KEVIN MAHAFFEY AND MIKE MURRAY

The Spectrum of Mobile Risk:

Understanding the full range of risks to enterprise data from mobility

The Spectrum of Mobile Risk:

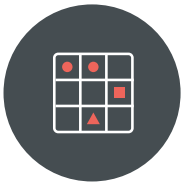
Understanding the full range of risks to enterprise data from mobility

The time has come for enterprise risk management to change. Mobile devices have become core to our personal and professional lives, yet most enterprises remain focused on traditional PC endpoints.

Although many of the same elements of risk that affect PCs also apply to mobile endpoints, simply extending current PC security controls to your mobile fleet is ineffective.

Enterprise risk management needs to evolve to address mobile risks, and security professionals must architect mobile-specific security.

To encourage this evolution, Lookout developed the Mobile Risk Matrix. Its purpose is to help security organizations understand the spectrum of risk on mobile devices and to provide data that demonstrates the prevalence of mobile risk.



THE MOBILE RISK MATRIX

Vectors

Components of Risk

	APPS	DEVICE	NETWORK	WEB & CONTENT
THREATS	**App threats** Malicious apps can steal info, damage devices, and give unauthorized remote access.	**Device threats** Device threats can cause catastrophic data loss due to heightened attacker permissions.	**Network threats** Data is at risk of attack via Wi-Fi or cellular network connections.	**Web & content threats** Threats include malicious URLs opened from phishing emails or SMS messages.
SOFTWARE VULNERABILITIES	**App vulnerabilities** Even well known software development companies release apps that contain vulnerabilities.	**Device vulnerabilities** The vulnerability window is the time it takes from the release of a new patch to adoption.	**Network vulnerabilities** Mobile devices encounter more hostile networks than laptops, and have less protection.	**Web & content vulnerabilities** Malformed content, such as videos, and photos can enable unauthorized device access.
BEHAVIOR & CONFIGURATIONS	**App behaviors & configurations** Mobile apps have the potential to leak data such as contact records.	**Device behaviors & configurations** USB debugging for Android or installing apps from non-official app stores.	**Network behaviors & configurations** Misconfigured routers, unknown captive portals, or content filtering.	**Web & content behaviors & configurations** Websites that don't encrypt credentials or leak data.

Get a printable version of the Mobile Risk Matrix here.

To create the Matrix, Lookout examined our massive global data set of mobile code, device software, web, and network attacks compiled from both enterprise and personal active users, and leveraged our ten years of research into mobile threats and vulnerabilities.

Of course, organizations will need to assess each element of the Mobile Risk Matrix within their business context. For example, even though the overall prevalence of targeted iOS spyware is low, an organization developing critical trade secrets might consider their executives to be high-risk targets and assign a higher level of risk to their mobile devices.

Understanding Mobile Threats

Mobile threats are now being reported with increasing frequency in the news on television, in online publications, and newspapers. Mobile threats also continue to increase in sophistication, with the Pegasus spyware on iOS and Android as the ultimate example of a professional mobile espionage attack. Pegasus is classified a device threat in the Mobile Risk Matrix. However, the full attack includes phishing a target (a web & content threat) and exploiting software vulnerabilities. This is the key to understanding mobile threats – malicious attacks that occur across vectors to gain access to data.

How to think about App Threats

Malicious mobile apps can do many nefarious things, including stealing information, physically damaging devices, and monitoring a user's or organization's activities. Common examples include legitimate mobile apps that have been injected with malicious code; malware that gets on a device through exploitation or carelessly granted user permission; or abusive apps with masked intent, such as a flashlight app that accesses all personal information for malicious or unauthorized commercial purposes.

Many enterprises think that their Mobile Device Management (MDM) solution will protect them from malicious applications, but because users can "sideload" apps onto their phone, Lookout sees a consistent incidence of malicious applications appear on our enterprise customers' devices.

How to think about the prevalence of App Threats

Over the fourth quarter of 2016 and first quarter of 2017, 47 in 1,000 of Android enterprise devices protected by Lookout encountered app-based threats, and only 1 in 1,000 iOS devices encountered an app-based threat.[1]

How to protect against App Threats

A comprehensive strategy to protection against app threats includes more than Mobile Threat Defense, it also includes:

- An MDM & Mobile Application Management (MAM) solution for corporate managed devices
- Intrusion defense systems (IDS) and intrusion prevention systems (IPS)
- The inclusion of mobile-specific information in threat intelligence feeds and network controls (e.g., blacklisting of mobile "command & control" servers in firewalls)
- Detecting and examining mobile app downloads through any URL filtering/web security controls.

[1] The analyzed data came from a large subset of global Lookout personal and enterprise sensors, and ranging in time periods between April 15, 2016 and April 16, 2017. The enterprise data includes both Android and iOS devices from financial institutions, healthcare organizations, government agencies and other notable industries. The personal data includes both Android and iOS devices from consumers around the globe, consisting of over 100M devices worldwide.

How to think about Device Threats

Security threats that affect mobile device operating systems and firmware have significant potential to cause catastrophic data loss and surveillance because attackers can obtain higher levels of permission than ordinarily granted to apps.

The Pegasus spyware is the most relevant example of a targeted, low-prevalence, high-impact device threat for both iOS and Android devices. With a single tap on a socially engineered phishing SMS, Pegasus can activate a phone's cameras and microphone to snoop on conversations taking place around the device and can also track a victim's movements and steal messages from end-to-end encrypted chat clients.

The real issue with Device Threats is that all other on-device security and management relies on the assumption that the device itself has not been compromised. However, a fundamental reality is that if a mobile device has been compromised, the container that securely houses corporate data (including all MDM & MAM solutions) is able to be compromised as well.

The issue becomes even more acute when organizations use mobile devices as part of a multi-factor authentication solution, which puts an immense amount of trust in the "soft token" placed on the mobile device as the default second factor.

Lookout Security Intelligence researchers have repeatedly seen this strategy employed in banking trojans, which compromise the device to steal both the user's password as it is entered and the second factor code to enable them to log into the bank using an SMS token.

Ultimately, whether installing security controls on the phone to protect corporate data or to serve as the access token for other resources, the device must be secure before that software is installed.

How to think about Network Threats

Network Threats take advantage of weakness in how web sites or applications establish TLS/SSL sessions over Wi-Fi, cellular, or other networks. These attacks can be executed directly by attackers or through malware using automated methods. Examples of these incidents include "man-in-the-middle" attacks, certificate impersonation, TLS/SSL stripping, or TLS/SSL cipher suite downgrades.

In the past, while network-based attacks were possible, they were rare and what was inside the firewall was generally considered safe. In the last few years however, mobility has multiplied the number of networks that a device will encounter: every day, every device in your mobile fleet will be on other networks for more time than they will be under enterprise control. This means that network attacks that were less prevalent when all of your devices largely stayed in the building have suddenly become more of a concern.

How to think about the prevalence of Network Threats

Over the last year, fewer than 10 in 1000 (.8%) enterprise devices encountered a man-in-the-middle threat.

It's worth noting that some of these man-in-the-middle attacks can include non-intentional interceptions of enterprise data, such as content filtering done at schools, but even without malicious intent these interceptions are in a real sense an "attack" on the data protection measures put in place to otherwise prevent others from looking at data in transit.

How to think about Web & Content Threats

Malicious content is most commonly delivered through phishing emails or text messages that contain links that direct users to websites that purport to be official login pages. For example, after a socially engineered phishing SMS, Pegasus begins as a website that exploits a browser vulnerability and later exploits a device kernel vulnerability.

Users on mobile are three times as likely to enter their credentials in a phishing page compared with desktop users, according to a 2011 study by IBM. The phishing messages usually contain links that lead to malicious websites that can cause drive-by downloads or the injection of malicious code onto a device.

How to protect against Web & Content Threats

It is incredibly important to focus on content threats because they're most often the entryway into corporate assets. Stopping the content threat often equates to stopping the entire kill-chain early, such as with the text messages that deployed Pegasus or a drive-by download that installs a trojan on the user's device.

In addition to a Mobile Threat Defense solution, stopping Web & Content Threats includes checking that email filtering and anti-spam have mobile-specific phishing protections, mobile specific protections in the web-content filtering, and even the deployment of social media security tools to protect your users against phishing that occurs through social networks (which are often a mobile-specific phishing attack like the one used to infect the Israeli Defense Force with the ViperRAT trojan in 2016).

Understanding Mobile Software Vulnerabilities

The challenge of securing the mobile environment is not limited to the wide array of threats aimed at mobile technology. The apps and devices themselves include vulnerabilities that can increase the likelihood of a security incident occurring.

How to think about App Vulnerabilities

Mobile apps have vulnerabilities just as PC software does. But vulnerabilities are a significantly bigger problem on mobile apps because most mobile apps are selected by end-users and are more likely to be built by small teams of developers. PC applications on the other hand, are more likely to be vetted by IT and developed by large software companies.

How to think about the prevalence of App Vulnerabilities

Researchers on the Lookout Security Intelligence team have performed in-depth analysis on numerous popular Android and iOS productivity and business applications. These assessments identified a diverse range of vulnerabilities, varying both in required attacker sophistication and impact to the end user. On the high-risk, high-sophistication end of the spectrum, Lookout discovered flaws in some of these apps that would allow adversaries to compromise not only the information a user viewed in an app, but also a victim's cloud service account and all information tied to that account.

A published example of an app vulnerability with high prevalence is Android's unsafe usage of addJavascriptInterface, where Lookout measured over 90,000 apps that were likely vulnerable – an impossible patch logistics problem.

How to protect against App Vulnerabilities

While security controls around data in transit from mobile apps have improved in recent years, even well known software development companies have released apps that contained security flaws, putting corporate and user data at risk.

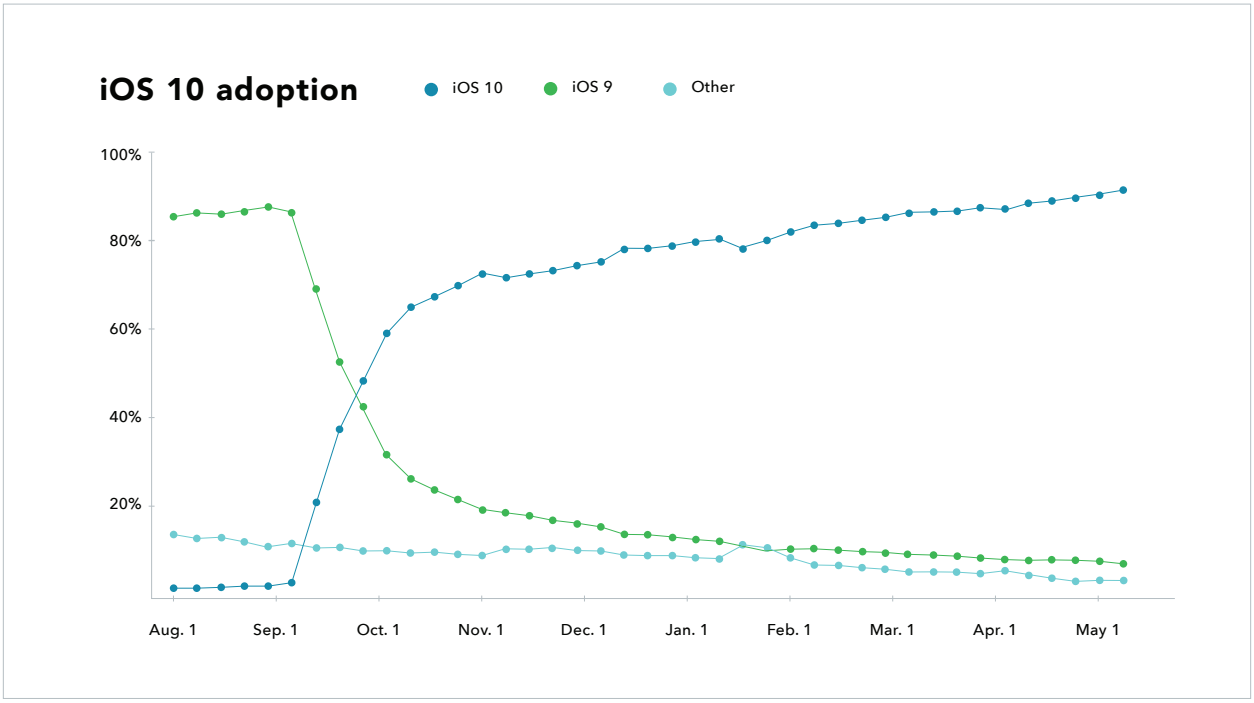
App Security Assessments often identify inadequate security controls around data in transit, with potentially significant ramifications such as inadvertently leaking sensitive information or providing malicious actors with a window of opportunity to directly attack a victim's device. These risks can have a minimal or catastrophic impact, depending on an adversary's sophistication and imagination.

As more organizations support the use of mobile apps that handle sensitive user and corporate data, expect this area to become increasingly attractive for adversaries seeking to exploit app weaknesses and gain access to this information.

How to think about Device Vulnerabilities

Mobile devices are also plagued by a large number of known vulnerabilities. Google and Apple regularly release security bulletins detailing the rising number of fixes for device vulnerabilities recently discovered.

Enterprises can measure risk from device vulnerabilities by tracking their "vulnerability half-life," or the amount of time it takes from the release of a new patch to full adoption of that update in their mobile fleet. In general, mobility programs based on bring-your-own-device (BYOD) tend to have a longer vulnerability half-life than programs based on company-owned devices, and Android device fleets have a longer window than iOS fleets. The vulnerability window of both mobile platforms is still significantly longer than the vulnerability half-life of the typical enterprise device, which vulnerability management vendor Qualys pegs as 30 days.



This data from Mixpanel shows that iOS was able to get to >90% adoption of iOS 10 within eight months.

How to think about the prevalence of Device Vulnerabilities

Across personal devices protected by Lookout, as of April 2017, just 43% of users have updated their iOS operating systems to version 10.3 or higher, 42% have updated to 10.2, and 6% have updated to 9.3.5.

This means many users are operating devices that do not have the latest security updates. Some 15% of the iOS users have iOS vulnerabilities around WebKit, the browser engine behind Safari, the App Store and many iOS apps.

As for Samsung Galaxy S6 users, 92% haven't updated to the latest version of the operating system, 7.0 Nougat.

How to think about Network Vulnerabilities

Network Vulnerabilities enable the device to be attacked through the network, by enabling the device to be compromised due to a vulnerability in the device operating system or data to be intercepted.

For example, in a talk at Black Hat Asia in March 2017, researchers showed how to exploit an iOS device remotely via Wi-Fi without any user interaction, completely bypassing the iOS sandbox. Even more recently, according to an article in SC Magazine, Apple issued iOS version 10.3.1 to fix a flaw that is exploitable via Wi-Fi and that enables someone within range of a vulnerable device to exploit the iOS flaw.

How to think about the prevalence of Network Vulnerabilities

While nearly every endpoint security suite since Windows XP has included a firewall and Host-based Intrusion Detection / Protection (HIDS / HIPS) solution, mobile devices don't have the same level of protection and have the potential to encounter many more hostile networks than the traditional laptop.

How to think about Web & Content Vulnerabilities

Any malformed content, including Web pages, videos and photos, can trigger specific vulnerabilities to exploit targeted application or operating system components to gain unauthorized access to a device.

The most widely known example is Stagefright, a device vulnerability that is exploited by a video file to access the media processing libraries of Android that could lead to exploitation over any number of vectors. These vectors include MMS messaging or arbitrary channels such as file downloads over the Web where media files are processed.

How to protect against Web & Content Vulnerabilities

While nearly every Web & Content vulnerability will be related to an app or device vulnerability, enterprises should consider them separately because of the opportunity to apply complimentary controls to prevent exploitation. Content vulnerabilities delivered through the web can take advantage of whatever web-content firewall already exists (at least while in the building or on VPN). Additionally, preventing mobile phishing through better email content protection, and even social media security products can assist in ensuring that content attempting to trigger a vulnerability will never reach the mobile device in the first place.

Understanding Behaviors & Configurations

Employees in many cases are a particularly high risk, because they're often using their own personal mobile devices for work, and these devices are much more likely to be configured in ways that conflict with an organization's security policy. Many CISOs want to be able to enable a BYOD policy, and would if they could carefully secure it. Getting visibility into behaviors and configurations is the first step to enabling secure mobility.

How to think about App Behaviors & Configurations

Sensitive app behaviors can lead to the leakage of enterprise data accessed by certain apps.

Examples include:

- Apps that access sensitive enterprise data and public cloud-based storage services not under enterprise control.
- Apps that access data with compliance requirements such as credit cards or personally identifiable information, and don't have adequate protection for the use, transmission, and storage of that data.

How to think about the prevalence of App Behaviors & Configurations

Among enterprise mobile devices protected by Lookout, from 4Q16 to 1Q17, 11% of iOS devices encountered sideloaded applications, 30% of apps accessed contacts, 30% accessed GPS, 31% accessed calendars, 39% accessed the microphone, and 75% accessed the camera.

Across iOS enterprise apps, 43% connected to Facebook and 14% connected to Twitter.

How to think about Device Behaviors & Configurations

The risk from Device Behaviors & Configurations largely stems from employees using mobile devices they have jailbroken or rooted, but can also be as simple as not enabling a passcode on a device. Most Device Behaviors & Configurations are device specific and include USB debugging for Android, installing apps from non-official app stores, and certain enterprise configuration profiles on iOS. Many of these examples can be addressed by a Mobile Device Management Solution.

How to think about the prevalence of Device Behaviors & Configurations

Among enterprise mobile devices protected by Lookout, 1 in 1,000 iOS devices are jailbroken, and 5 in 1,000 Android devices are rooted.

How to think about Network Behaviors & Configurations

Network Behaviors & Configurations are best understood as the risk from employees using public Wi-Fi. The more "promiscuous" end-users are in connecting to public Wi-Fi, the greater the risk to enterprise data.

Traveling employees may take advantage of Wi-Fi in airports, hotels, coffee shops, or other public facilities and never know if they connect to a misconfigured router, unknown captive portal, or a network that decrypts traffic for content filtering.

How to think about the prevalence of Network Behaviors & Configurations

To understand the scale of this challenge, consider every employee in your organization – potentially with multiple devices per employee – and multiply that by the number of networks those devices will encounter. For a global enterprise the result is a significant number of new potential risks of data leakage on mobile.

How to think about Web & Content Behaviors & Configurations

Enterprise employees on a regular basis open email attachments from unknown people, or click links in SMS messages and other messaging apps. Attachments might contain any type of content, but tend to be media files. When accessed, these files pose the risk of exploitation and phishing by malicious content or a malicious web page.

Protecting against the spectrum of mobile risks in your organization

The next steps for extending your security program to mobile start with thinking through each element of the Mobile Risk Matrix and developing a strategy to manage that risk in the context of your security environment.

No two organizations' use of mobile are alike. Each will have different needs that are functions of their unique business. After assessing the likelihood and impact of these risks, organizations will be in a better position to plan their bespoke security strategy, rather than pursuing a "one-size-fits-all" model.

Start this process by asking two key questions of your security organization:

1. How you are measuring the risk from each element of the matrix in your current environment?
2. Then ask how you are controlling for that element of your mobile risk?

Most security organizations will find that they have very limited visibility into most mobile risks, and are similarly limited in how to control these risks with existing solutions.

> "Security and Risk managers responsible for endpoint and mobile security must start now to evaluate Mobile Threat Defense (MTD) tools, and gradually implement these solutions in complement to EMM."
>
> **Gartner Predicts 2017: Endpoint and Mobile Security, Nov 2016**

For this majority, the next step would be to follow Gartner's recommendation that, "Security and Risk managers responsible for endpoint and mobile security must start now to evaluate Mobile Threat Defense (MTD) tools, and gradually implement these solutions in complement to EMM."

Security organizations that gain visibility into the entire spectrum of risk, as well as provide an effective mobile threat defense, assurances of mobile app reputation, and mobile vulnerability management, will enable their employees to get the most value from mobile technology, securely.

About the authors

Kevin Mahaffey
CTO and co-founder of Lookout

Read more from Kevin

Mike Murray
Vice President of Security Intelligence

Read more from Mike