overlooked, but it is a basic component of the concept of mobile computing. Mobile devices, including smartphones and tablets, are designed for individuals and have become a sort of extension to people in many aspects of their lives. From this perspective, how individuals interact with mobile devices remains unique.

SECTION 2 //

Current State of Mobile Computing

2.0 Threats to Mobile Computing

Mobile computing brings with it threats to the user and to the corporate environment. From personal information to corporate data, mobile devices are used for a wide variety of tasks by individuals and companies. Mobile devices have added a new threat to the corporate landscape as they have introduced the concept of bring your own device (BYOD). While this is not necessarily an entirely new concept, the wide acceptance of BYOD with mobile devices has created a paradigm shift, where the security and safety of the device is not necessarily to protect the corporate data, but to keep the personal data out of the hands of corporate management.

In July 2012, the Cloud Security Alliance and the Mobile Working Group surveyed 210 security practitioners from 26 countries. Respondents were approximately 80% "experts in the field of information security," which includes security admins, consultants and cloud architects. Twenty percent of respondents held these roles at cloud service providers. The survey asked users to rank mobile top threats in order of both their concern and likelihood of a threat: occurring this year, next year, or not likely to happen. After considering over 40 different top threats to the mobile landscape, the top candidates were dubbed "The Evil 8."

2.1 The Evil 8: Top Threats to Mobile

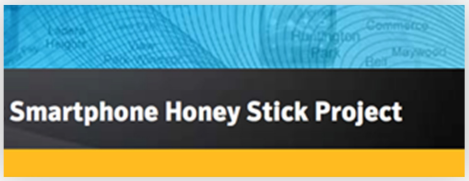
1. Data Loss from lost, stolen, or decommissioned devices
2. Information stealing mobile malware
3. Data Loss and data leakage through poorly written third-party applications
4. Vulnerabilities within devices, OS, design, and third-party applications
5. Unsecured WiFi, network access, and rogue access points
6. Unsecured or rogue marketplaces
7. Insufficient management tools, capabilities, and access to APIs (includes personas)
8. NFC and proximity-based hacking

2.1.1 Threat #1 – Data Loss from Lost, Stolen, or Decommissioned Devices

By their nature, mobile devices are with us everywhere we go. The information accessed through the device means that theft or loss of a mobile device has immediate consequences. Additionally, weak password access, no passwords, and little or no encryption can lead to data leakage on the devices. Users may also sell or discard devices without understanding the risk to their data.

The threat level from data loss is high, as it occurs frequently and is a top concern across executives and IT admins.

2.1.1.1 Threat Example



The Symantec Smartphone Honey Stick Project[1] was designed to collect information on what happens when a smartphone is lost. The company "lost" 50 smartphones, each containing simulated personal and corporate information. The results were astonishing:

- 83% had attempts to access business apps
- 89% had attempts to access personal apps
- 96% had attempts to access at least some type of data
- 50% of finders contacted the owner and offered to help return the phone
- The most popular apps accessed were:
  - Contacts
  - Pictures
  - Social networking
  - Webmail
  - Passwords

2.1.2 Threat #2 – Information-Stealing Malware

Android devices, in particular, offer many options for application downloads and installations. Unlike iOS devices, which need to be jailbroken, Android users can easily opt to download and install apps from third-party marketplaces other than Google's official "Play Store" marketplace. To date, the majority of malicious code distributed for Android has been disseminated through third-party app stores, predominantly in Asia. Most of the malware distributed through third-party stores has been designed to steal data from the host device.

This threat level is high, as Android malware in particular is becoming a more popular attack surface for criminals who traditionally have used PCs as their platforms. Kaspersky Labs found that malware targeting Android users nearly tripled in the 2nd quarter of 2012 from the 1st quarter (14,923 malicious programs in Q2, up from 5,441 in Q1).[2]

[1] http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=symantec-smartphone-honey-stick-project
http://www.streetwise-security-zone.com/members/streetwise/adminpages/honeystickproject
[2] http://www.securelist.com/en/analysis/204792239/IT_Threat_Evolution_Q2_2012#3

2.1.2.1 Threat Example

One of the most prevalent pieces of malicious code for Android is called "Zitmo." This is a mobile version of the Zeus malware, which is designed to steal information from the device by defeating the SMS-based banking two-factor authorization.[3]

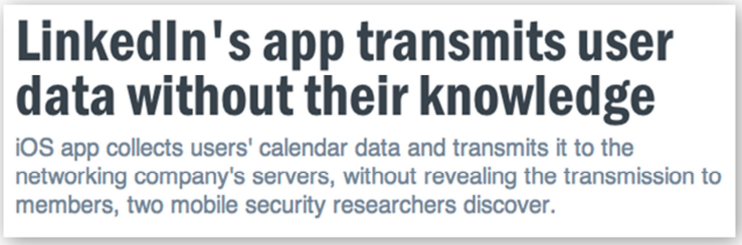
Another example is the Nickspy Trojan, which began infecting mobile devices in 2011. This application disguises itself as a Google Plus app but contains the ability to record phone conversations to an audio file, which it uploads to a remote server managed by the app's originators.

2.1.3 Threat #3 – Data Loss and Data Leakage through Poorly-Written Applications

Applications for smartphones and tablets have grown exponentially on iOS and Android. Although the main marketplaces have security checks, certain data collection processes are of questionable necessity; all too often, applications either ask for too much access to data or simply gather more data than they need or otherwise advertise.

This is a mid-level threat. Although data loss and leaking through poorly-written applications happens across mobile operating systems, it is not exploited nearly as often as other threats in the Evil 8.

2.1.3.1 Threat Example



A report published by Arxan, a private software security company, states that more than 90% of top paid mobile apps have been hacked, and few apps use security defenses that keep user data protected.[4] For example, LinkedIn recently jeopardized user data by unknowingly enabling privileged access to calendar data within their iPad and iPhone apps.[5] Without user knowledge, LinkedIn's application on iOS devices transmitted passwords, meeting notes, and other information from calendar entries.

[3] http://securitywatch.pcmag.com/none/299291-fake-android-security-app-is-mobile-zeus-malware-in-disguise
[4] http://www.darkreading.com/mobile-security/167901113/security/application-security/240005962/most-paid-apple-ios-google-android-apps-have-been-hacked.html
[5] http://news.cnet.com/8301-1009_3-57447966-83/linkedins-app-transmits-user-data-without-their-knowledge/

2.1.4 Threat #4 – Vulnerabilities in Hardware, OS, Application and Third-Party Applications

Mobile hardware, OS, applications and third-party apps contain defects (vulnerabilities) and are susceptible to exfiltration and/or injection of data and/or malicious code (exploits). The unique ecosystem inherent in mobile devices provides a specialized array of security concerns to hardware, OS, and application developers, as mobile devices increasingly contain all of the functionalities attributed to desktop computing, with the addition of cellular communication abilities.

This is a mid-level threat; although the possibility is high, the number of exploits is not.

2.1.4.1 Threat Example

This is seen in the exponential growth of mobile malware with hardware that sends data back to the manufacturer and weak coding techniques that are easy to exploit by criminals. ZTE phones sold in the US exposed backdoor code infiltration in hardcoded password/keys.[6] iOS approved a third-party Stock app that could exploit user data leakage.[7] Another flaw in a Citibank app created unsafe sensitive data storage/transmission onto the device.[8]

2.1.5 Threat #5 – Unsecured WiFi, Network Access, Rogue Access Points

Unsecured WiFi has been available for years. However, as more users are mobile and data plans become more limited, users will increasingly use WiFi in public locations. The number of locations that provide WiFi—in particular, free WiFi—has exploded over the last few years. This has increased the attack surface for users who connect to these networks. In the last year, there has been a proliferation of attacks on hotel networks, a skyrocketing number of open rogue access points installed, and the reporting of eavesdropping cases.

---

[6] http://www.google.com/url?q=http%3A%2F%2Fwww.reuters.com%2Farticle%2F2012%2F05%2F18%2Fus-zte-phone-idUSBRE84H08J20120518&sa=D&sntz=1&usg=AFQjCNG6a3VmgIR_f1PavV4pbpI-01-Tug

[7] http://www.google.com/url?q=http%3A%2F%2Fwww.iphonehacks.com%2F2011%2F11%2Fresearcher-reveals-security-vulnerability-in-ios-demos-it-in-apple-approved-app-gets-booted-from-app-store.html&sa=D&sntz=1&usg=AFQjCNEuvsC7_ch356CdxdHRqiDLI3DIDg

[8] http://www.google.com/url?q=http%3A%2F%2Fwww.pcworld.com%2Fbusinesscenter%2Farticle%2F201994%2Fciti_iphone_app_flaw_raises_questions_of_mobile_security.html&sa=D&sntz=1&usg=AFQjCNH8-ut3R6fsjmsr4jUqO30fToEsKQ

This threat level is high. Increased access to public WiFi, along with increased use of mobile devices, creates a heightened opportunity for abuse of this connection. Firefox's Firesheep extension is a perfect example of how one can gain access to data through public unsecured WiFi.

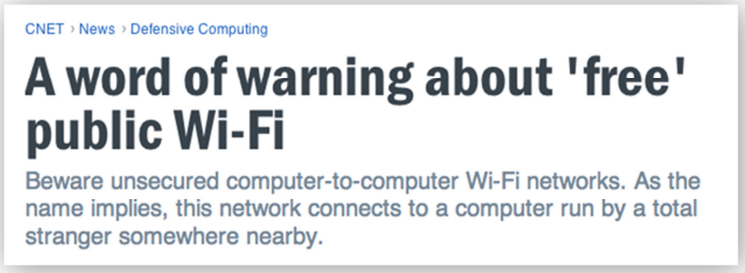
2.1.5.1 Threat Example

Faceniff

Faceniff is the Android version of the Firesheep Firefox extension that uses packet sniffing technology to intercept unencrypted cookies, thereby compromising a user's login credentials.

Hotel & Airport Hacking

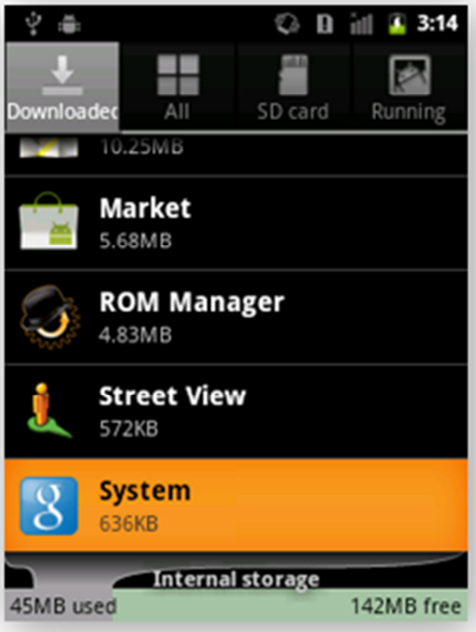
Unsecured wireless networks at hotels have proven to be ideal places for hackers to commit a wide variety of crimes. Fake WiFi access points are designed to look like real hotel WiFi networks. These malicious networks may contain the hotel's name or other deceptive descriptions. [9]


CNET › News › Defensive Computing

A word of warning about 'free' public Wi-Fi

Beware unsecured computer-to-computer Wi-Fi networks. As the name implies, this network connects to a computer run by a total stranger somewhere nearby.

2.1.6 Threat #6 – Unsecured or Rogue Marketplaces



Android devices, in particular, offer many options for application downloads and installations. Unlike iOS devices, which need to be jailbroken, Android users can easily opt to download and install apps from third-party marketplaces other than Google's official "Play Store" marketplace. To date, the majority of malicious code distributed for Android has been distributed through third-party app stores, predominantly in Asia. Most of the malware distributed through third-party stores has been designed to steal data from the host device.

This threat level is high: Android malware in particular is being distributed through these marketplaces more and more frequently.

2.1.6.1 Threat Example

Disguised as a popular app and unseen on the home screen, Tigerbot is downloaded involuntarily to devices from third-party

[9] http://news.cnet.com/8301-13554_3-9941355-33.html

marketplaces. TigerBot is a bot designed to gather confidential data from a mobile device and uses SMS to control the installed bot. This has been discovered on several marketplaces in Asia. In the image to the left, the TigerBot malware hides from the user by masking itself as a popular icon, such as Google's search app, and a generic application name (ie. "System").[10]

2.1.7 Threat #7 – Insufficient Access to APIs, Management Tools, and Multi-Personas

Granting users and developers access to a device's low-level functions is a double-edged sword, as attackers, in theory, could also gain access to those functions. However, a lack of access to system-level functions to trusted developers could lead to insufficient security. Additionally, with most smartphone and tablet operating systems today, there is little, if any, guest access or user status. Thus, all usage is in the context of the admin, thereby providing excessive access in many instances.

This is a mid-level threat. Actual reported instances are not as frequent as several other threats in the Evil 8.

2.1.7.1 Threat Example

Lack of Access to APIs/OS Architecture

An anti-virus vendor may not have the ability to read programs in memory for real-time protection, leading to malicious code being run. Additionally, operating systems may limit access to core OS architecture, entirely leaving anti-virus vendors out of the equation, as is the case with Apples iOS.

User Error

Additionally, a user may simply leave the phone unlocked, which allows someone with access to read and modify all information on the phone, including configuration settings.

2.1.8 Threat #8 – NFC and Proximity-Based Hacking

Near-field communication (NFC) allows mobile devices to communicate with other devices through short-range wireless technology. NFC technology has been used in payment transactions, social media, coupon delivery, and contact information sharing. Due to the information value being transmitted, this is likely to be a target of attackers in the future.

The threat level is low, as the threat is still in the proof-of-concept phase.

[10] http://www.csc.ncsu.edu/faculty/jiang/TigerBot/

2.1.8.1 Threat Example


SECURITY & PRIVACY

Google Wallet Hack Shows NFC Payments Still Aren't Secure

A drive-by payment occurs when, based on the user's physical location or proximity, an attacker can receive currency from the user's smartphone (AKA digital wallet). Exposing Google Wallet's unencrypted user data and hacking into the Nexus S NFC shows early vulnerabilities in this new technology.[11]

2.2 Considerations

Businesses should not consider mobile devices to be business as usual when it comes to security and where to focus security efforts. Most of these threats are either new to the IT landscape or enhanced by mobile devices. Mobile devices are typically not connected directly to the corporate network, so traditional security controls like network firewalls, IDS, centralized content filtering will do little to help protect the data that is being passed back and forth to the mobile devices.

The consumer nature of acquiring apps for mobile devices also shows up a couple times in this top threats list. While previous technologies lent themselves to centralized IT control, mobile devices put the person holding the device in control of what can be added or changed on the device.

[11] http://techland.time.com/2012/02/10/google-wallet-hack-shows-nfc-payments-still-arent-secure/

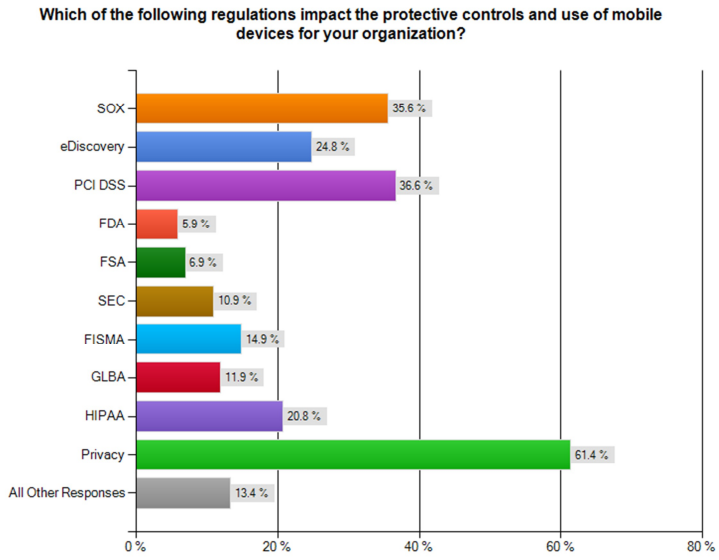
3.0 Maturity of the Mobile Landscape

Smartphones, tablets, and other advanced mobile technology continue to gain acceptance and, in some cases, prominence in the enterprise work environment. Mobile computing is still relatively new to the corporate environment, and as such, companies are still trying to determine how to best use and manage these devices. As with every new technology, there is an associated maturity model to determine the current environment. The CSA Mobile Working group put together a questionnaire to help gauge the maturity of the mobile computing landscape.

The questionnaire was designed to help CSA, as well as enterprises and individual consumers, to understand the current maturity level of the mobile marketplace.[12] The results from this survey will be used to develop processes for individual enterprises to continue to advance their use and management of mobile technology. Maturity models change over time, and we expect this to be the first of multiple surveys, as we expect the overall maturity of mobile devices to continue to increase.

3.1 Demographic Data

Country: The majority of respondents (44.6%) report living in the United States, while 26.7% live in countries otherwise not defined and 11.9% are from the United Kingdom.



All charts in this section originated at SurveyMonkey.com

Business Sector: Primarily, 41.2% of respondents are in the technology sector, with consulting/professional services amounting to 13.7% of those surveyed. Banking/financial services (8.8%), telecommunications (7.8%), communications (5.9%), and government (4.9%) sectors are also represented.

Position: Thirty-three percent of respondents are in a vice-president or director position at their place of employment, while 29.4% are managers, 24.5% are staff, and 12.7% are C-level executives.

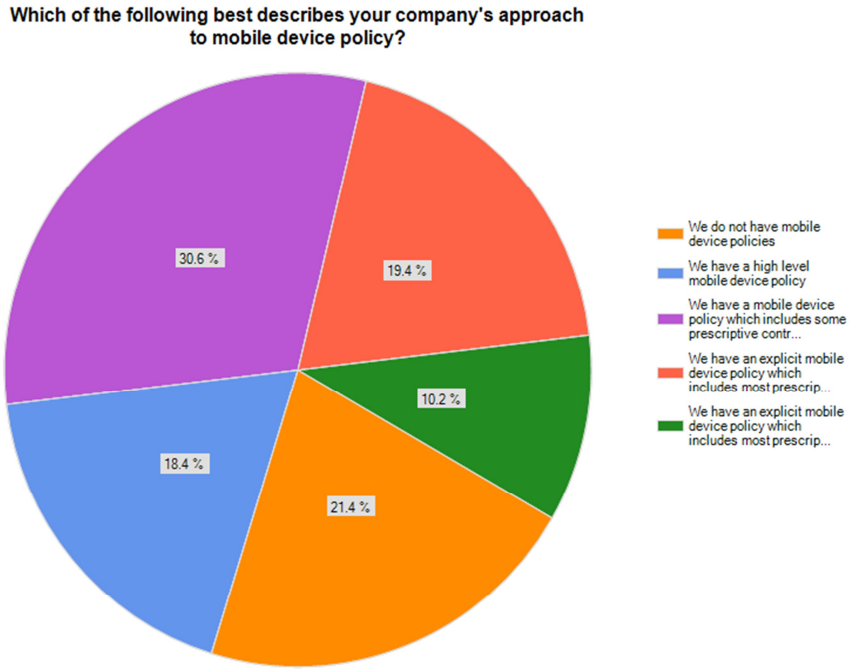
IT Role: Forty-six percent of respondents are in IS assurance/security/audit/risk management, 28.4% are in information systems management

[12] Each question had five possible responses ranging (in most cases) from 1) no corporate oversight 2) minimal corporate involvement 3) some level of manual or automated control 4) centralized management and control 5) use of advanced features and technologies.

or IT professional, and 23.5% are business buyers/influencers/or users of information technology.

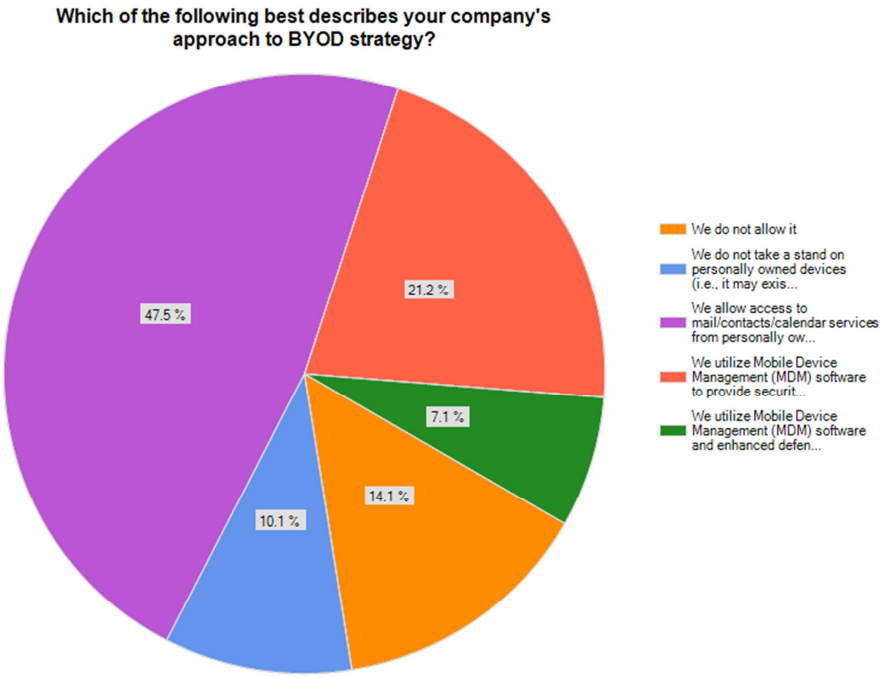
Company Size: Thirty-seven percent of those surveyed report companies with more than 5,000 employees. Twenty-nine percent are small businesses with 1-99 employees, 18.6% are mid-sized businesses with 100-499 employees.

3.2 Policy



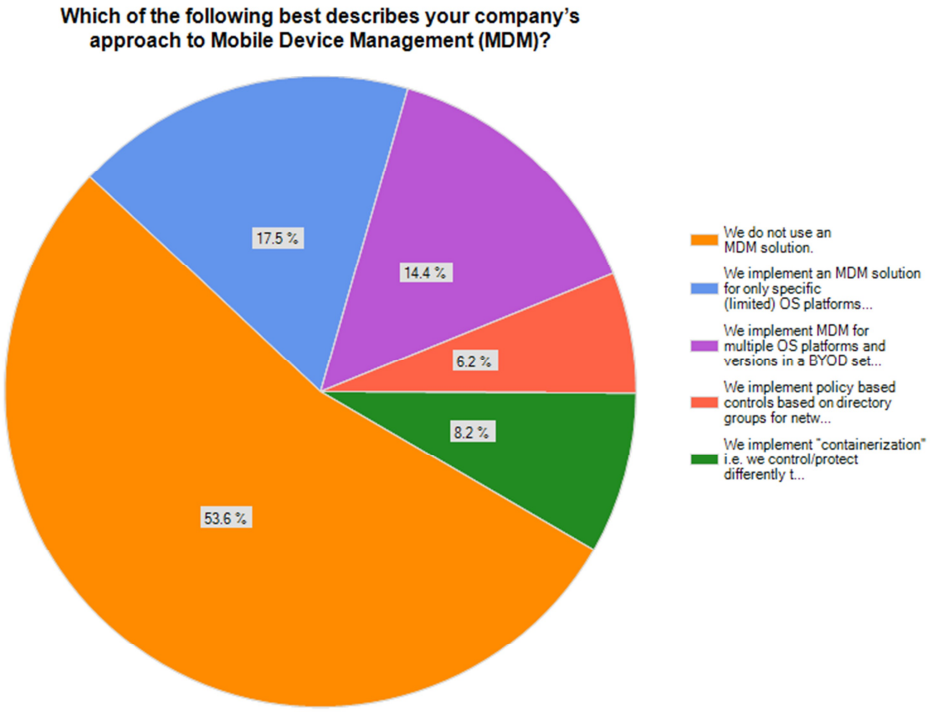
The results show an interest and understanding of mobile capabilities and threats, with 78% of respondents stating they have some level of policy in place that specifically addresses mobile devices. However, with the majority of 69% having a low maturity of policy—from non-existent to partially addressing mobile device security and privacy controls—it seems most organizations are still wrestling with some of the tougher privacy directives of BYOD owners and organizational data security on BYOD.

3.3 Bring Your Own Device (BYOD)



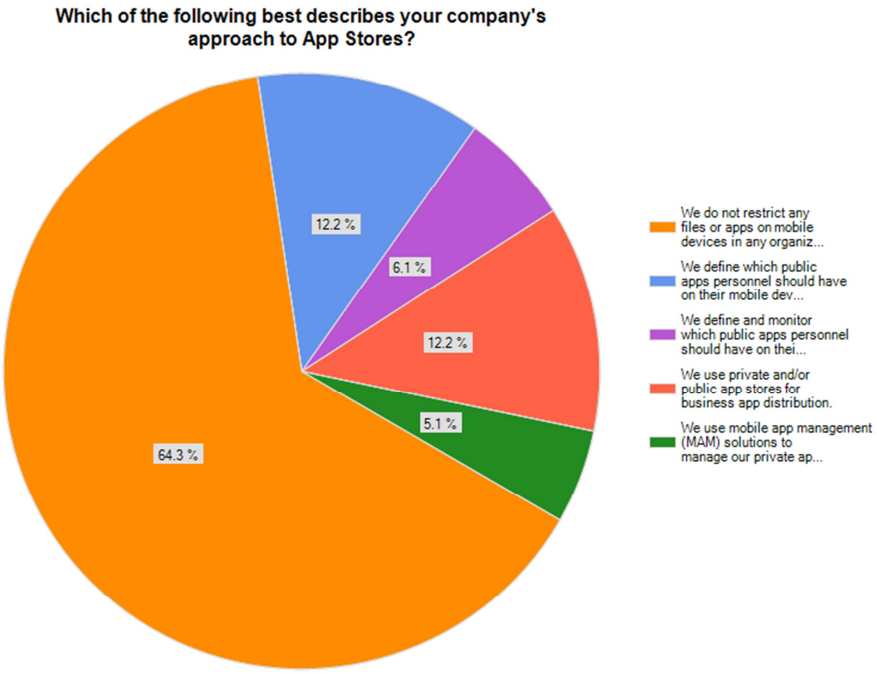
Mobile devices are typically designed as consumer devices. This lends itself to the concept of BYOD, in which companies allow employees to use their own devices to access corporate resources. Nearly 86% of respondents report their companies allowing a BYOD-approach to mobile devices. Personally-owned mobile devices are used to access corporate data and systems within over 75% or the respondent organizations. However, organizations are still in an early state of maturity, with 47.5% only allowing access to mail, contacts and calendar systems, and only 28% employing technical security controls beyond those available on the device.

3.4 Mobile Device Management (MDM)



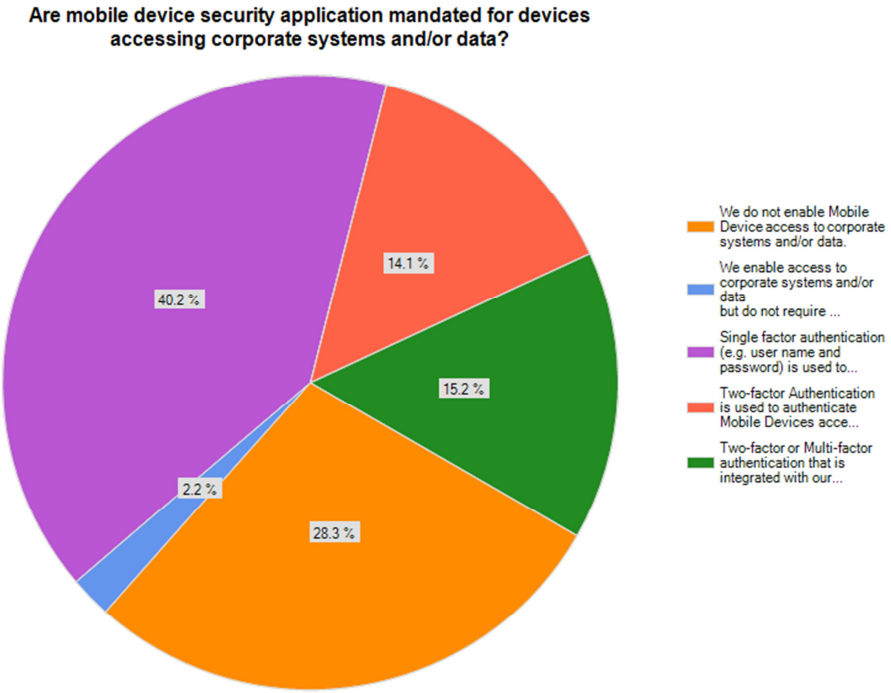
Going deeper into mobile acceptance in the corporate environment, questions were asked around mobile device management (MDM). This is where we start to see the mobile maturity curve needing more focus by companies. The above chart shows that over 53% of respondents do not use an MDM solution.

3.5 App Store



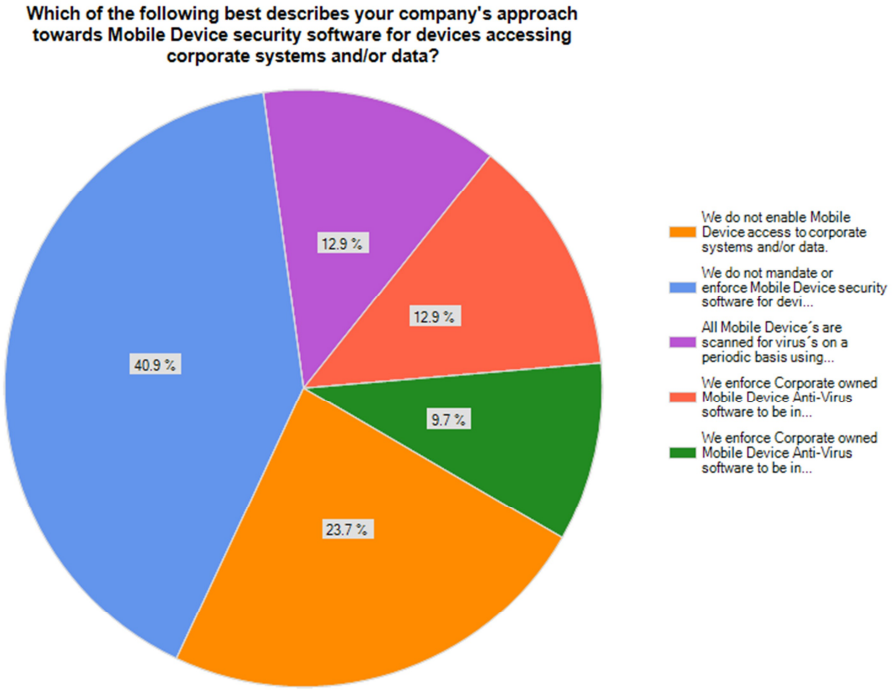
With over 64% of respondent organizations not restricting files or applications on mobile devices, this suggests there is a significant potential data leakage gap exasperated by the extent of BYOD access.

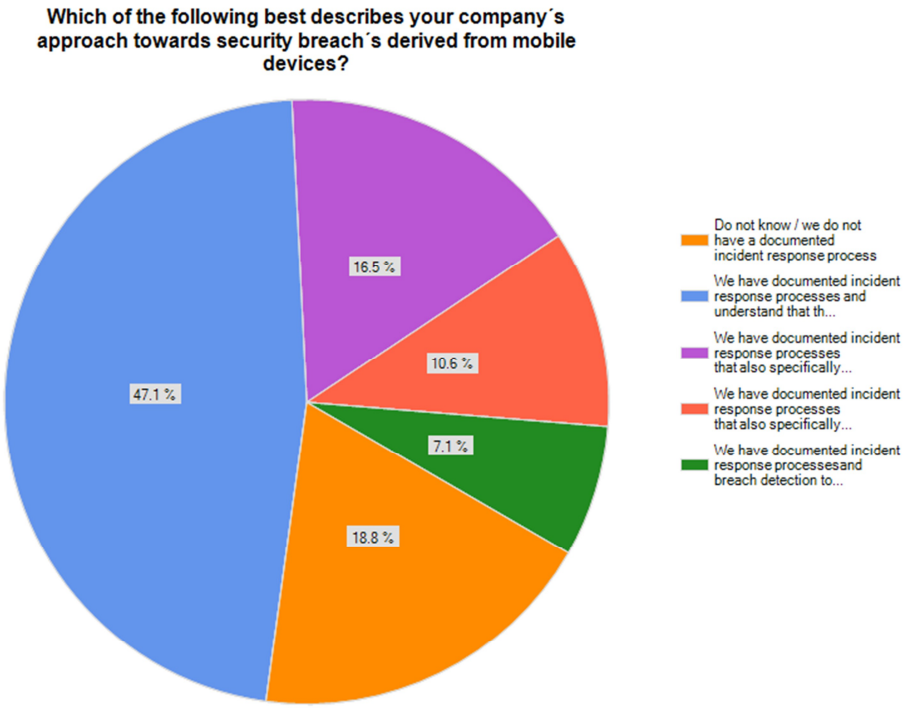
3.6 Authentication

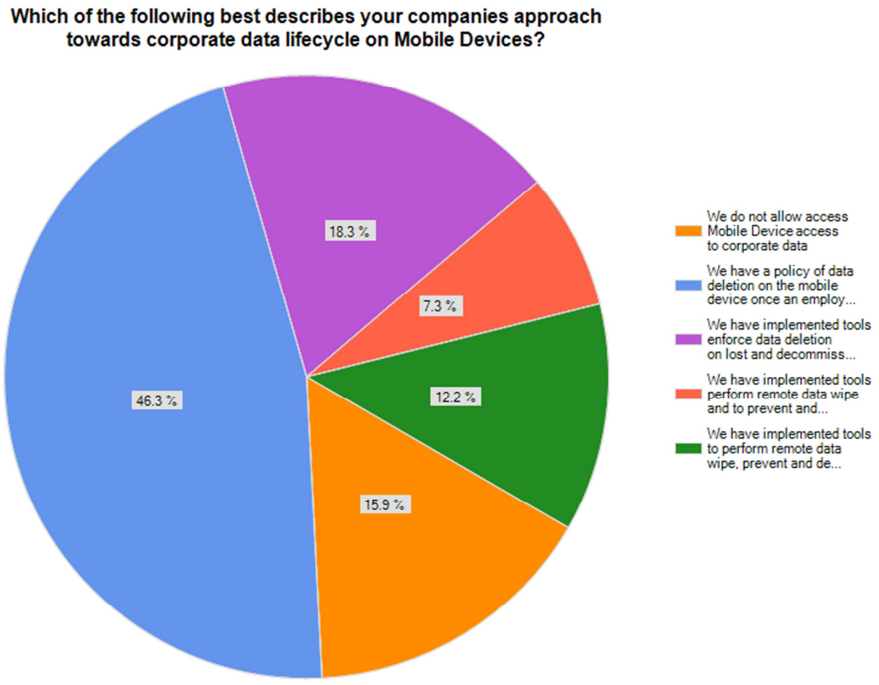


The authentication chart continues to show where the mobile space needs to continue maturing. Forty percent of respondents implement only a single-factor authentication when accessing corporate systems.

3.7 Security







The charts above demonstrate that a traditional end user security approach may not work with mobile devices. We see that, from a security perspective, nearly 41% of respondents do not implement mobile device security software in order to access corporate systems or data, with an additional 24% of respondents saying mobile devices are not allowed direct access to corporate information. This chart shows that the maturity of security controls on mobile devices is lacking, either because the technology does not lend itself to mobile devices, or because an enterprise strategy has not been formed.

SECTION 3 //

Mobile Components for Consideration

4.0 BYOD

It is becoming common for employees to request the ability to use their personal mobile devices in the course of work-related activities. Allowing them to do so may improve employee productivity, talent retention, and business agility but most likely runs contrary to existing corporate/IT policy. A strategy should be chosen to provide the desired level of control, such as a containerization of company data and applications, or a full-device, MDM-centric approach. A policy can then be established in support of the BYOD program and the unique considerations, challenges, and risks it brings. Transitioning from company-owned, IT-managed devices to an environment that is more open and has less controls can pose a real challenge both to the policy as well as traditional ways of thinking. This document is intended to provide guidance for those starting out on the BYOD journey. Highlighted below are a number of key areas that should be considered and addressed in such a program.

4.1 Employee Privacy

Employees want transparency to trust in the enterprise BYOD program. Privacy and data protection laws are likely to apply to workplace monitoring, as an individual's rights are not surrendered at the office door. The level to which data on a mobile device is remotely readable varies based on the specifics of the platform, but employees should be aware of the level of visibility the company will have on their device. Even in situations where personal data cannot be directly accessed, information may be leaked by other means, such as inference made from a listing of installed applications. Additionally, employees should be aware of the implications of litigation holds and the eDiscovery process.

Remote data wipe capabilities may also impact personal data. Most MDM platforms possess the ability to segregate information and selectively delete data, but those capabilities do vary by platform and implementation. Also of note, a wipe after repeatedly failed authentication usually affects all data on the device. The destruction of personal data by company systems or policies may be prohibited by law in some regions.

4.1.1 Employee Questions

- Will the company read my personal data?
- What will happen to my device during a legal investigation?
- What happens if I lose my device?
- Can I request a complete data wipe if I lose my device?
- What happens if I leave the company?

4.1.2 Policy Considerations

- In what situations will the company require taking possession of the device?
- In what situations will the device be wiped? Consider local laws and regulations.
- Monitoring of employee data/actions should be proportionate to the risks facing the employer. Special consideration should be applied to the storage of location information.

- Those individuals who can authorize the monitoring of employees should be identified and aware of their responsibilities.
- Any monitoring should be carried out in the least intrusive way possible and the capture of personal data should be minimized.
- The implications to non-employees should be understood in cases where they are likely to use the employee's device, e.g. family members.
- Device wipes should be limited to company data.

4.2 Financial Liability

The questions of cost liability should be closely considered and handled in your policy. If the employee is paying for the service and incurs usage overages, is it up to them to cover the costs? Additionally, the loss of the use of a device due to damage or theft can potentially impact productivity, and the burden of technical support may impact existing support organizations. There is potential for new costs to be incurred based on how these issues are addressed. Within the device life cycle, consideration should be given to which company-owned devices may have ownership transferred to the employee at the end of their useful business life and how transference and continued use is managed.

4.2.1 Employee Questions

- Who pays for plan overages or roaming charges?
- Must I buy a specific phone or software or use a specific provider?
- Who provides technical support?
- Who covers costs in the event of loss or damage?
- How would I be compensated if my device were held for legal reasons?

4.2.2 Policy Considerations

- Define how costs will be handled. Will a stipend be paid?
- Define a process or policy around the handling of damaged or stolen devices.
- Issue guidance on mobile plan selection and how overages or roaming charges will be addressed.
- Consider technical support responsibilities.
- Define how retired company owned devices are accounted for and ownership transferred.

4.3 Compliance and Legal Concerns

The use of personally-owned devices in the workplace may pose a challenge for regulatory compliance. Certain systems or data types may need to be off-limits to personal devices that cannot meet the standards dictated by specific regulations. Alternate access methods may need to be considered. Audit log capabilities may be inadequate in many cases. The hours employees work, or limitations thereon, are often subject to regulation by local laws. Access may need to be controlled by time of day or class of employee (e.g. exempt, non-exempt). Union agreements may also impact the policy.

Most developed nations and/or states have laws and regulations surrounding Repetitive Strain Injury (RSI) that should be investigated with regards to mobile devices. Appropriate policies and procedures should be evaluated to reduce the risks of RSI within the environment.

Finally, local laws may impact the ability for a personally-owned device to be held as part of an investigation for either civil or criminal cases. eDiscovery and litigation holds should be considered.

4.3.1 Employee Questions

- What data/systems are allowed to be accessed from my device?
- Which job functions are allowed or prohibited on my device?
- Will I be paid overtime if I access company systems on my own time?
- How are repetitive strain injuries and prevention addressed?

4.3.2 Policy Considerations

- Clearly define permitted job functions and applications.
- Align your BYOD policy to data classification policy.
- Employee eligibility should be clearly defined.
- Consider local laws and how they impact after-hours work and the use of personal assets.
- Consider union agreements and how they may impact/be impacted.
- The ability to perform eDiscovery should be considered.

4.4 Appropriate Device Usage

As part of a transparent BYOD program, employees should be clearly informed of the consequences of violating the policy. An unenforced policy may as well not exist, but an overly invasive policy will deter participation. The actions taken in the event of policy violation should not come as a surprise.

Employees may not appreciate the limits of appropriate usage when a personal device is used for both personal and company functions. This is further complicated by the fact that mobile devices do not typically support multiple user profiles. Any use of the device by different users is not attributable to the individual. Additionally, employees should be given direction on how to thoroughly wipe a device prior to resale or disposal.

4.4.1 Employee Questions

- What if my device is used by a family member?
- Can I still do [*specific_activity*] with my device?
- Am I free to upgrade the software on my device?
- Are there restrictions on which applications I may use on my device?
- What if I want to replace or sell my device?

4.4.2 Policy Considerations

- The applicability of the Acceptable Use Policy (AUP) to the use of personal devices should be clearly defined along with any other existing policies that me directly impacting.
- The use of cloud backup solutions should be limited to personal data.
- A stance on jailbreaking/rooting should be set.
- The treatment of policy violations should be clearly defined.
- Appropriate steps to be taken prior to device disposal should be outlined.

4.5 Conclusion

Allowing employees to use their preferred, personally-owned devices in the course of their work can increase productivity and retention, but it also brings additional risk. With a clear, well-communicated policy, both parties can be more comfortable with the situation. The policy should be written in easily understood language and should be thorough but not so long as to become unapproachable. The policy should be appropriate to the needs of the business, as an over-controlling policy may expose the company to increased legal liability. It should also clearly define which systems, applications, and data are permitted to be accessed from mobile devices and which would create an unacceptable security posture. Such a clear and concise policy creates a solid foundation for a successful BYOD program.

5.0 Authentication

5.1 Overview of Authentication

What is Authentication?

Authentication is the process of establishing trust in the identity of a user, process, or device. It plays a critical role in regulating access to information systems, services, and transactions. Authentication verifies user identity, which then enables the authorization of users to access resources, providing levels of barriers to unauthorized access. Authentication may be required for many scenarios, such as remote access to a corporate database, checking bank balances from a tablet device, or when completing a secure online purchase.

Traditionally, verification of identity was completed as an in-person transaction, where physical presence was an important element of identity. Identity was established based on comparing qualified proof of identity, such as a driver's license, against the physical presence of an individual. Identity could be further verified by actions such as collecting a signature.

In distributed computing environments such as the Internet, physical presence is removed as a variable to establishing identity. The challenge is to develop other methods of authenticating identity that achieve comparable levels of trust. Alternative methods should rely on a credible set of information that can be used to register and verify identity. Additionally, the process of authentication should be commensurate with the needs of the user, the security requirements of an organization, and where authentication takes place.

5.1.1 Credentials of Authentication

Authentication is accomplished through the use of discrete set of information, also known as credentials, to establish identity. The set of information may consist of a combination of elements from one or more of the following categories: what one knows, what one has, or what one is. Use of what one knows is the most common form of authentication information.

5.1.2 Authentication Categories and Factors

Category of Information	Description
What one knows	Use of information or knowledge about a user, device or transaction as a basis for identity determination. Usernames and passwords are a commonly deployed exampled.
What one has	Use of a device, token or object that is used to establish proof of identity. A mobile phone or USB dongle are examples.
What one is	Use of personal physical criteria such as a fingerprint or retina scan to determine identity.

Selection of the information set required to establish identity depends on several factors, including the confidentiality of information, as well as confidence in the systems and processes to reliably establish identity. The choice of one or more categories to establish identity depends on the degree of certainty and assurance required for the environment being accessed or transaction being conducted. When there is a need for greater certainty, two or more categories of information may be required to establish an acceptable protocol for authentication. The determination of categories for authentication is also described in terms of authentication factors:

Type	Description
Single	A single source of information is provided to establish the identity of a user. For example, in web-based authentication, this is often a username and password.
Two Factor	This is a stronger form of authentication than single factor identification. Two factor authentication involves a combination of two elements from what you know, who you are or what you have. An example of two factor authentication the use of a fingerprint (who you are) and a challenge question (what you know).
Multi Factor	Multi factor authentication is the strongest form of authentication. An example of multifactor authentication would the use of a username and password, a fingerprint, and a hardware token such as a USB dongle.

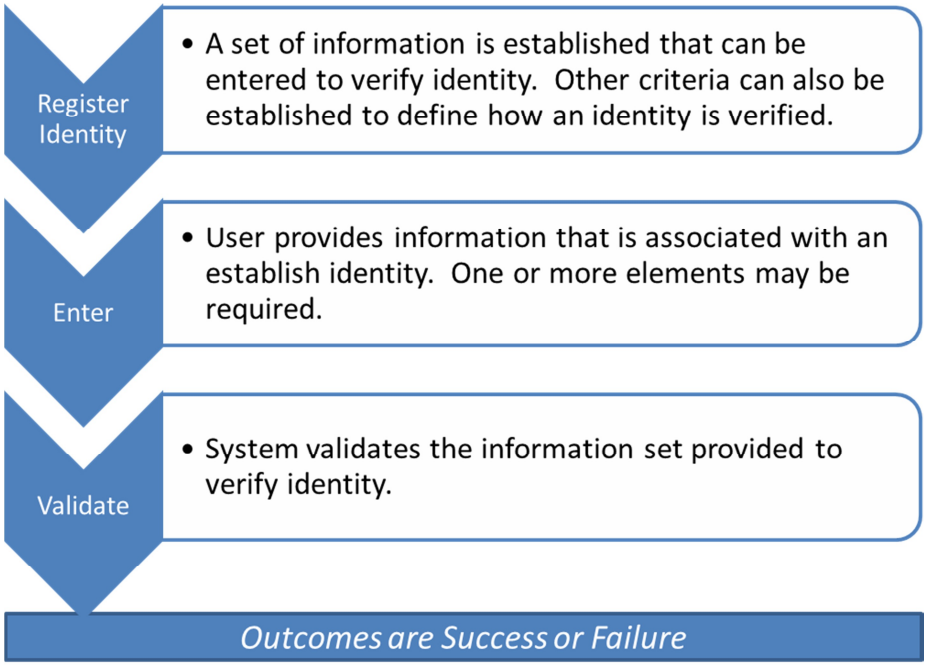
5.1.3 Levels of Assurance in Authentication Process

The selection of authentication often depends on the level of assurance that is required to establish and prove identity. The level of required assurance may be defined by legal statute or requirements such as restricted access to high-value information systems. For higher levels of assurance, authentication may be coupled with encryption and secure data transmission protocols to further limit access and reduce risks such as compromise of the authentication process (e.g. a hacker acquiring a user's authentication credentials).

Level of Assurance
1. Little or no confidence in the asserted identity's validity
2. Some confidence in the asserted identity's validity
3. High confidence in the asserted identity's validity
4. Very high confidence in the asserted identity's validity

5.1.4 Authentication Process

There are two parts to an authentication process: establishment of identity, which serves as the foundation of proof for verification, the second part of the authentication process. Verification of an entered identity may be performed once or several times.



Simple Authentication Process

5.1.5 Use Case to Illustrate Authentication

A simple use case for logging into a website user account is presented to demonstrate a single-factor authentication process.

1. The first time a user visits a website, the user choses to create an account.
2. The user enters personal information, including a username and password to register his or her account.
3. After the account is registered, the user enters a username and password to login.
4. The successful entry and verification of the username and password completes the authentication process.

NOTE: The authentication process may use encryption and secure transmission protocols to protect the users' credentials throughout the authentication process.

5.2 Mobile Authentication Trust Boundary Identification

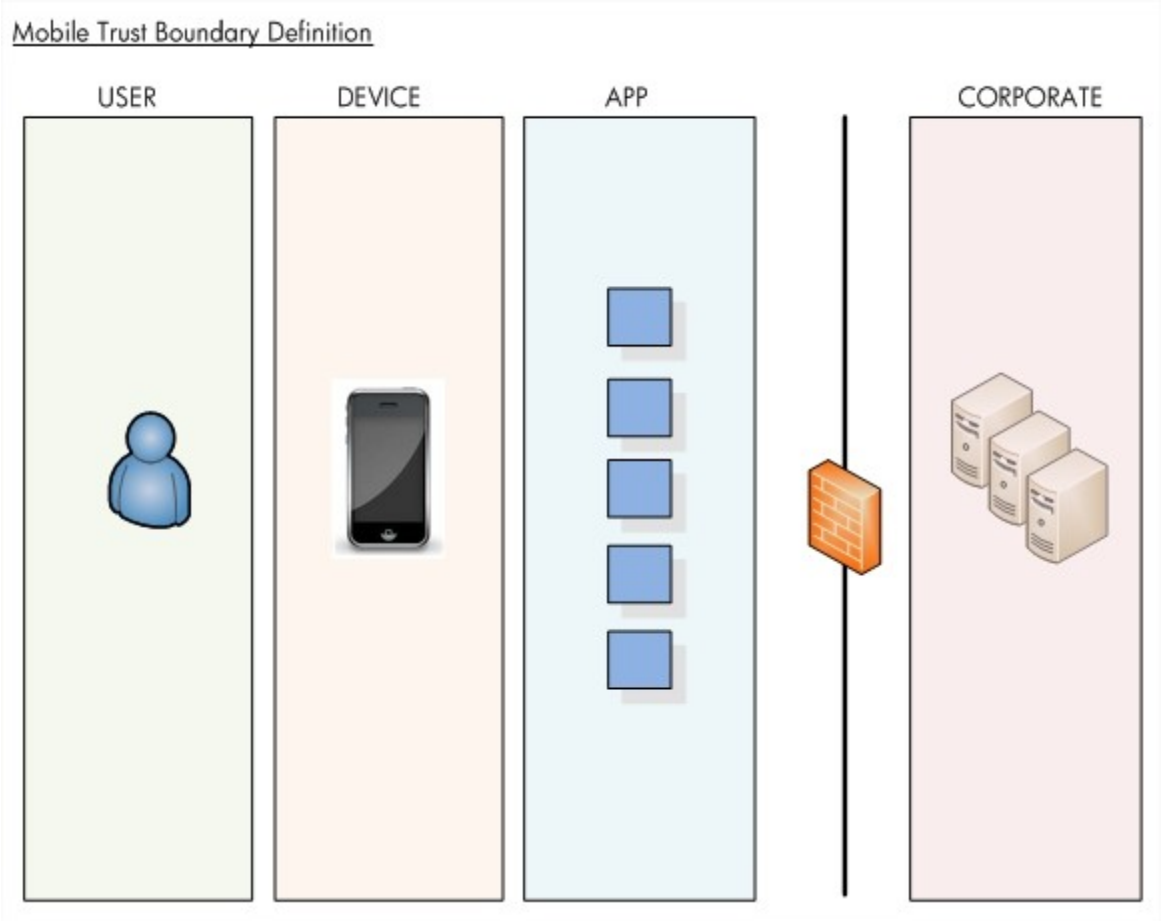
This is a project aimed at highlighting trust boundaries between various components in a mobile ecosystem. There are three sections to this deliverable:

1. A diagram illustrating the primary trust boundaries in a mobile ecosystem
2. A listing of trust boundaries and authentication options for each of those boundaries

3. A set of use cases seen in day-to-day business and personal life, with a set of recommended authentication types for each

5.2.1 Trust Boundary Diagram

The trust boundary diagram is a simple visual that highlights the separations between the user of a mobile system, the mobile device itself (operating system), the applications on the mobile device, and the corporate network. Other components can be substituted or added as desired for various audiences, but these are the primary components in question.



Next, the authentication types possible between each layer will be added (at the trust boundary). This will give a visual indication of how each type of authentication can be used at different layers of the mobile ecosystem, e.g. from the user to the device one can employ password, PIN, face-recognition, voice recognition, etc.

5.2.2 Trust Boundary Definition

Building on the trust boundary diagram is a list of the trust boundaries that can be found within the mobile ecosystem. These will include but not be limited to:

Trust Boundary	Type of Authentication
User to OS	[Password, PIN, face recognition]
User to Application	[Password, social media login, two-factor]
Application to Application	[IPC, Remote Methods, Intents, Custom URLs]
OS to Network	[NTLM, Kerberos, 802.1x]
Application to OS	[What can an application read/write on OS?]
OS to Application	[What can the OS read/write from application data?]
Application to Backend	[User credential, client-side certificate, etc.]

This table should be expanded to all boundaries possible in all scenarios, and should include all the various combinations based on backend, corporate architecture, and mobile operating system. As technology evolves, the listing can be updated to reflect new developments in authentication technologies.

5.2.3 Authentication Use Case Definition

Sitting on top of the trust boundaries themselves (and on the visual that depicts them) are a set of authentication use cases that are likely to be seen by users looking to deploy mobile technologies. These will include but not be limited to:

Use Cases
User of BYOD mobile device wishes to access internal employee directory
User of corporate-controlled mobile device wishes to access internal email
Developer of internal mobile app wishes to properly authenticate client to backend
Traveling users wish to employ stronger corporate access authentication while not at home
Developers want to know which authentication types to use for different data types
Developer wants to know minimum acceptable authentication for non-sensitive applications

All of these scenarios are likely to be seen by various users, and CSA should have guidance that gives, ideally, recommendations, and at the very least—options in each case. For example:

> "For users looking to provide completely non-sensitive information within an application it is acceptable to have no additional authentication for the application itself, i.e. to rely on the operating system's authentication settings as the primary layer of authentication for the session. In any case where the information is sensitive, however, the CSA recommends that one of the other authentication methods are employed, e.g.: Password/PIN, Face, Voice, etc."

5.3 Defense Mechanism

5.3.1 Security Policy Elements

The following are countermeasures to mitigate major authentication threats as described in the attack trees below. The threat is followed by the countermeasures. Some are security policy elements, which can be implemented by device administrators, some can only be addressed by app developers, and some can only be addressed by OS developers.

Authentication bypass:

The most common methods of authentication bypass are all possible because of developer errors. However, an enterprise IT department can test software for vulnerabilities.

- SQL Injection – Implement escaping of reserved SQL words and characters such as ',=,OR etc…
- Direct URL request – Access control system not applied beyond gateway resources. Access control should be applied to all resources.
- Session-ID prediction – Insufficient session-ID unpredictability – session-IDs should be randomly selected from a large space.
- Buffer overflow – Errors in memory management and address space predictability. Techniques such as ASLR (Address Space Layout Randomization) can be used to mitigate.
- Open-device – Always enforce use of device lock.

Valid credentials from device not owned by user – relevant attacks and countermeasures include:

- Password brute force
  - Enforce password rules
  - Throttle authentication attempts (limited failed authentication attempts). Throttling should be cloud-based, not device-based (otherwise physical access can defeat it).
  - Use context/behavioral anomaly detection (location, language, who-you-know, voice etc…), where possible
- Username space brute force
  - Enforce password rules
  - Use context/behavioral anomaly detection (location, language, who-you-know, voice), where possible
- Phishing

    - User awareness, contextual authentication support 2-factor authentication
- MITM, replay and network compromise
    - Use unpredictable one-time session tokens or time-stamps to prevent replay.
    - Verify PKI certificates of web services
    - Always transmit credentials using SSL/SSH

Valid credentials from user-trusted device – relevant attacks and countermeasures include:

- Physical access to storage (allows attacker to circumvent PIN throttling)
    - Use secure, tamper-proof hardware (e.g. secure micro-SD) to store credentials, always ensure credentials are encrypted using a private key which is password protected by a high entropy password (this should usually be the device unlock PIN to ensure minimum usability cost).
    - Always use disk encryption for all sensitive data on mobile memory.
    - Enforce password rules for unlock PINs (use ASCII, entropy, > 6 digit, dictionary resistant). Bear in mind that unlock pins often also give access to (decrypt) encryption keys, such as disk encryption keys and other credentials stored on the device. User-to-device authentication is therefore especially important.
    - Do not use insecure biometric device unlock mechanisms without liveness detection, such as face recognition, for sensitive applications.
    - Never store passwords in plain text—use salted hash[13]
    - Decommissioning/loss/theft procedures should be in place (e.g. remote-kill, locate, lock
    - Always enforce use of PIN-lock.
- OTP theft/relay
    - Do not use OTP generators on same device as primary login (e.g. Google authenticator)
    - Ensure all anti-malware measures are in place on primary and secondary device (e.g. PC and mobile phone)
- Malware on device
    - Take all possible measures to ensure malware does not reach the device – e.g. disallow jailbreak, use app-whitelist + pre-test enterprise apps.
    - Use MDM software with jailbreak detection/ other healthcheck support
    - Never store passwords in plain text—use salted hash
- Side channel attacks (e.g. smudge attack, accelerometer attack)
    - App and OS developers should block access to accelerometer during password entry
    - Use of PIN is more secure than pattern.
    - Use reverse patterns (covering the same digit more than once) where possible (although this is not allowed on Android), wipe screen regularly.
- NFC authentication failure – e.g. relay attack
    - Use time-bounding protocols to prevent relay attacks.

[13] http://www.enisa.europa.eu/media/press-releases/FlashNotePasswords.pdf

User->Device specific attacks:

- Biometric spoof
  - Do not use biometric device-lock or other biometric systems which operate without any sophisticated liveness detection.
- No pin-lock
  - Enforce pin-lock
- Data not encrypted
  - Enforce disk encryption

General advice: Authentication strength inevitably involves a tradeoff between security and usability or user-cost, as well as deployment cost. You should weigh up the risk to the assets accessible via your mobile devices (this includes assets in the cloud) against the user cost involved. Try to minimize user-involvement while providing an adequate level of security for the assets involved.

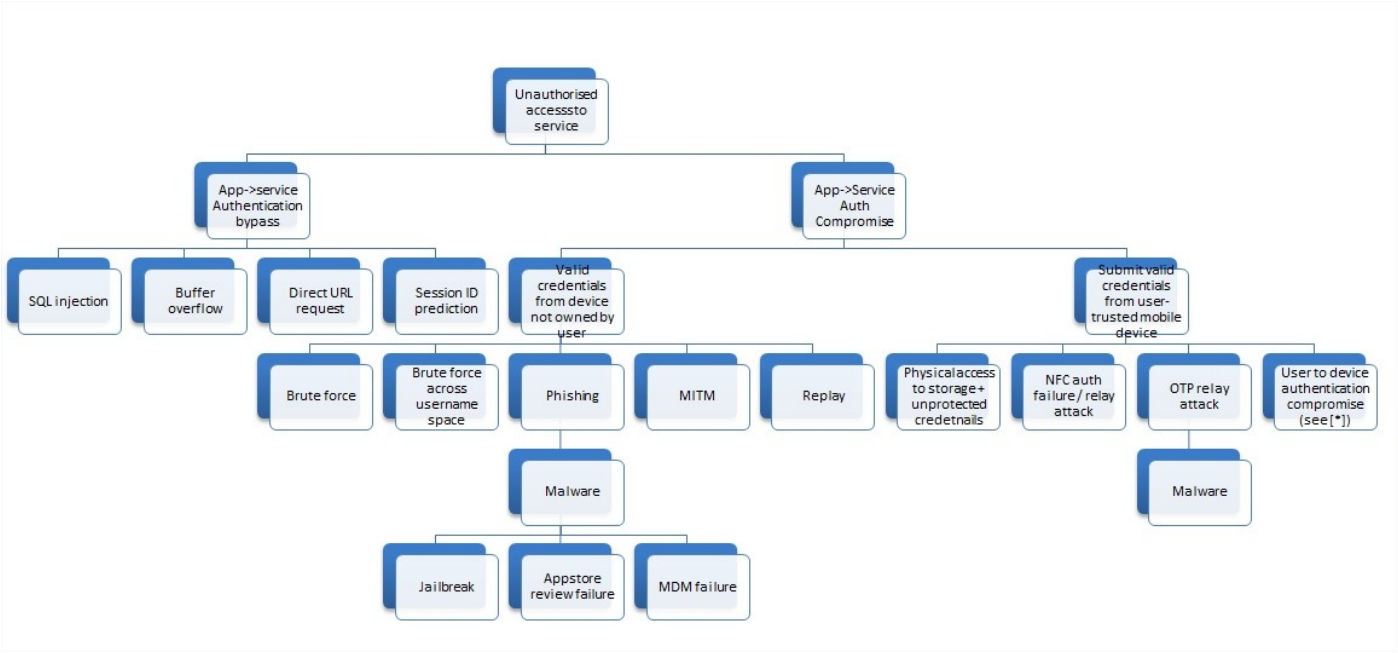
The following are taken from the OWASP Top Ten Mobile Controls and are relevant to authentication:[14]

- *Use authentication that ties back to the end user identity (rather than the device identity).*
- *Instead of passwords consider using longer term authorization tokens following the oauth model. Encrypt the tokens in transit (using SSL/TLS). Tokens can be issued by the backend service after verifying.*
- *Some devices and add-ons allow developers to use a Secure Element e.g. (5) (6) – sometimes via an SD card module - the number of devices offering this functionality is likely to increase. Developers should make use of such capabilities to store keys, credentials and other sensitive data. The use of such secure elements gives a higher level of assurance with the standard encrypted SD card certified at FIPS 140-2 Level 3. Using the SD cards as a second factor of authentication though possible, isn't recommended, however, as it becomes a pseudo-inseparable part of the device once inserted and secured.*

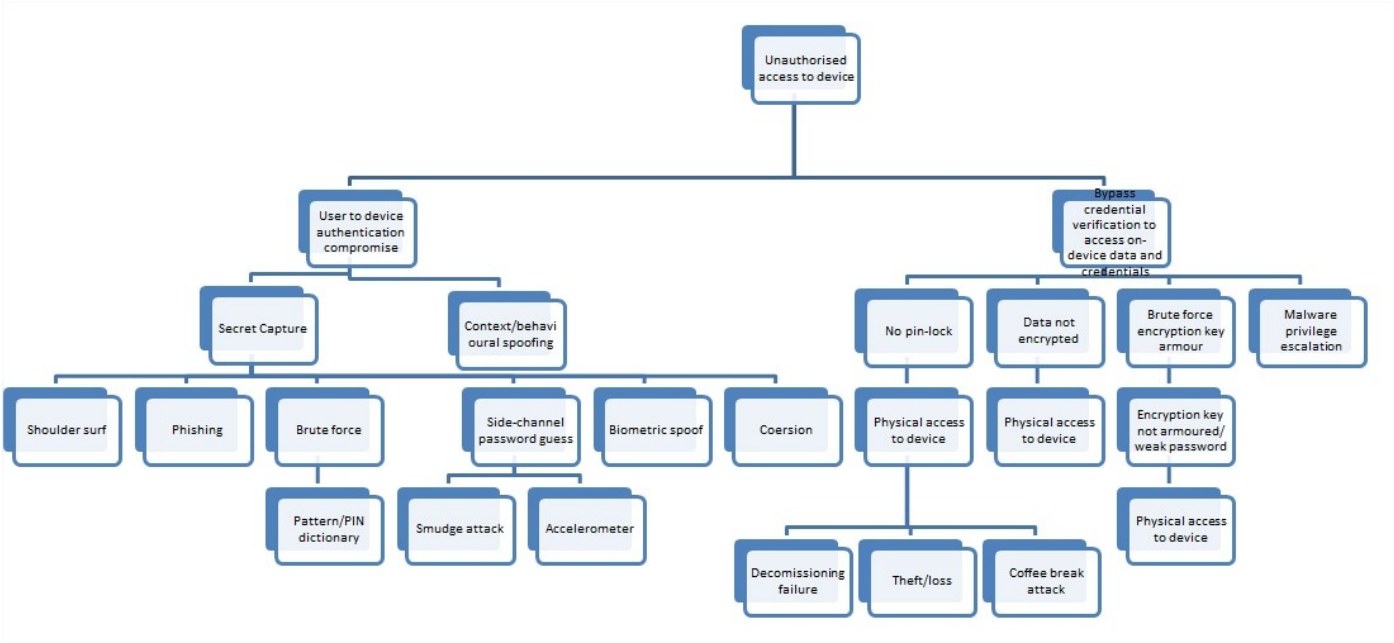
Finally, on the positive side, smartphones can be used to enhance other authentication systems:

- As a one-time password generator
- As an always-available on-person, remote killable, token
- To provide natural/haptic interfaces such as swipe, touch and accelerometer
- To provide enhanced contextual anomaly detection (e.g. location, accelerometer)

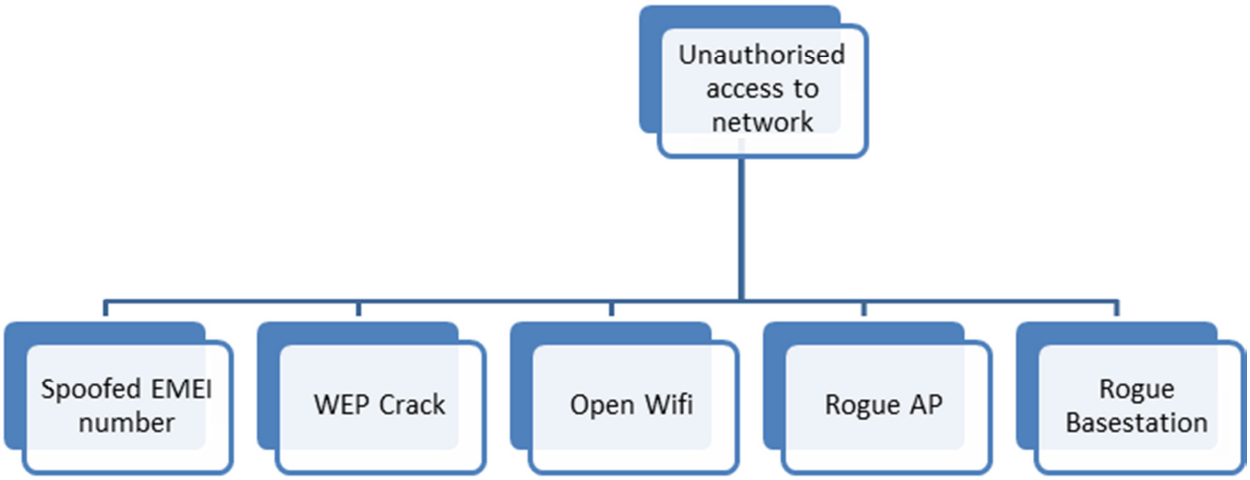
[14] https://www.owasp.org/index.php/OWASP_Mobile_Security_Project



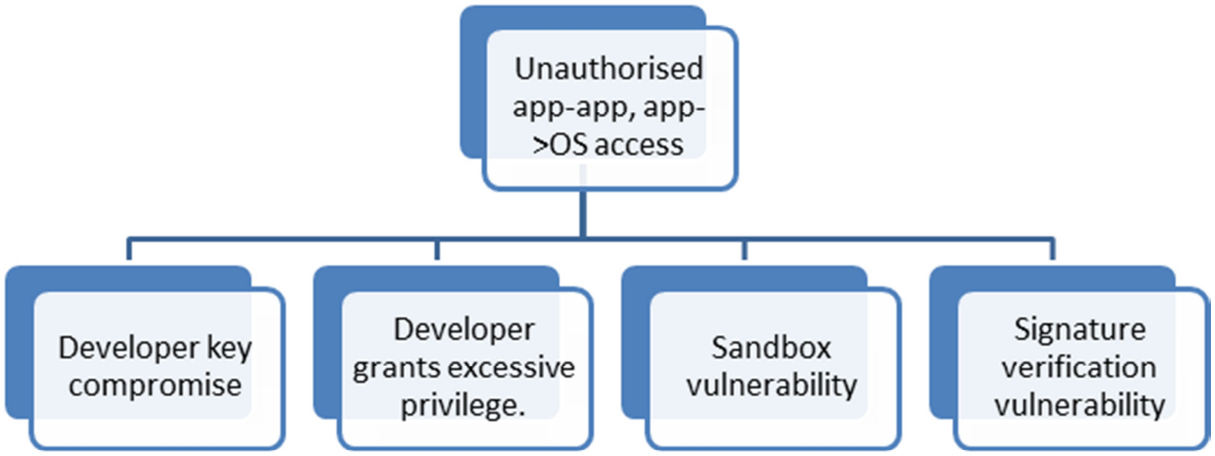
Attack Tree 1 - App->to-back-end and user->app authentication



Attack Tree 2 - User to device/OS authentication compromise



Attack Tree 3 - OS-Network authentication attacks



Attack Tree 4 – App-app, app->OS authentication attacks

5.4 Threat Level and Risk

The selection of an authentication approach should be based on a comprehensive understanding of the threats and related risks for the environment where authentication will be implemented. Authentication choice should align with business needs and account for the level of risk associated with the business and the respective data and systems. Risk factors include sources and types of threats, systemic vulnerabilities, value of the data, and legal environment.

An overview of authentication threats and risks are provided as a foundation to conduct an appropriate risk assessment. This information may be used as part of a process to conduct a risk assessment regarding choice of authentication. Decisions regarding authentication should be carefully evaluated for each specific application and care should be taken not to group all authentication decisions into a single bucket.

5.5 Threats Defined

A threat is a potentially adverse event and may be incidental or malicious. Authentication threats may stem from unintentional user actions such as loss of token or intentional attacks to bypass or break through authentication systems.

Identification and assessment of threats at all layers of authentication is an important precursor to understanding and identifying the risks. Threat identification may begin with an assessment of potential authentication vulnerabilities in the environment where authentication will be deployed. Vulnerabilities may arise from system architecture, application design, data flow, or user actions. Additionally, vulnerabilities may be singular such as code vulnerability or stem from a combination of factors such a system that provides local email access and authentication to a secure system.

Threat assessment may be performed as part of a risk evaluation. Risk evaluation employs a combination of risk assessment tools, methodologies and analyses to appropriately categorize a threat and provide insight for responding to a threat.

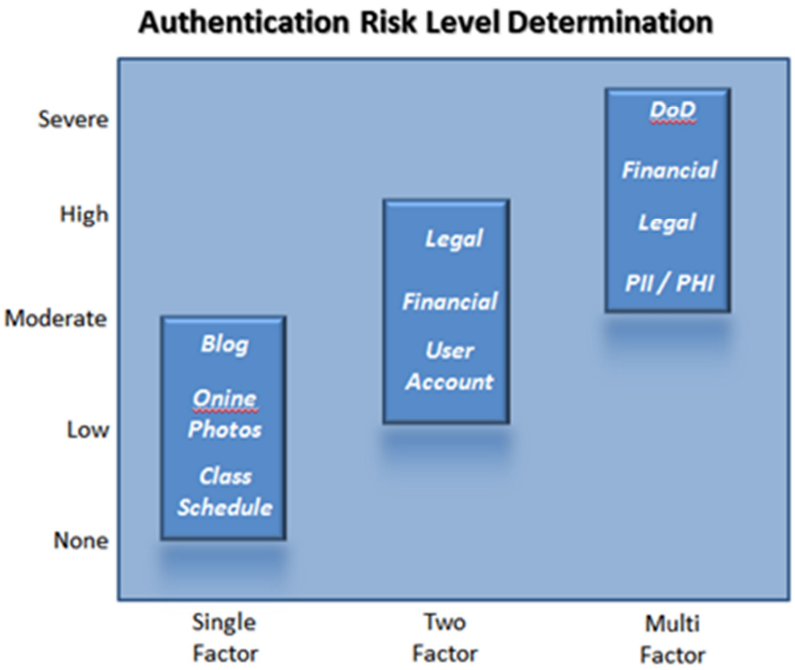
5.6 Risk Levels

Risk refers to the likelihood that an event or action will result in exposure, damage, liability or harm. The table provides a summary of risk levels that may be used to classify threats. The risk categories are broadly defined and provide a foundation for threat evaluation. There are other models for risk assessment that provide additional methods for classifying risk.

Risk Level	Description
None	Breach of authentication protocols will not result in exposure, damage or harm. May include publically available information such as on a website.
Low	The risk of breaching authentication protocols is low. Unauthorized or inappropriate access would not a significantly negative outcome. There may be a requirement for some assurance about proof of identity. The environment may have other security requirements that also reduce significant threats. Risks such as user sharing passwords would not compromise data or system being accessed.
Moderate	The risk of breaching authentication protocols is moderate. The risk of unauthorized access, data exfiltration or exposure could result in a moderately negative consequence. There may be a requirement for reasonable and current proof of identity—including multiple forms of identification. There may be limits imposed on initial authentication and re-authentication. The environment may require multiple levels of security including stronger

	authentication protocols. Scenarios may include remote access to CRM systems, access to executive-level corporate email or shared administrative/ corporate HR documents.
High	The risk of breaching authentication protocols is high. Authorized access is limited to pre-approved individuals and strong authentication provides control over access. Authentication may require multiple forms of identification and may have token expiration or other limits imposed during the authentication process. Authentication is part of strong security protocols to minimize unauthorized access. Scenarios may include limited access to protected health information (PHI), attorney-client privilege documents or financial systems.
Severe	The risk of breaching authentication protocols is severe. Authorized access is limited to highly screened and approved individuals. Strong authentication requires multiple forms of identification and may be restricted to specific locations and systems. Identification could involve the use of token, biometric encryption and user identification as part of a single authentication. Full authentication may be required every time and there may be no re-authentication. Users may have Department of Defense (DoD) or other high-level security clearances. Unauthorized access poses the highest level of risk and an exceedingly high probability of harm, injury, damage, or liability.

5.7 Authentication Risk Assessment



Authentication risk assessment is the process of ensuring that selection and implementation of authentication is consistent with the environmental risks and threats and probability of threat occurrence as well as sensitivity and vulnerability of data and systems. Authentication methods which were defined earlier in this paper should be evaluated against risk criteria.

1. **Single-Factor Authentication** is based on what one knows such as a password. Single-factor authentication may be appropriate for lower to moderate levels of risk. If appropriately implemented, single-factor authentication can provide reasonable security. For example, if the risk level is moderate and the environment is restricted to authorized personnel, long passwords with specific alphanumeric character user requirements and expiration dates may be sufficient to provide proof of identity. Single-factor authentication has an increased risk of compromise as the level of difficulty of acquiring a password or bypass authentication is lower.

2. **Two-Factor Authentication** is a combination of information that a user must provide to establish identity. Two-factor authentication should be considered for low to higher levels of risk. The decision to select two-factor authentication may be driven by a combination of assessed risk level, the environment and sensitivity of data or systems. Regulatory requirements such as state-specific privacy laws for medical information may stipulate two-factor authentication as a minimum standard.

3. **Multi-Factor Authentication** is a combination of three or more information elements that a user must provide to establish identity. Multi-factor authentication should be considered for moderate to severe levels of risk. Multi-factor authentication is most likely to be found in environments with a risk level determination of severe—such as a top-secret government laboratory or at an embassy. Similar to two-factor authentication, there are several factors that impact the choice of multi-factor authentication, and there may be mandatory requirement for multi factor authentication. Given the cost to implement certain forms of multi-factor authentication, cost may play a considerable role in the final design and implementation of multi-factor authentication.

When conducting the risk assessment, one may consider a higher risk determination if the probability of unknown threats is high. Additionally, if there are factors such as high employee turnover or vendor remote access, then a higher risk determination may be appropriate due to combinatorial threats which can significantly increase the level of risk. The choice of authentication should be commensurate with the assessed level of risk, regulatory or legal mandates, and the cost to design and implement authentication.

5.8 Conclusion

This section should not serve as the final decision-making authority for the level of authentication required for a specific scenario. A risk assessment for a specific authentication implementation is required to make this determination.

Data is an asset to any business, and may be the most valuable asset a business owns. Data must be treated with the same degree of concern required to protect any significant asset. Allowing unauthorized access could lead to various avenues of risk exposure, including identity theft, privilege escalation, and fraud. Identity and access management functions are critical parts of any data protection mechanism.

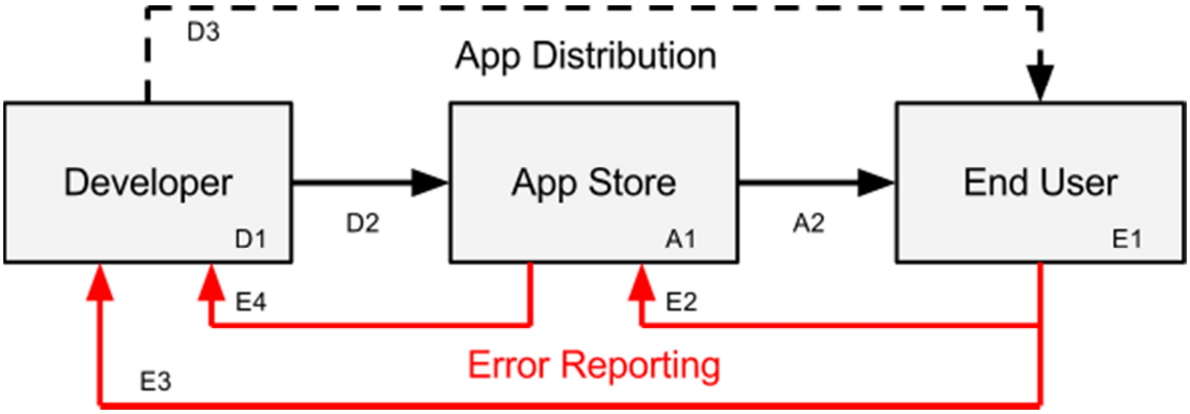
6.0 App Stores

There are presently roughly over 2 billion smartphones and tablets in use worldwide. The simple feature that differentiates these devices is the ability to tailor them to each user's needs by adding applications. There are over 1 million apps available, of which roughly 80% are currently available on either the Apple or Google stores.

Reports indicate that, during 2012, over 50 billion smartphone apps have been downloaded by users. In 2012, both Apple and Google announced that each had exceeded 25 billion downloads.

An area of concern in terms of security occurs from the developer to the app store to the end user. This can be a complex channel and represents opportunities for software (apps) to be infected, modified, or distributed with embedded malware.

6.1 The Distribution Channel



Channels of App Distribution

The actual channel of distribution is more complex than the simple flow chart. Each block can have variations and the paths for payments, refunds, updates, announcements and problem reporting. Our focus is on app distribution and error reporting, as well as security vulnerabilities at each major point in the distribution channel. The dashed line indicates lower security.

Each entity and path for app distribution is indicated by codes. D1-3 are entity and developer paths, A1-2 are app store paths, and E1-4 are end user and error reporting paths. Path D3 is dashed to indicate higher risk.

Entity	Type	Estimated App Security Risk
Developer	Independent Software Developer	High
Developer	Software/Hardware Corporate Dept./Group	Moderate
App Store	Distributor/Reseller	High-Moderate
App Store	Internal to Corporation, Enterprise	Moderate
App Store	Internal to Government or Military organization	Moderate
App Store	Smartphone or Tablet Developer/Manufacturer	Moderate
End user	Consumer	High
End user	Corporate/enterprise employee	Moderate to High
End User	Government or Military organization	Moderate

Since error reporting is addressed in this policy guideline and from outside organizations, it is briefly touched on as part of the "Distribution Channel." Error reporting generally starts with the end user or the app store. The "life" of a security report for a problem in a mobile device is not very clear; reports go to the app store (E2), then an action by the app store is required. Notification goes to the developer (E3 or E4) and possibly to the AV software company that supplied the AV software for the mobile device if the user contacts them. We have to assume that the AV software company will notify the OS company, as well as NIST CERT and NVD. There is a need to educate the end user, as well as a need for an industry guideline error reporting for developers and app stores.

Each additional element, "Developer," "App Store," and "End User" will be addressed separately, each containing several versions.

6.2 Developer

There are no general industry standards for app developers. Each OS developer does recommend general practices to insure the security and safety of their app. The most common security issues are:

- Allowing more "permissions" than are actually required by the app
- Can the downloaded app be "trusted?"
- Has a mechanism been provided for the app stores or end users to determine the download is secure and hasn't been tampered with? Several AV vendors are offering an app signature or a wrapper for apps. Previously the size of the download was provided by a source code repository. None of these is a standard for apps yet.
- Have the developers used SDK and API software and tools that are from trusted sources?
- Is there a list of trusted developers (app sources) and a standard to determine compliance with reasonable internal security practices?

Small developers are likely to continue to comprise a high percentage of available apps through the various distribution channels, as well as directly to users from their own websites. Many small developers offer apps at no cost to users. These free apps generally seem to have a higher percentage of malware. A common practice is to copy the code of a popular app, simply rename it, and offer it at a lower per copy price. The app can have malware added with a minimal amount of reverse engineering.

The diagram addresses the developer practices of distribution from developer to developer (D1), developer to app store (D2), or developer to user (D3). The highest risk path is D3, as the user is only as secure as the developer and the app the user selected to download. All Android smartphones have a setting called "Unknown sources, allow installation of non-Market apps." Enabling this setting increases the user's exposure to potentially higher risk unless the source is trusted or from a trusted market such as Google Play, Apple App Store, Amazon Appstore for Android, or Microsoft Windows Phone Store.

6.3 App Store

Popular (most visible) app stores do some testing for submitted apps, but currently, there is no standardization. Although based on limited published information, all app stores use similar approaches:

- Google Play uses a more automated approach by employing a Google tool called Bouncer but has recently announced an enhanced app approval process which may add more curation, encrypt the app, and improve security
- Apple Store is "curated" but some tools are used for common checks
- Microsoft Windows Phone Store is "fully curated" but some tools, including Hopper, are used for common checks
- Amazon Appstore for Android is "curated" but some tools are used for common checks

The current major difference is the amount and extensiveness of personal testing. All seem to scan for viruses/worms (malware) based primarily on signatures. A check is made for the maturity (age sensitivity) and offensive or pornographic material. There appears to be some differences between the stores concerning the use of third party APIs and SDKs, which appear to be treated the same as the app. There are some checks for duplicate apps.

All four major app stores appear to have, at a minimum, a signature unique to the app version and the registered developer. None have gone to the next step, or have not publicized, securing the apps with a wrapper or a more advanced code-signing providing details on the actual app.

Many of the major app stores, while manufacturing mobile devices or contract manufacturing, generally develop the mobile OS or significantly extend the software for a specific product niche. The primary mobile device manufacturers attempt to differentiate and tailor their mobile devices to a carrier's requirements.

App Store Types[15]

Type	Examples	Comment	Est. App Security Risk[16]
Device Manufacturers App Stores	Apple, Google, Amazon, Microsoft	This category could also include, for example, Samsung, which is a hardware mfg., but which is rumored to be developing a mobile OS and currently has an active App Store	Low to moderate
App Distributors Private	DOD, Navy, GE	There are many developers offering plug and play App Store software packages	Moderate
App Distributors Public	Getjar, AppsFire, Appbrain	Many companies, lots of changes, as everyone is trying to find user solution	Low
App Developers	(Too many to list)	A variety of distribution methods, most use major App Stores	Low

6.4 App Store Security Responses

Presently, there is no standardized procedure or response when an app store is advised of an infected app the end user had downloaded. The present response is to remove the infected app. Hopefully, the developer is notified and asked for a new version that is not infected and which the app store subjects to testing before making available to end users.

Historically, as compared to desktop PCs, we are roughly at the 1990-1992 anti-virus era of technology using binary scanning to compare code from applications to known signatures of code from identified malware. The detection and removal technology has traditionally lagged behind the malware and it is likely to also follow the historical model in mobile devices.

In the ENISA paper *App Store Security*[17], a "kill switch" is recommended to disable an app. Does this necessarily disable the malware? What are the legal implications of a "kill switch"? Would user notification via email or updating the infected app with a curated uninfected update be a better solution? A "kill switch" has potential legal implications and so is unlikely to be implemented in the US without supporting federal legislation.

[15] http://en.wikipedia.org/wiki/List_of_mobile_software_distribution_platforms
[16] "Est. App Security Risk" is a somewhat subjective estimate based on the authors' research.
[17] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/appstore-security-5-lines-of-defence-against-malware

Mobile devices (Android) have an auto-update service that the user can choose to enable. Currently, this is a legal method of potentially removing a malware infection on a mobile device by simply overwriting the infected app. This is relatively adequate until the security of the OS "sandbox" in the mobile devices is breached by hackers.

Notification is another option, to the mobile device or to an alternate traditional email to a personal computer. Notification potentially represents use of carrier-provided services that may result in charges to the user. This is likely to be avoided by developers and app stores until the legal situation is clarified regarding charges, or until the cellular carriers offer support for a solution.

Other possible solutions include a central clearing house. NIST NVD already exists is and is working on mobile device security[18]. It has been posting mobile device vulnerabilities to the NVD (National Vulnerability Database) since 2002. The NVD is successfully being used, by mobile device AV developers, to update their end user security packages for mobile devices. Commercial work is being done by several vendors.

A developer and app store "trust identification" list could be built and made available on the Internet as a way of demonstrating an app's reputation.

6.5 End User

There is not a single or simple type of end user (EU). The EU can fit in many roles, ranging from a consumer working for a small business, to corporation/enterprise employee or governmental/military organizations. Further, the end user's access to sensitive data will vary by position. A technician and a CEO handle data of different sensitivity to their organization.

All users should follow some basic security guidelines:

1. Always backup your mobile device and configuration. How frequently the user backs up is determined by the time required to recover your device. This provides protection from malware and from device failure or loss.
2. End users should install anti-virus, anti-malware and other security software, from trusted sources. Your mobile device is operating in the same Internet environment as your PC.
3. Where should the end user download apps from? It is generally accepted that major app stores are less likely to be a source of malware. If you are an employee of a corporation, enterprise, military, or government organization, check with your IT help desk for their recommendation. A good practice, for all users, is to simply do a search for the name of the app, the source, and the word "complaint" (Example "pinball madness 123 app store complaints"). If the search result has negative reviews, you should re-evaluate downloading the app.

[18] https://docs.google.com/viewer?url=http%3A%2F%2Fwww.us-cert.gov%2Freading_room%2Fcyber_threats_to_mobile_phones.pdf

4. The user should always check the permissions that claim to be required by the app they wish to download. When the app has been downloaded, the actual permissions can be viewed under Settings > Application > [*Downloaded App*].
5. If your phone contains sensitive or confidential data, it may be important to have an app package that locates the device and allows you to erase or lock the phone. Most phones will still allow a restore to default state but it does prevent or limit the misuse of your data. In addition, major app stores will allow users to re-load purchased apps after the initial install to the same device/phone number, so remotely erasing your mobile device does not imply you must re-purchase your apps. This is also not the ENISA "kill switch" and is completely up to the end user or organization to determine if it is appropriate.

6.6 Recommendations

A list of app stores needs to be developed and contacts need to be made with the app store's management to solicit their participation in developing procedures, practices and supporting CSA recommendations. This is especially important for consistent app AV error reporting. App stores that participate could get a CSA mobile security logo indicating the level of participation or certification. As part of this, a survey should be conducted indicating the current general security measures being used by each participating store. CSA would be interested in the measures being taken to improve the app trust for users and to reduce end user mobile device infections. An important element is notification of an AV security problem to the app developer, mobile hardware device manufacturer, and AV software companies. The only apparently clear path to NIST for NVD and CERT is through the OS developer and AV software companies.

Another recommendation would be to develop a checklist or "best practices" for app developers indicating the security measures utilized to protect their app and its users. This guideline could be the basis for a voluntary listing and award of a CSA app security logo. If malware is found, the right to use the CSA app security logo would be rescinded. This approach appears to have much less complex legal issues.

The end users should be offered guidelines that provide a very simple set of steps of how to prevent getting infected apps and how to report the app security problem to the appropriate organizations. The app security problem should be reported to the app store to stop distribution of the app, and the developer should be alerted of the potential security problem. An alert to the cellular carrier and AV software provider of the security problem should also be carried out. Currently, cellular carriers generally depend on using the "resetting to default" mobile device configuration, which clears an infected app.

Guidelines could be packaged for local CSA chapters to present as part of an ongoing educational effort for end users and organizations.

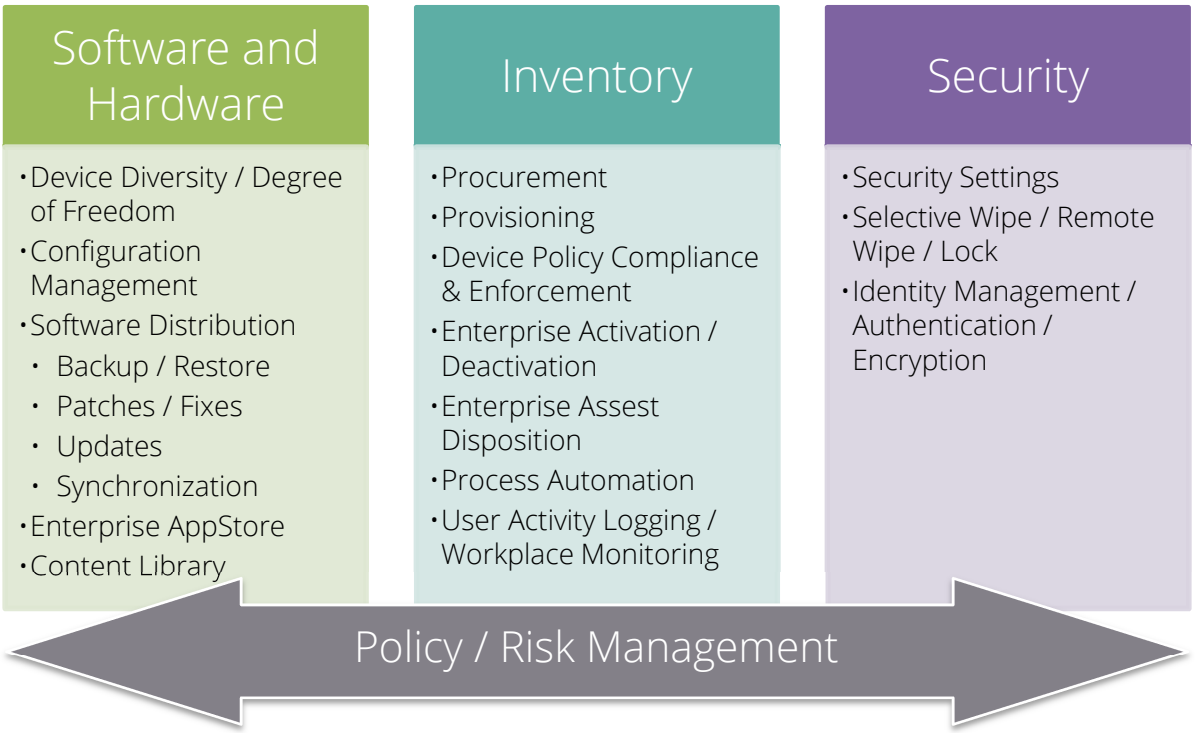
7.0 Mobile Device Management

With the growth in the number of applications, content, and data being accessed through a variety of devices, **Mobile Device Management (MDM)** is vital to managing the mobile enterprise. MDM is about much more than device management alone—it includes system-centric functionality to secure and manage data and applications, as well as information-centric functionality such as the delivery of the enterprise application store or content library.

MDM is a critical component of the device lifecycle, covering the device hardware, software, and attached services.

Full lifecycle management is required, and IT is fully responsible for the company-owned devices, including setting hardware/OS standards, application support and enterprise liability. However, organizations might choose a "degree of freedom" for their users, such as increased hardware and OS choices by BYOD support, or might provide limited capabilities such as corporate email or web services only. Both will create shared responsibilities and a mix of enterprise and user liabilities that should be properly defined, communicated, and managed.

7.1 MDM Key Components to Consider in Both Scenarios – BYOD or Company-Owned Devices



7.1.1 Policy

Rating[19]: Must Have

The definition and distribution of a **policy** is a critical prerequisite of mobile computing strategies. Organizations should assess the needs of the workforce and build or revise the mobile policy accordingly. Risk assessment and management should be performed to recognize the significance of IT and information risk, which both defines a basis for developing awareness and enables analysis of the business risk impact. A well-defined policy provides management direction and support for IT and information security and is the foundation for a solid MDM framework implementation.

7.1.2 Risk Management

Rating: Must Have

Risk management means the entire process of analysis, planning, implementation, control, and monitoring of defined measurements and the enforced policy. Organizations should consider the impact of the introduction of mobile devices as end-point devices within their corporate network. If risks are identified, the appropriate mobile device policies can be applied. In an extreme case, if the risk is deemed too high, additional controls

[19] The initial rating is based on common importance and risk level of each component. Depending on organizations individual risk assessment results, the rating might change dynamically case-by-case.

should be implemented to bring the risk to an acceptable level, allowing seamless access to IT resources from mobile devices. On the other hand, if the risk is low or non-existent, the organization can require minimal controls for the mobile devices, thereby reducing overall costs.

As part of risk management, organizations should perform risk assessment periodically (i.e. once a year) or on-demand (i.e. introducing new devices, services, or significant infrastructure changes) to provide a temporary view of assessed risks and to review the risk management process, either in parts or entirely, and make necessary changes accordingly.[20]

7.1.3 Device Diversity / Degree of Freedom — Rating: Optional

Both scenarios—BYOD and company-owned devices—require segmentation and acceptable usage planning built on a multi-dimensional matrix, which includes the user's role, responsibility (including ownership and support), data, networks and applications, and which states the user's degree of freedom for each area. This planning also defines the capabilities provided, such as corporate email, web services, support, multimedia, specialized applications and services, corporate databases such as CRM, and analytics.

7.1.4 Configuration Management — Rating: Must Have

Configuration management involves automated configuration of device settings, such as password strength and policy, email, VPN and WiFi. Configuration management aids in the elimination of user errors and minimizes vulnerabilities caused by misconfiguration, including configuration lockdown according to a degree-of-freedom definition, as well as hardware lockdown such as camera, Bluetooth, and WiFi. Configuration management is also used in an effort to enforce corporate IT mobility policies.

7.1.5 Software Distribution — Rating: Must Have

Software distribution includes applications and software accessed over-the-air or by PC synchronization. It includes updates for applications or OSs, patches, fixes, backup and restore functionality, background synchronization, and basic file distribution capabilities. Backup and restore functionality accessed over-the-air or via PC-sync in particular becomes important in situations of device crash and replacements, intentional wipeout (i.e. in case of lost or stolen device) or unintentional wipeout (i.e. kids play with device and try password too often), so the device can be recovered quickly without significant productivity loss. Aligned to the corporate mobile policies it ensures the distribution of only security assessed mobile applications to the device. Along with Configuration Management, software distribution helps to enforce the corporate approach of black-listing and/or white-listing applications and other software on the device. Mobile device management systems generally do not have a capability to analyze mobile applications for security risk. The analysis of these applications should be conducted separately in order to populate the white-list and black-list approaches with actionable application security assessments.

[20] Visit European Network and Security Agency (ENISA) website at http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms for an introduction on Risk Management and Risk Assessment.

7.1.6 Enterprise App Store — Rating: Optional

An **enterprise app store** ensures that only secure and trusted applications along with associated content will be deployed on mobile devices while providing several paths of accessibility: through deployment of mobile applications over-the-air, recommended apps from the public app store, or via a company-specific app repository. App stores include appropriate code-signing of specialized or in-house applications to ensure the integrity of the application. Enterprise app stores provide an excellent environment in the corporate mobile ecosystem to implement security testing and application whitelisting.

7.1.7 Content Library — Rating: Optional

A **content library** distributes corporate content, such as documents and multi-media videos, to provide a secure enterprise container with near-real-time updates and specific views. The library may include the secure usage of Cloud storage providers, or sandbox/virtualized environments to separate corporate content from private content. In the case of different containers it may be necessary to control applications and information differently with different policies depending on whether they or corporate or personal apps and information.

7.1.8 Procurement — Rating: Must Have

With devices evolving into application development and integration platforms, IT is likely taking ownership of the end-to-end solution by contracting wireless carriers and programs and managing service usage. However, the finance department maintains responsibility for monitoring and controlling mobility costs, such as contract and expense management. It is important to collaborate and align with Legal and HR departments to define certain terms and conditions in the policy and employee agreements. In particular, BYOD creates a mix of corporate and personal liability and responsibility. Liability for all parties should be clearly defined in these agreements and should include subjects such as private usage of corporate services, expense compensations, employee privacy policy, shared responsibilities for device and content security, misuse, secure wipe of the device including personal data in the event the device is lost or stolen, or the rights to control the device through a device management client.

7.1.9 Provisioning — Rating: Optional

Provisioning devices with a three year refresh is acceptable for company-owned devices, but IT cannot possibly manage employee-liable devices that are refreshed annually (or in even shorter cycles for smartphones and tablets). Expectations about end-user support should be clear and frequently refreshed, as self-help is often not accepted by some users, in particular those with brand new devices.

7.1.10 Device Policy Compliance & Enforcement — Rating: Must Have

Device policy compliance and enforcement is involved in device supply, control, and tracking. Asset inventory assessments are critical prerequisites for policy enforcement to comply with corporate and regulatory requirements around policies, encryption, jail-broken or rooted-device detection, and privacy-related separation of personal content vs. corporate content. Compliance and enforcement also includes approval and review processes of apps in the organization's app store, as well as approval of mobile configurations to ensure that they meet the organization's security policies before roll out. The organization will allow or deny access to

devices based on their approval status. This is an ongoing monitoring and enforcement process, often described as plan-do-check-act approach of policies in various information security management system standards and frameworks such as ISO 27001 or COBIT. It also requires alerts and notifications capabilities to provide asset reporting about devices, users, and apps. As part of the organizational infrastructure change control or similar processes, it is highly recommended to document that the policy and standard has been applied to the device and has been acknowledged by the user before the device is distributed.

7.1.11 Enterprise Activation/Deactivation Rating: Must Have

Enterprise activation or deactivation is usually a self-service functionality that activates or connects mobile devices to the enterprise network, or that allows or denies access to users based on directory groups. A proper implementation of it (in particular an implementation as a self-service) will reduce the administrative burden of provisioning and re-provisioning at the IT department. User acceptance is an important factor of it and should be clarified and well communicated in the beginning. In particular, in environments where users bring in their own devices, choosing enterprise activation will likely share certain details like operating system, device identifier, IMEI number, and more as part of the provision process. The process can be either automated through a provisioning portal to enter the required details and follow the workflow to activate the device, or it can be a manual process where the administrator will do the complete activation by taking the required details from the user. In addition, after enterprise activation, some characteristics of the device may be changed, like enabled encryption, changed password settings, certain application restrictions.

7.1.12 Enterprise Asset Disposition Rating: Must Have

Enterprise asset disposition involves removal of physical devices by decommission or by releasing the device to the BYOD owner in case of device exchange, upgrade, or permanent decommissioning. Appropriate technical and procedural controls should be in place on inventory management, user receipts or acknowledgements, and related physical actions required for proper handling during decommissioning. It is important to securely wipe the corporate data from a personal device before it is decommissioned. If the device itself is not owned by enterprise, it should be handed over to the device owner ideally without touching the personal data, music, and apps.

7.1.13 Process Automation Rating: Optional

Process automation creates and implements automated processes that link together people, processes, and technology. It automates regular tasks like device registration and lost devices (e.g. if a device is lost or stolen, an automated workflow should be initiated that remotely wipes the device and revokes particular access rights. Then, a new device should be provisioned, with appropriate pre-load and configuration prior delivery to the user). Process automation also includes technical tasks such as backup restore, as well as procedural tasks where human attestation is required (e.g. management sign-off for the order).

7.1.14 User Activity Logging/Workplace Monitoring Rating: Must Have

More and more organizations are turning to workplace monitoring[21] and data loss prevention (DLP) technology. Workplace monitoring is usually governed by a variety of privacy laws, rules, and regulations. In some countries, the laws on telecommunications regulate the monitoring of email and other electronic communications. In other countries, an employer's rights to monitor employee communications may be governed by collective bargaining agreements, employment contracts, or general privacy and data protection legislation. It is important to understand that privacy is treated as a fundamental human right and, as such, cannot be bargained away. This becomes more complex with environments with both corporate supplied and BYOD devices where laws and regulations are significantly different. Organizations are highly recommended to seek legal counsel to understand the privacy and data protection laws of the individual countries in which they operate.

7.1.15 Security Settings Rating: Must Have

According to company policy, **security settings** provide advanced security on devices irrespective of ownership. They set, deploy, and update settings like passwords, wipe, and application/resource restrictions, usually without any user intervention. Security can be broken into two basic components; user security and data security. While user and data security are tightly coupled, there are some distinct differences which must be accounted for and sometimes handled quite differently. In both cases, companies must take steps to protect the user and the data from potential threats.

7.1.16 Selective Wipe/Remote Wipe/Lock Rating: Must Have

Selective wipe securely wipes the corporate data from a personal device, without touching the personal data, music, and apps. It will also delete documents from the user's Content Library. If a device is lost or stolen, a **remote wipe** must be performed by either the administrator or the end user. The remote wipe will, in effect, wipe all information from the device returning it to factory default configuration. Similarly, a **Lock** can be performed on a device by the administrator or end user to ensure that protection is in place should the device become temporarily misplaced. If the wrong password is entered multiple times, an automatic wipe will be triggered.

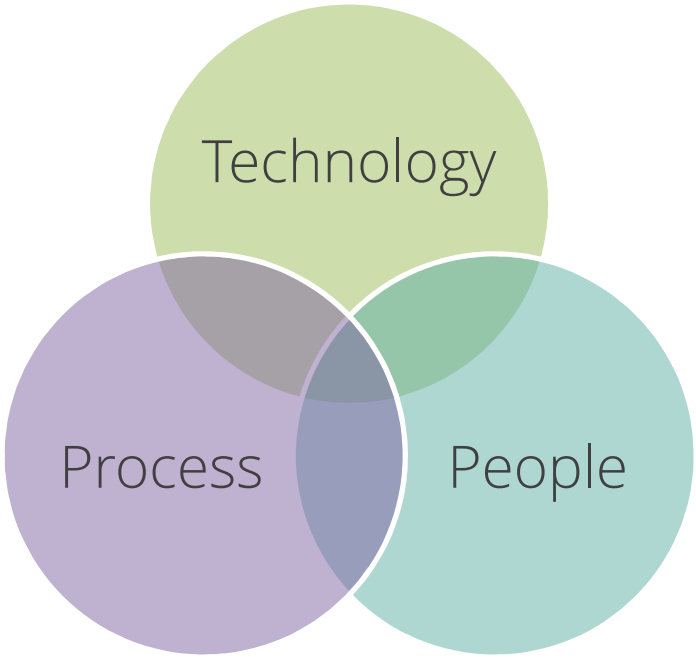
7.1.17 Identity Management Rating: Must Have

Identity management, authentication, and encryption involved management of strong encryption of local data (device memory, external memory cards) and data in motion (such as email S/MIME encryption and authentication). It requires certificate distribution capabilities and certificate-based authentication (including device ID, OS version, phone number) to identify the device and user properly. Strong certificate-based authentication enables secure access to corporate email, web-based applications, VPN and WiFi. It comes along with overlaying identity management processes and mechanisms by which enterprise employees are issued

[21] The term "monitoring" is used broadly to refer to any reading, collection, or storage of electronic communications. Monitoring is, therefore, more than the interception of communications in transit. Copying of employee emails for backups or scanning messages to detect viruses are both considered to be monitoring.

accounts and credentials required to provide access to the device, the business applications and services based on a context-aware policy that includes who they are, their role, their device, their network and their information and application. It could also enables employees access to cloud applications and services on mobile devices via single sign-on credentials and identity brokering to authenticate to third-party SaaS.

7.2 Conclusion



Mobile devices have quickly become a mainstay in enterprise environments, and while mobile devices continue to be consumer driven in both form and function they have found their way into our day-to-day business lives. Mobile device management, like management of any technology or resource in the corporate space, has to start with the basic understanding of the key components of that eternal "people, process, technology" triangle. While most companies already have security policies in place, those policies need to be reviewed and possibly updated to account for the many components of mobile technology that have been spelled out in this document. Every company will have a different tolerance for risk and will adopt mobile technology in different ways, but there are still several fundamental components of mobile device management that have to be considered and incorporated into policy and practice to ensure that introducing this technology will not compromise security.

As the mobile technology continues to advance, and new uses for it are discovered some of these key components outlined in this document may become more critical to a successful security strategy than others. There may also be new components to mobile device management that come into play as the technology continues to advance. Mobile devices are a great personal enabler and the consistent availability of mobile devices makes the integration of personal and business objectives almost inevitable. As such, the Cloud Security Alliance Mobile Working group will continue to work on educating and developing guidances around mobile devices and how best to manage and integrate them into our work environments.