Tutorial T-20: Android Security

Presenter: Thomas Chen (City University London, UK), Jorge Blasco (City University London, UK)

Tutorial Overview

Android is the most prevalent operating system in smart phones today. Anticipating that smart phones would be popular targets for criminals, Android was designed with numerous security features built on top of the Linux kernel, which provides a solid security foundation. On the other hand, the openness of Android (in terms of installable apps) exposes smart phones to threats such as malware, which has been growing quickly every year. Despite the efforts of Google and antivirus companies, mobile malware - which almost exclusively targets Android - is not only growing in numbers but also in complexity. During the last year, the total number of malware samples collected by McAfee grew by 167%, reaching the 200 million barrier of accounted malware samples. Attackers have also innovated in the way they infect new devices, using third party developer stolen keys to sign malware samples and taking advantage of zero days exploits to get root access to the device.

This tutorial provides an essential overview of the Android security architecture that many users may find helpful to understand the strengths and limitations of security protections in their phones. The tutorial will also be useful to researchers to learn about open research issues in the field of smart phone security. The expected audience will have a background of computer science with desirable previous experience in information security or software development. The tutorial includes an overview of the Android OS. The audience is not required to have any previous experience in Android app development or mobile malware. The tutorial outline is as follows:

1. Introduction
2. Android software architecture
    - 2.1. OS and layers
    - 2.2. Apps
    - 2.3. Components
    - 2.4. IPC and intents
3. Android App Distribution
    - 3.1. App development
    - 3.2. App markets
4. Overview of Android Security Architecture
    - 4.1. Access control
    - 4.2. Linux
    - 4.3. Android security approach
5. Linux Kernel Security
    - 5.1. Permissions
    - 5.2. Process isolation
    - 5.3. Secure IPC
6. Android Security Specifics
    - 6.1. Filesystem
    - 6.2. Memory management
    - 6.3. App signing
    - 6.4. Sandboxing
    - 6.5. Securing IPC
    - 6.6. Permissions
7. Malware

7.1. Malware threats
7.2. Static detection methods
7.3. Dynamic detection methods
7.4. Hybrid methods
7.5. Local vs Remote detection
8. Conclusions and Open Research Issues
9. References

Presenter Biographies

Thomas Chen is a Professor in Cyber Security at City University London since 2013. From 2008 to 2013, he was Professor in Networking at Swansea University, Wales. From 1997 to 2008, he was an Associate Professor in the Department of Electrical Engineering at Southern Methodist University in Dallas, Texas. Previously, he worked on ATM research at GTE Laboratories (now Verizon), Waltham, Massachusetts. He received the BS and MS degrees in electrical engineering from the Massachusetts Institute of Technology in 1984, and the PhD in electrical engineering from the University of California, Berkeley, in 1990. He was former editor-in-chief of IEEE Communications Magazine (2006-2007), former editor-in-chief of IEEE Network (2009-2011), and founding editor-in-chief of IEEE Communications Surveys. He serves as an editor for Journal of Security and Communication Networks and International Journal of Digital Crime and Forensics. He is the co-author of ATM Switching Systems (1995) and Forward Error Correction Based on Algebraic-Geometric Theory (2014), and co-editor of Broadband Mobile Multimedia: Techniques and Applications (2008), Mathematical Foundations for Signal Processing, Communications, and Networking (2012), and Cyber Terrorism (2014). He received the IEEE Communications Society's Fred Ellersick best paper award in 1996.

Jorge Blasco is a Research Fellow at City University London. He is now actively working in a research project related to smart phone security and emerging mobile malware threats. The project is funded by the EPSRC and includes Coventry and Swansea Universities and McAfee as partners. He was formerly an assistant lecturer at University Carlos III of Madrid, where he obtained his PhD in 2012 with a dissertation in the field of information security and insider threats. His main research interests are smart phone security and cyber security. He has authored several research papers on mobile malware detection, cyber security situational awareness and information security event correlation. He is an active Android and iOS app developer with several apps being available in both OS official markets. He has collaborated with Telefonica in a project to apply artificial intelligence techniques for intrusion detection and event correlation.