

# Mobile Security: Are You at Risk (Yet)?



Shridhar Mittal  
CEO | Zimperium

*“Cat and mouse, often expressed as cat-and-mouse game, is an English-language idiom dating back to 1675 that means “a contrived action involving constant pursuit, near captures, and repeated escapes.” [1] The “cat” is unable to secure a definitive victory over the “mouse”, who despite not being able to defeat the cat, is able to avoid capture. In extreme cases, the idiom may imply that the contest is never-ending.”<sup>1</sup>*

*Clearly, whoever came up with that phrase a few centuries ago, must have known about Internet security. The smartest minds and billions of dollars later, we are still in the midst of an incredible “cat-and-mouse” game with no end in sight.*

## What's Next? – Evolution of Security Solutions

Without going too far back, there have been many multi-billion dollar waves and companies created in security. Desktop security plays like Symantec (Norton) and McAfee were followed by the firewalls (Checkpoint and Cisco) and Intrusion Detection (IDS) and Prevention (IPS) vendors like Sourcefire/Cisco and ISS/IBM. Then came the next generation firewall (Palo Alto Networks) and advanced threat protection (FireEye) companies. So what's next?

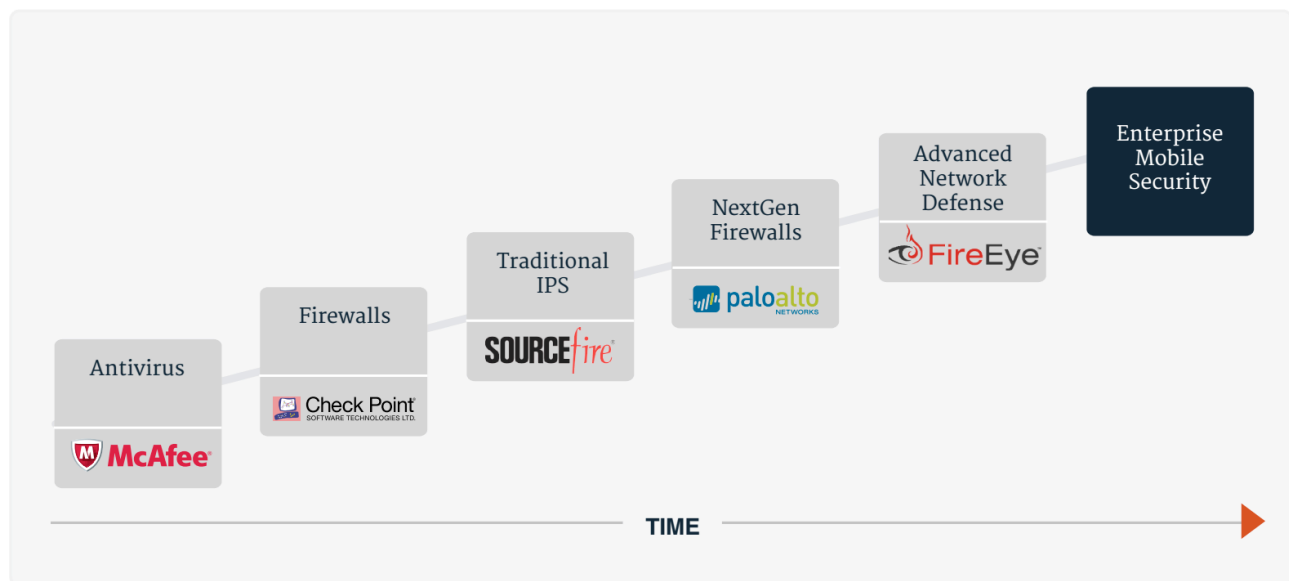


Figure 1. The evolution of security solutions

The Wall Street Journal boldly stated on July 31, 2014 that “Smartphones Become Next Frontier in Cybersecurity”<sup>2</sup>. This comes after Mobile Device Management (MDM) companies like AirWatch (acquired by VMware for \$1.5B), Zenprise (acquired by Citrix for \$400M) and MobileIron (Nasdaq: MOBL) have all garnered significant valuations. But are these really “security” companies or are we just scratching the surface of the problem?

1. [http://en.wikipedia.org/wiki/Cat\\_and\\_mouse](http://en.wikipedia.org/wiki/Cat_and_mouse)

2. <http://online.wsj.com/articles/smartphones-become-next-frontier-in-cybersecurity-1406808182>

## Is It Enough? – Some Significant Shortcomings

The Gartner view: “Nearly **2.2** billion smartphones and tablets will be sold to end users in 2014 according to Gartner, Inc. With the number of smartphones and tablets on the increase, and a decrease in traditional PC sales, attacks on mobile devices are maturing. By 2017, Gartner predicts that the focus of endpoint breaches will shift to tablets and smartphones and 75 percent of mobile security breaches will be the result of mobile application misconfiguration. The best defense is to keep mobile devices fixed in a safe configuration.”<sup>3</sup>

I would agree with Gartner's analysis. Let me give you a few examples of the rapidly increasing issues that are being experienced globally.

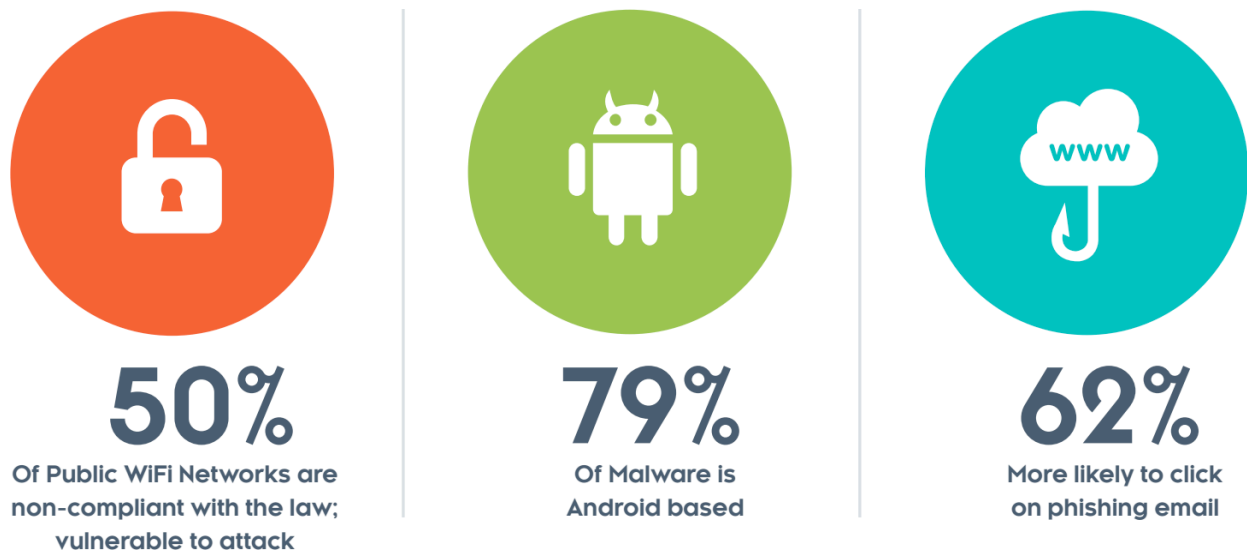


Figure 2. Nature of security threats

## WiFi attack example: Global Fortune 500 CFO visiting the Philippines

Andy is on a short business trip to Manila. Given his position, he has permission to access the company's financial information. He logs into the hotel WiFi on his company-issued iPad to catch up on the latest baseball highlights and complete some online bill pay. His tablet is equipped with the leading MDM and mobile AV solution. Unfortunately, however, there's a hacker on the same WiFi, who does a Man-in-the-Middle (MITM)<sup>4</sup> attack. For good measure, he injects a few malicious scripts to Andy's traffic, to compromise his machine by exploiting the browser vulnerability. Once Andy returns from his trip and logs back into the corporate network, the infection spreads from his tablet and begins to send high value data back to the attacker. Given his elevated privileges, the damage is quite significant despite the state-of-art MDM and mobile AV solution.

## App Store example: Bypassing mobile anti-virus using Download-and-Execute

Donna, a key engineer at a leading Silicon Valley startup, is traveling with her family and her son decides to download a new game recommended by one of his friends, onto his mom's smartphone. The app turns out to be malicious, despite a scan by the leading signature-based AV installed by corporate IT. This was not caught because it was a “zero day” or “unknown” malicious app, which is not picked up by signatures. The malware then installs a Remote Access Tool (RAT), allowing an attacker to remotely execute commands. Even though Donna's phone has a secure container solution issued by corporate IT, the device is compromised and the attacker enables a keylogging and/or a screenshot capture feature, obtaining sensitive data within the Secure Container Solution.

3. <http://www.gartner.com/newsroom/id/2753017>

4. [http://en.wikipedia.org/wiki/Man-in-the-middle\\_attack](http://en.wikipedia.org/wiki/Man-in-the-middle_attack)

## Spear-Phishing – Targeted email attack via document attachment

CEO Bob is not directly targeted with malicious emails. However, the online behavior of Bob's assistant Charles, exposes CEO Bob to unknown security risks. Charles likes to open links through social media, especially those links with tempting titles like, "Last day to sign up for XYZ conference". Charles clicks on a malicious link and unknowingly compromises his mobile device. Attackers can now use Charles' compromised device as an entry point to target CEO Bob by chaining a MITM attack. As soon as Bob uses his browser on the same Wi-Fi network as Charles, traffic can be redirected through the compromised device and injected with the same browser vulnerability that initially compromised Charles' device. This attack pattern can be used repetitively to hack anyone's mobile device throughout the organization.

There are a growing number of such threats that are just NOT addressed by the existing options currently available in the market.

## Legacy Mobile Security Solutions Leave Gaps

I believe there are three main groups of established software companies that are attacking the mobile security problem.

- The legacy anti-virus vendors like McAfee, Symantec and Trend Micro as well as some of the consumer-focused companies like Lookout (moving more into enterprises) that scan for malicious applications.
- The mobile device management (MDM) players like AirWatch (VMware), MobileIron and Zenprise (Citrix) are focused on device asset management and "secure data access" to email and line-of-business apps.
- The network security leaders like Palo Alto Networks, FireEye and Sourcefire (Cisco) are just beginning to focus on the mobile edge of the network and advanced mobile threats. However, there's a definite lack of visibility once the devices leave the corporate perimeter.




LEGACY MOBILE SOLUTIONS	METHODOLOGY & INTENT	MOBILE SECURITY GAP
 Network Security	Protect mobile endpoints from cyberattacks on the corporate network	Can't see mobile threats or protect mobile traffic after it leaves the corporate network
 Mobile Device Management	Stop non-compliant devices from connecting to the corporate network	Can't protect mobile devices against cyberattacks
 Anti-virus	Scan for known malicious apps using signatures	Can't protect mobile devices against unknown threats on or off the corporate network

Figure 3. Legacy Mobile Security Solutions

Legacy approaches to mobile security only solve pieces of the problem. Enterprises need to adopt a security solution optimized for mobile devices that provides complete visibility and protection against known and unknown threats around the clock. Ideally, this solution should detect threats even without connectivity, to ensure the device is continuously protected without impacting the user experience or violating user privacy. If IT Security Administrators have visibility to mobile traffic both on and off the corporate network, combined with risk profile data for every device, appropriate policies can be implemented to protect the device and corporate network from an exposure.

According to Gartner's July 2014 report on the Hype Cycle for Enterprise Mobile Security, "all current solutions (especially in the first two buckets above) are entirely based on application layer attacks on mobile devices (Layer 7). OS vulnerabilities and lower stack device and radio layers are likely to be exploited." With more business being conducted on the go, outside of the office, on WiFi or cellular networks than ever before, the risk of cyberattacks is significantly increased. One compromised mobile device from either a host or network attack can result in a security breach, compromising an organizations data, assets and brand.

## Should Enterprises Care Now? The mobile attack vectors on businesses

The Sierra Ventures CIO Advisory Boards<sup>5</sup> has over 100 senior technology executives from various F2000 companies. This Advisory Board recently consulted with Zimperium and shared that they have already received numerous requests from global telcos, international banks, premier media outlets, consumer retailers and others, who are looking beyond their current MDM and AV solutions for "true mobile security".

Businesses have invested in deploying "1st Generation" mobile cyber security solutions such as Mobile Device Management (MDM), Mobile Application Management (MAM) and Anti-Virus. Most reports highlight Apps as one of the most dangerous threat vectors, with huge recent increases in modern mobile malware targeting mobile devices likely to top the 1 million mark by the end of this year. Although impressive in volume, other types of attacks have the potential to cause significantly more impact to organizations than malicious Apps have seen to date. Due to the growing mobile device market, and the recent wave of attacks like [Shellshock](#), [Masque](#), and [WireLurker](#), the Zimperium Security Labs team believes that 2015 will be the year that previously undetected mobile attacks go mainstream and wreck havoc on the enterprise.

### There are two primary threat vectors:

#### 1. Host attacks

- Spear-Phishing via email/sms: Browser link, Doc, PDF and other client side attacks
- Kernel Exploits
- OS Exploits
- Apps

#### 2. Network attacks

- Starts with Reconnaissance Scans (IPv4/IPv6)
- Man-In-The-Middle (MITM)
- SSL Stripping
- Rogue AP
- Rogue Base station / Femto cell

Advanced hackers have already adapted to mobile environments and are using similar techniques to what they used to infiltrate Fortune 500 companies in the past:

1. Attacks that require user interaction like spear-phishing – hackers send an email with a link or Doc/PDF attachment – as soon as you open the file or link your device is compromised.
2. Attacks without user interaction: network attacks that include MITM and injection of browser or other client side vulnerabilities.

Usually (1) and (2) are chained with additional attacks, which allows the hackers to completely takeover the device using Kernel/OS exploits.

5. <http://www.sierraventures.com/cio-network/>

## Why Is Mobile Different? – The Unique Challenges of Mobile Security

Mobile devices are difficult to protect. Enterprises are struggling to deal with the fact that employees are accessing sensitive corporate data across both private and public networks. Whether its the hotel network or the malicious application in the earlier examples, Chief Information Security Officers (CISOs) have a major problem on their hands. And here are just a few of the reasons why mobile security poses unique challenges:

- **No root privileges:** most security solutions need access to root privileges in order to detect and block threats. The traditional methods that are known and used by many vendors for years in the PC / Network world, cannot be applied on mobile devices.
- **Host attacks:** the attacks are happening outside of the security vendors' sandbox – therefore they are blind to see simple attacks like 'download-and-execute'.
- **Network attacks:** Mobile devices constantly roaming to unknown environments. Airports, hotels and conferences WiFi's are extremely dangerous.
- **Battery life and CPU:** this is probably one of the greatest challenges that security vendors have never had to deal with before. Solutions have to perform without a significant drain on battery life or being too CPU intensive.
- **BYOD:** the wide range of devices being brought into an enterprise has resulted in a large number of operating systems to protect and comply with policies of Google, Apple, etc. Across Android devices, the solution needs to support multiple architectures, vendors and settings.
- **User experience:** mobile security solutions need to be un-intrusive and cannot alter the user experience or impede user productivity given the critical nature of the user's phone.
- **User Privacy:** most security solutions reply on sending data to the cloud for inspection – opening up complaints from users about their right to privacy.

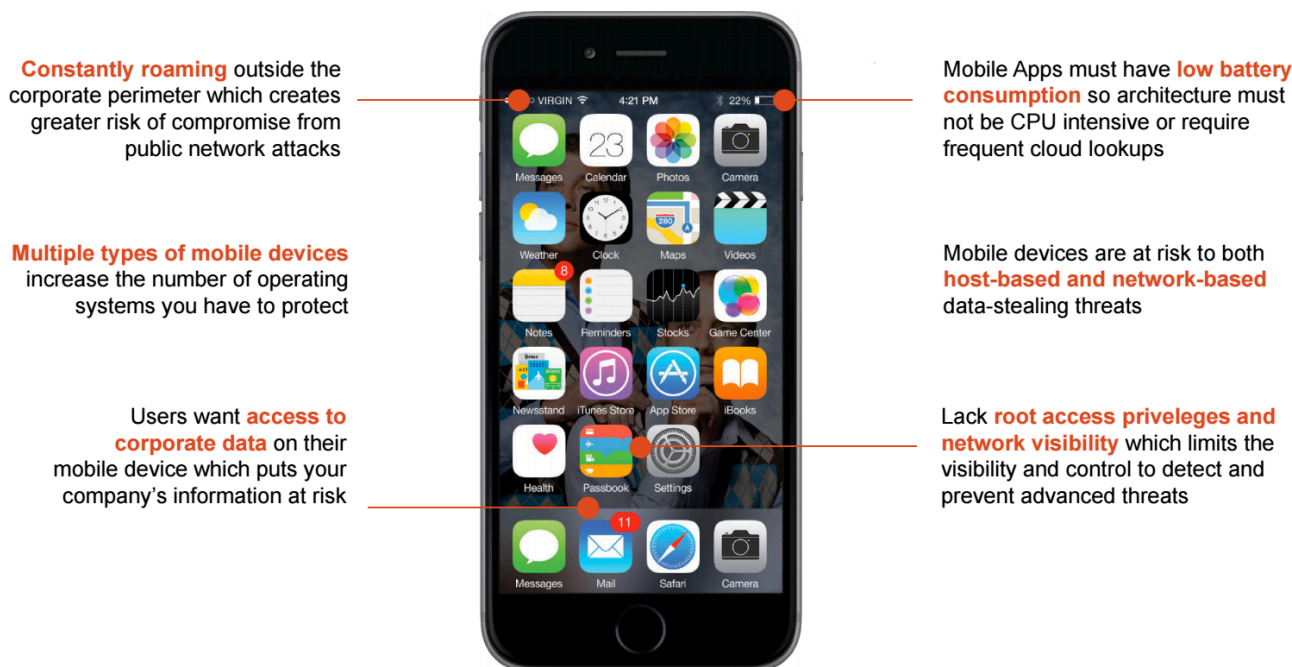


Figure 4 Mobile Security Requirements<sup>6</sup>

6. Source: Zimmerium Inc.

# What To Do Next? – Look for True Mobile Security Solutions

Zimperium is a new and exciting company built from the ground-up to focus on mobile security. Zimperium recently developed a revolutionary mobile security system that provides complete enterprise protection against sophisticated network and host based threats for both iOS and Android devices. It is the only mobile threat defense system capable of monitoring processes outside of its own sandbox. Zimperium utilizes an on-device, behavior-based detection engine to monitor and secure the entire device for malicious behavior (rather than just scanning apps) without introducing latency. Zimperium integrates with existing mobile management solutions like MDM to ensure easy deployment with an organization's existing security infrastructure. Zimperium offers the key features that enterprises are looking for today:

- › Endpoint protection, behavior – based detection of abnormal activity on the device.
- › Protection against host (spear-phishing, malicious apps) and network attacks to prevent mobile devices from coming back into the enterprise and compromising the corporate network.
- › 'Always-On' protection – don't need to be connected to be secure. Works across public or private WiFi, 3G, or no connection (unlike antivirus and other solutions that rely on the cloud and/or WiFi to protect you), without draining your battery (problem with cloud-assisted solutions).
- › Platform agnostic – works on both Android and iOS, and ultimately secures all mobile devices.

Organizations that are concerned with securing against advanced network and host based attacks need to know more than if the device has been rooted or whether a malicious app has been installed. A true mobile security solution needs to provide an enterprise with a way of measuring the risk to the whole device and the resulting impact to the business. Enterprises will be best served by implementing a mobile security solution that can integrate with existing MDM and MAM technologies to manage, secure and protect mobile devices around the clock. An organization will know they have been successful with their implementation if they can answer the simple question – has a mobile device within my organization been compromised and what actions should I take to mitigate the risk?

The majority of businesses today are realizing that their current defense strategies have serious security gaps when it comes to securing mobile devices. We are seeing an increasing demand from customers, large and small, who have previously deployed MDM and mobile AV solutions across their organizations. The recent slew of attacks has increased the level of urgency and elevated it to a boardroom topic. It's just a matter of time before every business re-examines their security policy to ensure they have a complete plan for protecting mobile devices and in turn their corporate networks from cyber attacks. Companies are beginning to look beyond the current MDM and AV solutions and seriously evaluate more robust mobile security solutions. It's just a matter of time before enterprise mobile security is widely adopted within the enterprise.



Zimperium is a leading enterprise mobile threat protection provider. Only the Zimperium platform delivers continuous and real-time threat protection to both devices and applications. Through its disruptive, on-device detection engine that uses patented, machine learning algorithms, Zimperium protects against the broadest array of mobile attacks and generates "self-protecting" apps.

## CONTACT US

101 Mission Street  
San Francisco, CA 94105  
Main: 415.992.8922 | Toll Free: 844.601.6760  
sales@zimperium.com  
[www.zimperium.com](http://www.zimperium.com)  
© 2016 Zimperium | All Rights Reserved