Mobile Intrusion Prevention: Threat Landscape

Zuk Avraham | Esteban Pellegrino | Eyal Elyashiv | Mark Murtagh

Executive Summary

The continuing evolution of today's digital society has mobility firmly at its core, where security and privacy combine to seek to protect personal information and other sensitive mobile data assets. Businesses have invested in deploying "1st Generation" mobile cyber security solutions such as Mobile Device Management (MDM), Mobile Application Management (MAM) and Anti-Virus. However, delivering adequate cyber security in today's mobile threat landscape is complex and is continuously evolving. The modern mobile threat landscape changes by the hour and requires on-going innovation - at the core of effective protection is the ability to quickly assess, monitor and automate preventative measures leveraging a new generation of cyber threat technology.

The Modern Mobile Threat Landscape whitepaper highlights a number of attack vectors that specifically affect mobile devices. The main focus of this whitepaper is network attacks, outlining fundamental techniques used by attackers to perform such attacks. As of today, existing solutions in the market do little to address these threats.

This article also demonstrates the impact of such threats by using publicly available tools and know-hows against the most up to date mobile operating systems.

The market highlights Apps as one of the most dangerous threat vectors, with huge recent increases in modern mobile malware targeting Android likely to top the 1 million mark by the end of this year.[1] Although significant in volume, other types of attacks have the potential to cause significantly more impact to organizations than malicious Apps we have seen to date. This paper covers the following:

- Describes attacks that can be used to infiltrate key executives in organizations.
- Demonstrates existing solution effectiveness against known techniques commonly used by attackers. Explains fundamental flaws in design of some of the most common solutions in the market.
- The techniques in this whitepaper describe a variety of methods from Network to Host based attacks.

ZIMPERIUM was also benchmarked with solutions such as Mobile Device Management (MDM), Mobile Application Management (MAM), Mobile Anti-Virus and non-mobile solutions such as Next-Generation Firewalls like Palo Alto Networks.

The results of the benchmark testing highlight ZIMPERIUM's unique approach and superiority in Network and Host Intrusion Prevention techniques. ZIMPERIUM provides advanced technology which operates in user-mode allowing instant BYOD deployment by using a new innovative technique called 'non-intrusive packet monitoring'. This technique is optimized for mobile devices resulting in minimal battery, memory and CPU consumption, combined with complete preservation of the user experience.

For more information, you are welcome to visit my personal security-related blog / twitter.

Zuk Avraham
Founder / CEO
ZIMPERIUM

The Mobile Threats

The mobile threats described here include several attack vectors of different threats that can be used. The attacks can be categorized into three segments:

- Network attacks
- Host attacks
- Growing Basestation threats

Only well-funded and extremely technical attackers will use this attack method. Since smartphone hardware is different from one vendor to another, and even in the same model there are sometimes differences in firmware, chips, etc - carrying out attacks using basestations are dependent on exact hardware specification and may become fragile thus the victim sometimes may suffer from strange reboots or bricking the device. Therefore, Basestation attacks are not widely used and generally attackers will seek for ways to go up the stack to Network / Host based attacks in the OS. Attackers that use hacked-femtocell typically elevate to the OS layer of attacks such as Network and Host attacks as well.

Please note that this paper is focused on Network and Host attacks.

Network attacks

Network attacks usually start in the same order among all attackers:

Network Reconnaissance

This phase will help the attackers to identify the targets. Network reconnaissance usually starts by scanning the targets. Once open ports or potential vulnerabilities are detected, the attackers would switch to phase 2 which is Server-side or Client-side attacks.

Server-side:

1. **IPv4:** Once an attack has been identified in an open service, the attacker may use this to hack the device remotely. Currently there are no open ports in default installations on smartphones. The only opened service scenario is seen when the victim opens a hotspot and the attacker has the opportunity to connect to it. At that point, the victim has port 53 UDP opened - No public attacks are known with this scenario - This attack scenario is unlikely.

   IPv4 scans are used nowadays to identify the target system, version, and other necessary information to carry out further attacks.

   IPv6: IPv6 Scanners already exists. Even though the communication is not fully IPv6 yet, it depends on the router you're connecting to. It is highly likely that IPv6 attacks will be an increasing threat on mobile devices especially when operators complete infrastructure upgrades to IPv6 world.

2. IPv6 scans are used nowadays to identify the target system, version, and other necessary information to carry out further attacks.

Client-side:

1. As demonstrated in previous Pwn2Own competitions[2] both iOS and Android were hacked remotely using browser attacks - An attacker can use MITM technique and combine it with 'Client-Side' exploit to take full control of the victim's device. These techniques are appealing to attackers as there is no direct interaction with the victim necessary.

Mobile Host Threat Landscape & Attack vectors

Host attacks[3] are very similar among all attacks observed in the last few years. In the smartphone arena it can be difficult to distinguish what the actual threat is - mainly due to superficial mass marketing and a sequence of common misconceptions. The purpose of this section is to highlight threats that external hackers targeting organizations will facilitate by compromising BYOD.

As explained in the network attacks section above, there is a distinct advantage executing network based attacks since there is no required interaction with the victim. However, the ultimate combination to take over an entire organization is by chaining both network and host attacks.

Smartphone host attack vectors

Firstly, it is important to understand that **Apps are not the most important threat vector!**

In the past 2-3 years, it seemed that Apps were the master of all evil. The way industry generated a need for containerization and additional sandboxing technology was to promote Apps as the primary threat vector. Unfortunately, this is not the reality of what we are dealing with!

Based on real world attacks, executives and other agents that are connected to important business services such as CRM are lucrative targets. Also consider, what are the odds that the targets will download the specific Apps developed by attackers? That app development is not their domain of expertise.

It also goes back to the traditional statement "iOS is safer because of the walled-garden." - again, it is unlikely Apps will be used by hackers to infiltrate organizations. Since both iOS and Android devices were hacked using other methods[4] described below the statement above is not relevant and both iOS and Android should be equally considered legitimate targets for today's threats.

So how do hackers infiltrate mobile devices such as smartphones and tablets?

Browser Exploits - Client-side attacks on browsers remain the most popular approach used by hackers. Vulnerabilities in WebKit[5] based browsers are not new. This attack will happen by sending a link to the victim followed by victim's natural call to action (open the link) the attacker will gain the same permission as the browser. Most attackers will now chain an Elevation of Privileges (EoP) attack to achieve persistency on the device.

Vulnerable Client-Side applications, such as PDF Reader[6] - I demonstrated onstage at the Intel Security Conference 2012 how to generate a malicious PDF in less than 40 seconds. It seems that this attack is becoming increasingly common and ZIMPERIUM already observed instances of such attacks happening in the wild. Similarly to Browser attacks, attackers will chain PDF vulnerabilities with EoP attacks.

Other client-side software - Calendar invites, default handlers, etc.

Food for thought

Key executives in organizations are not necessarily directly opening emails with links / unknown PDFs. The executive's assistants may be targeted to open links through social engineering, especially with interesting titles like "Last day to sign up for XYZ conference". At which point, the device of the assistant becomes compromised. Attackers can then use this compromised device as an entry point to the key executive by chaining a Man-in-the-Middle attack. As soon as the executive uses their browser on the same Wi-Fi network, traffic can be redirected through the compromised device which in its turn will inject the same browser vulnerability that was used to hack the assistant's device. This same attack can be used repetitively to hack others throughout the organization.

Due to lack of privileges exposed by the OEMs, security vendors often make use of the existing APIs to offer limited security enhancements. The following table provides some insight into existing security solution approaches and the primary disadvantages of these approaches.

Security approach	Fundamental limitations and design flaws
Container (MAM)	Container is an additional sandbox to contain several sandboxes. A single kernel exploit will allow the attackers to control the entire device including all different sandboxes and containers within the device[7]
Lock/Wipe (MDM)	1. Additional security layer is needed to detect a compromised device[8] 2. Some devices do not support complete wipe, need to assure that the data that is valuable for the user is deleted upon wipe command.
Signature-based detection (Mobile AV)	1. Does not detect browser / PDF attacks run in a different sandbox as described above. 2. Fundamentally cannot detect Download-and-Execute payloads (see benchmark). 3. Detection software runs in sandbox and not accessible to OS attacks (e.g: folders without permissions to check). 4. Once a threat was found, the AV cannot "remove" / "uninstall" as the attacker now has higher permissions than the AV software. 5. Signature can be easily manipulated[9]
VPN	1. Does not detect attacks. 2. Device can be compromised during Wi-Fi "accept terms-of-service" phase - Connectivity must be established to setup a tunnel. 3. Latency 4. Cost 5. Usually disabled when inside company network, 3g and 4g.

Mobile AntiVirus vs. Download-And-Execute payload

Based on our research we observed that when planting an exploit in the app file, it may get detected by the AV engine – if modifications were not performed on the exploit code. Due to the way that Mobile AntiVirus operates this makes complete sense – as they have access to the App files and can check the files that are bundled with it[10]

The average attacker does not plant exploit code in the app in order to avoid detection. This technique, unfortunately misleads most commonly used 'Mobile AntiVirus'.

During our research tests existing Mobile AntiVirus solutions failed to detect **ALL** of the attack attempts due to previously described fundamental AntiVirus sandbox limitations – Mobile AntiVirus cannot see anything that is outside of their sandbox, so Download-and-Execute payloads are the ultimate approach used by hackers today to evade detection by this type of vendor solution.

For example, we have tested 4 exploits vs. commonly used Mobile AntiVirus solutions, producing the following results:

Exploit	ZIMPERIUM	McAfee	Symantec	Kaspersky	AVG	Avast	Sophos	Lookout
ZergRush	Yes	NO	NO	NO	NO	NO	NO	NO
Gingerbreak	Yes	NO	NO	NO	NO	NO	NO	NO
RageAgainstTheCage	Yes	NO	NO	NO	NO	NO	NO	NO
Exploid	Yes	NO	NO	NO	NO	NO	NO	NO

Mobile Network Threat Landscape & Attack vectors

Currently, hackers are using the following techniques and attack vectors to achieve their end goal which is infiltrating organizations or obtaining valuable information that can be extracted from key executives or high-profile targets.

Smartphone network attacks are increasingly endangering organizations as many of today's Wi-Fi networks are in uncontrolled environments such as Airports, Cafés and are even now present on Commercial Airlines.

Existing smartphone attack vectors & attack chains

Network Attack Vector	Attack chain	Severity	Threat	Damage
Network Reconnaissance (IPv4)	Server-side exploit	Important	Information Disclosure	From information disclosure to potentially compromised device. Early discovery can help identify potential Zombies/compromised devices in organization.
Network Reconnaissance (IPv6)	Server-side exploit	Important	Information Disclosure	From information disclosure to potentially compromised device. Early discovery can help identify potential Zombies/compromised devices in organization.
Network MITM	Client-side exploits	Critical	Remote Code Execution (RCE)	Device can be compromised using a chain of client Side exploit such as PDF or Webkit vulnerability
Rogue AP	Client-side exploits | SSL Striping | Passive	Critical	RCE, Information Disclosure, Password stealing	Device can be compromised using a chain of client side exploit such as Webkit vulnerability. Attacker can strip SSL sessions to achieve confidential information without hacking the device.

The Test Environment

Testing Devices:

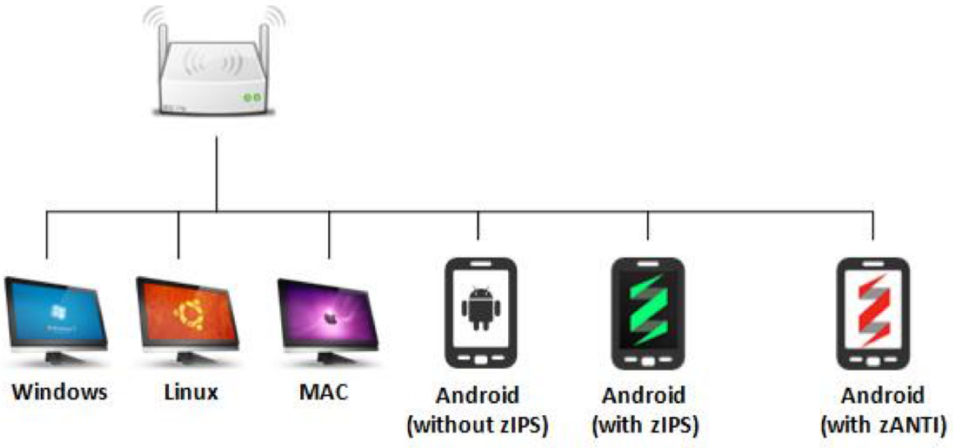
DEVICE	OS Type
Samsung Galaxy Tab	Android 4.1.2 Jelly Bean
Samsung Galaxy Y Young	Android 2.3.6 Gingerbread
Samsung Galaxy S Duos	Android 4.0.4 Ice Cream Sandwich
iPhone 5	iOS 7.0.4

Lab Setup:

zIPS™ is a revolutionary new product that transcends current mobile security solutions beyond basic monitoring and protection. zIPS is a seamless mobile security suite that identifies malicious threats and takes immediate preventative action. Zimperium's professional security scout is trained to combat threats automatically using z9™ behavioral analysis engine.

zANTI™ is a comprehensive network diagnostics toolkit that enables both IT Managers and Penetration Testers to perform complex security audits and assessments at the push of a button. zANTI provides a cloud-based reporting platform that walks you through simple guidelines to ensure network safety.

A zIPS enabled smartphone connected to a Wireless Network (Home/ Office) where malicious activities that involve different Network attacks including IPv4, IPv6, MITM including wide variety of techniques.



Pentesting Platforms and Tools

Operating System	Attack Test Tools
Windows 7	• Nmap CLI/GUI v6.25 • Cain and Abel • ARP Spoof • Simsang 1.8.0 • SwitchSniffer Scan • Blue Port Scanner • NScan
Android phone	• zANTI2 • dSploit • Port Scanner UTOPICSOFT • Port Detective Net Audit TCP Port Scanner • TCP Port Scanner Network Scanner -IP Discovery • Network Discovery • Fing Network Tools
Ubuntu / Backtrack	• Nmap CLI/GUI v6.25 • Ettercap • ARPSpoof • Scapy • Intercepter-ng • Hping3 Scan Mode • Hping3 Spoof Mode • Fing • Net Discover • Intercepter-ng • TCP Fast Scan • Unicorn Scan • PBNJ 2.04 • Netifera • Knocker • Genlist • Protos • Netcat • Alive6 • Detect Sniffer • Exploit Test • Firewall Test • Fragmentation Test • Fuzz IPv6 • Implementation6

Network IPS

Benchmarks: Network Intrusion Prevention System

Comparison of zIPS detection capabilities (on-device) running over multiple networks vs. Palo Alto Networks VM-300 next-generation firewall.

Attack Types	zIPS	Palo Alto Networks VM-300
Scanning - IPv4		
Basic Scan	Yes	Yes
TCP Connect Scan	Yes	Yes
TCP Syn Scan	Yes	Yes
TCP Ack Scan	Yes	No
TCP Fin Scan	Yes	No
TCP XMAS Scan	Yes	No
TCP Software Fingerprinting	Yes	Yes
TCP Null Scan	Yes	No
RPC Scan	Yes	Yes
TCP Evading IDS Scan	Yes	No

* Currently the test could not be completed, as the ZIMPERIUM lab is not equipped with appropriate equipment. If you own a Network IPS and would like to volunteer to be part of further tests, please do not hesitate to contact us.

Benchmark: zIPS vs. Mobile Antivirus

Scan	Commands	**Mobile AV** (McAfee/AVG) (Avast/Lookout) (Symantec/Kaspersky)	**MDM** MobileIron ZenPrise Fixmo / etc	**ZIMPERIUM**
Basic Scan	nmap $target	No detection	No detection	Success
TCP Connect Scan	nmap -sT $target	No detection	No detection	Success
TCP SYN Scan	nmap -sS $target	No detection	No detection	Success
TCP ACK Scan	nmap -sA $target	No detection	No detection	Success
TCP FIN Scan	nmap -sF $target	No detection	No detection	Success
TCP XMAS Scan	nmap -sX $target	No detection	No detection	Success
TCP NULL Scan	nmap -sN $target -Pn	No detection	No detection	Success
UDP Scan	nmap -sU $target	No detection	No detection	Success
Protocol Scan	nmap -sO $target	No detection	No detection	Success
RPC Scan	nmap -sR $target	No detection	No detection	Success
Window Scan	nmap -sW $target	No detection	No detection	Success
Evading IDS	nmap -f $target	No detection	No detection	Success
Version Detect	nmap -sV $target	No detection	No detection	Success
Hping3 Scan Mode	hping3 --scan known $target	No detection	No detection	Success
Hping3 Spoof Mode	hping3 -a 192.168.1.23 -- scan known $target	No detection	No detection	Success
Fing	fping -g 192.168.1.0/24	No detection	No detection	Success
Net Discover	netdiscover -i eth0	No detection	No detection	Success
Simsang 1.8.0	Start Simsang > Scan Network > Scan	No detection	No detection	Success
SwitchSniffer Scan	Select the Interface > Scan	No detection	No detection	Success
Blue Port Scanner	Input the Scan IP and Scan	No detection	No detection	Success
NScan	Single Host> Initial Host : 192.168.1.52 > Start	No detection	No detection	Success
TCP Fast Scan	./tcp-fast-scan 192.168.1.52	No detection	No detection	Success
Unicorn Scan	Unicorn 192.168.1.52	No detection	No detection	Success
PBNJ 2.04	./scanpbnj 192.168.1.52	No detection	No detection	Success
Netifera	./netifera New Space > Input 192.168.1.0/24 > Right Click Discover TCP Services	No detection	No detection	Success
Knocker	./knocker -H 192.168.1.52 -SP 1 -EP 1024	No detection	No detection	Success
Genlist	genlist –scan 192.168.1.0/24	No detection	No detection	Success

Protos	Protos -i eth3 -d 192.168.1.52	No detection	No detection	Success
Netcat	Nc -v -w 2 -z 192.168.1.52 1-1024	No detection	No detection	Success
Port Scanner UTOPICSOFT	Target: 192.168.1.52 Port Range 1-1024 Scan	No detection	No detection	Success
Port Detective	Target: 192.168.1.52 Port Range 1-1024 Scan	No detection	No detection	Success
Net Audit TCP Port Scanner	LAN DISCOVERY	No detection	No detection	Success
TCP Port Scanner	IP: 192.168.1.52 Port Ranges: 1 to 65535	No detection	No detection	Success
Network Scanner - IP Discovery	Scan Select the Target Scan Ports	No detection	No detection	Success
Network Discovery	Discover	No detection	No detection	Success
Fing Network Tools	On Start	No detection	No detection	Success

IPv6 Attacks	Commands	Mobile AV (Detection)	MDM (Detection)	zIPS (Detection)
Alive6	./alive6 wlan0	No detection	No detection	Success
Detect Sniffer	./detect_sniffer6 wlan0 fe80::b2ec:71ff:fe89:e30c	No detection	No detection	Success
Exploit Test	./exploit6 wlan0 fe80::b2ec:71ff:fe89:e30c 80	No detection	No detection	Success
Firewall Test	./firewall6 wlan0 fe80::b2ec:71ff:fe89:e30c 22	No detection	No detection	Success
Fragmentation	./fragmentation6 -p -n 1 wlan0 fe80::b2ec:71ff:fe89:e30c	No detection	No detection	Success
Test	./fuzz_ip6 -s 22 -n 1 wlan0 fe80::b2ec:71ff:fe89:e30c	No detection	No detection	Success
Fuzz IPv6	./implementation6 wlan0 fe80::b2ec:71ff:fe89:e30c	No detection	No detection	Success

MITM Attacks	Mobile AV (Detection)	MDM (Detection)	zIPS (Detection)
ICMP Redirect	No detection	No detection	Success
SSL Strip	No detection	No detection	Success
ARP spoof	No detection	No detection	Success

Conclusion

Robust mobile security begins with enhancing network inspection and prevention solution capabilities. This is particularly important as more businesses and other enterprises encourage or permit employees to adopt BYOD.

You can see in our research above that the mobile arena is still considered immature in terms of Mobile Intrusion Prevention System (Mobile IPS) technologies. There are solutions in the market that address narrow use cases but the need for a robust solution is increasing. Another prominent point in this article is that there is no such thing as a 'secured mobile OS' both Android and iOS share the same threat vectors when it comes to advanced security. The benchmark results above outline today's market and its offering.

The overall research results show less emphasis needs to be placed on 1st generation mobile device management (MDM) and Anti-Virus systems designed to operate by leveraging containers and traditional signatures – Today's Modern Mobile Threat Landscape requires a new approach, one which ZIMPERIUM is pioneering.

It's not only about protecting organizations from potential threats being introduced by BYOD - which we like to call "Bring Your Own Threat", ZIMPERIUM Mobile Intrusion Prevention System, zIPS, utilizes Machine Learning algorithms to turn BYOD devices into sensors which detect attacks inside and outside of the organization. The result being every smart-device in the organization is capable of being turned into a powerful Mobile Intrusion Prevention System ecosystem.

You may download zANTI from our website to evaluate certain network attacks.

You can contact us for more information about a number of benchmarks, tests and tools you can use to evaluate existing solutions.

CONTACT US

101 Mission Street
San Francisco, CA 94105
Main: 415.992.8922 | Toll Free: 844.601.6760
sales@zimperium.com
www.zimperium.com