Overview of Mobile Cybersecurity Technologies

Presented by: WTI
www.wti-solutions.com
703.286.2416

LEGAL DISCLAIMER

WTI's informational publications are made available for educational purposes only as well as to give you general information and a general understanding of technology, not to provide technical advice. By reading our informational publications you understand that there is no contractual relationship created between you and WTI. Although the information in our informational publications is intended to be current and accurate, the information presented herein may not reflect the most current technical developments. These materials may be changed, improved, or updated without notice. WTI is not responsible for any errors or omissions in the content of this publication or for damages arising from the use or performance of this publication under any circumstances. We encourage you to contact us or other technology companies for specific technical advice as to your particular matter.

What is Mobile Cybersecurity?

Mobile devices have become the preferred targets of cyberattacks.

Mobile devices have become popular repositories for sensitive information due to a growing user base conducting both work and personal business and as a result are particularly desirable targets for attackers.[1]

- **Cybersecurity** is commonly defined as the ability to protect or defend the use of cyberspace from cyber-attacks [2] as well as the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. [3]

- **Mobile Device** traditionally refers to portable computing and communications devices with information storage capability, to include notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices.[4]

- **Mobile Cybersecurity,** also coined by industry as "mobile threat defense," [5] refers specifically to the detection and mitigation of attacks on mobile computing devices.

[1] Furnell, S. (2009). *Mobile security*. Ely, U.K: IT Governance Pub.
[2] *Glossary of Key Information Security Terms,* NIST IR 7298 Revision , Richard L. Kissel, June 5, 2013 The National Institute of Standards and Technology (NIST)
[3] TechTarget Network WhatIs.com® , retrieved from http://whatis.techtarget.com/definition/cybersecurity
[4] *Security and Privacy Controls for Federal Information Systems and Organizations*, National Institute of Standards and Technology, NIST Special Publication (SP) 800-53 Revision 4, April, 30, 2013 retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[5] "Mobile Security Turns Into Big Business for Cyber Firms", Fortune Magazine, Jeff John Roberts, January 6, 2017, retrieved from http://fortune.com/2017/01/06/mobile-cyber-security/

Why is Mobile Cybersecurity Critical?

Mobile Cybersecurity poses a unique challenge for both Government and Industry:

Government Perspective "Threats to the Government's use of mobile devices are real and exist across all elements of the mobile ecosystem. The enhanced capabilities that mobile devices provide, the ubiquity and diversity of mobile applications, and the typical use of the devices outside …. traditional network boundaries requires a security approach that differs substantially from the protections developed for desktop workstation"[6]

- Conclusions of "Study on Mobile Device Security", presented to Congress as a joint effort of the Department of Homeland Security in consultation with the National Institute of Standards and Technology via the National Cybersecurity Center of Excellence

Industry Perspective "The cyberthreat landscape changes literally by the hour and requires constant vigilance and innovation throughout the entire U.S. mobile industry …. It is a constant risk to be managed, where opposing forces must constantly adapt their strategies and tactics to keep the advantage. Today's mobile cybersecurity protections must be flexible and adaptable in the face of increasingly sophisticated and persistent global threats."[7]

- Conclusions of Today's Mobile Cybersecurity presented by CTIA-The Wireless Association®

[6] *Study on Mobile Device Cybersecurity,* prepared by the Department of Homeland Security (DHS) in consultation with the National Institute of Standards and Technology, April 2017, retrieved from https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf

[7] *Today's Mobile Cybersecurity*, page 3, prepared by CTIA-The Wireless Association® , retrieved from http://files.ctia.org/pdf/CTIA_TodaysMobileCybersecurity.pdf

What Makes Mobile Devices Preferred Cyberattack Targets?

Mobile devices have inherent weaknesses making them more vulnerable to attacks.

- Mobile technology features to include Short Message Service (SMS, aka text messaging), Multimedia Messaging Service (MMS), Wi-Fi, Bluetooth and the Global System for Mobile Communication (GSM) are vulnerable because they have limited security functions to protect them.[8] SMS is vulnerable to spoofing, MMS to embedded code, Wi-Fi to poor security setup, Bluetooth to handshake exploits, and GSM to overflow attacks.
- Technical security measures (firewalls, antivirus, and encryption) are uncommon on mobile devices.[9]
- Mobile operating systems are not updated as frequently as those on personal computers.[9]
- Mobile device portability makes them easy to steal with all stored data; an attacker can defeat most security features and gain access to any information they store.[9]
- Many seemingly legitimate software applications are malicious; anyone can develop apps for the most popular mobile operating systems and mobile service providers offer third-party apps with little or no safety evaluation.[9]
- Legitimate smartphone software can be easily exploited.[9]
- Phishing attacks use electronic communications to trick users into installing malicious software or giving away sensitive information.[9]

[8] Furnell, S. (2009). *Mobile security*. Ely, U.K: IT Governance Pub

[9] "Cyber Threats to Mobile Phones", page 2, Paul Ruggiero and Jon Foote, United States Computer Emergency Readiness Team, retrieved from https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf

Is Mobile Cyber Threat Increasing?

Mobile cyber threat is on the rise.

- A 2017 Avast analysis on over 160 million mobile devices concluded that mobile cybercrime is on the rise with an increase of 40% in mobile cyberattacks.[10]
- CSO, which provides news, analysis and research on security and risk management, reports that mobile devices are coming under increasing attack, with MacAfee reporting 16 million mobile malware incidents in 2017 (almost nonexistent a decade ago).[11]
- A Dimensional Research report on the growing threat of mobile device security breaches conducted a global survey of security professionals and concluded that "mobile devices are now considered by threat actors to be one of the weakest links in the infrastructure of most enterprises" with 20 percent of the companies reporting their mobile devices breached via a broad range of attacks with little means to prevent or defend due to "the constant evolution of threats and the relentless barrage from hackers."[12]

[10] "New Research Reveals Increased Mobile Threats", Jennifer Bennet, September 7, 2017, retrieved from https://blog.avast.com/mobile-users-at-risk-to-increasing-threats

[11] "Five new threats to your mobile security, Stacy Collett, August 1, 2017, CSO Magazine, retrieved from https://www.csoonline.com/article/2157785/data-protection/five-new-threats-to-your-mobile-security.html

[12] "The Growing Threat of Mobile Device Security Breaches – A Global Survey of Security Professionals", April, 2017, Dimensional Research, retrieved from https://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf

What are the Newest Threats to Mobile Security?

- A 2014 report by Kaspersky Lab identified mobile device security threats on the rise due to unintentional data leakage from mobile apps, unsecured Wi-Fi, network spoofing with fake access points, phishing attacks with legitimate-seeming emails, spyware, broken cryptography caused by weak encryption algorithms or improper implementation with "back door" entry, and vulnerability in use of tokens that enable users to perform multiple actions without re-authenticating their identity.[13]
- An August 2017 CSO report identified five new threats – including enterprise-class spyware, mobile botnets, ad and click fraud, Internet of Things (IoT) malware, and "dead" (obsolete and unsupported) apps that are not deleted by users.[14]
- An April 2017 Dimensional Research report on the growing threat of mobile device security breaches conducted a global survey of security professionals and reported a broad and evolving range of attacks to include malware, SMS phishing, networks attacks via malicious Wi-Fi, interceptions in calls or texts messages over mobile carrier's network and key logging or credential theft.[15]

[13] "Top 7 Mobile Security Threats: Smart Phones, Tablets, & Mobile Internet Devices – What the Future has in Store" retrieved from https://usa.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store

[14] "Five new threats to your mobile security, Stacy Collett, August 1, 2017, CSO Magazine, retrieved from https://www.csoonline.com/article/2157785/data-protection/five-new-threats-to-your-mobile-security.html

[15] The Growing Threat of Mobile Device Security Breaches – A Global Survey of Security Professionals", April, 2017, Dimensional Research, retrieved from https://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf

Mobile Cybersecurity in the News – iPhone 7

REMOTE WI-FI ATTACK BACKDOORS IPHONE 7 [16]

- **The Threat** - Disclosed by Google's Project Zero, the exploit enables a background code execution that allows for a persistent presence on the device to monitor and change commands.
- **How it Works** - A backdoor is inserted into the firmware, allowing remote read/write commands to be issued to the firmware via crafted action frames (thus allowing easy remote control over the Wi-Fi chip).
- **The Solution -** The vulnerability should be patched by iOS 11 update.

[16] Mimoso, Michael, (September 27, 2017) "Remote Wi-Fi Attach Backdoors iPhone 7", Threatpost, retrieved from https://threatpost.com/remote-wi-fi-attack-backdoors-iphone-7/128163/

Mobile Cybersecurity in the News – MS Office

ATTACKERS USE UNDOCUMENTED MS OFFICE FEATURE TO LEAK SYSTEM PROFILE DATA [17]

The Threat - An undocumented Microsoft Office feature in both iOS and Android versions allows adversaries to gain system profiles for further attacks by getting recipients to open a Word document with embedded commands within it.

How it Works - The malicious Word document then uses Object Linking and Embedding (OLE2) - normally used to point to online graphics - to instead execute several URLs from third party websites, which then execute a number of testing attacks, giving attackers sensitive system information to use in follow-up attacks.

The Solution - No patch is available yet.

[17] Spring, Tom. (September 17, 2017). "Attackers Use Undocumented MS Office Feature to Leak System Profile Data", Threatpost; retrieved from: https://threatpost.com/attackers-use-undocumented-ms-office-feature-to-leak-system-profile-data/128011/

Mobile Cybersecurity in the News – Bluetooth

WIRELESS 'BLUEBORNE' ATTACKS TARGET BILLIONS OF BLUETOOTH DEVICES [18]

The Threat - Researchers at security firm Armis announced they had found an attack vector, dubbed "BlueBorne" that can jump from one compromised Bluetooth device to comprise another wirelessly. The firm estimates that 5.3 billion devices are at risk.

How It Works - Since Bluetooth can used for remote control of devices, any vulnerability that allows an external user to take control gives them access to most system functions.

The Solution - Apple iOS devices running (10.x or newer) are safe. Only 45% of Android phones are patchable, leaving 1.1 billion active Android devices older than Marshmallow (6.x) vulnerable.

[18] Spring, Tom. (September 17, 2017). "Wireless 'BlueBorne' Attacks Target Billions of Bluetooth Devices", Threatpost, . retrieved from: https://threatpost.com/wireless-blueborne-attacks-target-billions-of-bluetooth-devices/127921/

Why does Mobile Cybersecurity matter to Government?

In May 2017, the Department of Homeland Security released to Congress a report, "Study on Mobile Device Security" with the following key threat points: [19]

- Threats to the Federal government's use of mobile devices exist across all elements of the mobile ecosystem.
- Mobility threats require substantially different protections than those developed for desktop workstations because mobile devices are exposed to a distinct set of threats, frequently operate outside of enterprise protections and have evolved independently of desktop architectures.
- Threats to mobile devices range from those perpetrated by nation-states, organized crime or hackers, to loss or theft of mobile phones.
- Federal government mobile device users may be targeted with additional threats simply because they are public-sector employees.

[19] News Release: DHS Delivers Study on Government Mobile Device Security to Congress. (May 04, 2017). Pages i,10,77. retrieved from: https://www.dhs.gov/science-and-technology/news/2017/05/04/news-release-dhs-delivers-study-government-mobile-device

What are the Latest Advances in Mobile Cybersecurity?

- CTIA - The Wireless Association ®, a nonprofit comprised of wireless industry stakeholders, reports ongoing efforts to counter emerging cyber threats to include "root of trust" enhancements to authenticate and authorize users, user credential protections, enhanced security features with tiered approaches/multiple layers, timely/automated software update distributions, technology based protections to address multiple air-interfaces (aka unsecured network connections, unencrypted Wi-Fi), and protections for machine-to-machine and near-field communication zones in a mobile environment.[20]

- The National Institute of Standards and Technology "National Cybersecurity Center of Excellence", a partnership between industry, government agencies, and academic institutions focused on cybersecurity, has ongoing mobile device security initiatives related to securing sensitive enterprise data accessed by and/or stored on mobile devices; reference mobile architectures that can be adapted to design, deploy and build in security for organizational mobility programs, and maintains a mobile threat catalogue to identify and mitigate threats to mobile devices.[21]

[20] *Today's Mobile Cybersecurity* – Industry Megatrends & Consumers, pages 22-23 prepared by CTIA-The Wireless Association® , retrieved from http://files.ctia.org/pdf/CTIA_IndustryMegatrends_Consumers.pdf

[21] Mobile Device Security, retrieved from https://nccoe.nist.gov/projects/building-blocks/mobile-device-security

Contact Information

WTI is a CMMI ® Level 3 appraised and SBA 8(a) Certified, Economically Disadvantaged Woman-Owned Small Business based in the National Capital Region, committed to helping the government and industry harness the power of actionable information through intelligence and IT solutions.

WTI's work in mobility spans multiple Federal Government executive departments and a number of independent Federal agencies. WTI has earned exceptional Government Contractor Performance Assessment Reports (CPAR ratings) and numerous awards and commendations for our mobile development work.

To find out more, contact: info@wti-solutions.com.