



openHPI – Internet Security Course Update: Current Security Topics

Prof. Dr. Christoph Meinel
Hasso Plattner Institute, Potsdam, Germany

Overview

In this video, we want to address some of the topics that have become particularly explosive during the course ...

- **Privacy:**

- ☐ Facebook and Cambridge Analytica

- **Botnets:**

- ☐ GitHub DDoS Attack

- **Ransomware**

- **Mobile Security**

- ☐ Stagefright vulnerabilities are still an issue

- **Hardware security**

- ☐ Do not relax even though Meltdown and Spectre CPU vulnerabilities are patched

Facebook and Cambridge Analytica

2015: Dr. Alexander Kogan proposes a Facebook App for Personality Prediction “thisisyourdigitallife” for psychology research

- ~270.000 user, **gave consent** for access of, e.g., their city, content they liked, or **friends’ information**
- ➔ **Data of friends** was also collected if their privacy settings allowed it, overall data collected of **around 50 million** users
- Although only allowed for research, data was passed from Kogan to 3rd party companies like **Cambridge Analytica**
 - **Cambridge Analytica** (mis-)uses data for political and governmental analytics all over the world

Remember: Come to informed decisions about what data you put on social networks and carefully manage your privacy settings

GitHub DDoS Attack 1/3: DDoS, IP Spoofing and Amplification Attacks

Reminder: Distributed Denial of Service attacks

- A variety of attack sources are synchronized to run a **Denial Of Service** attack on a specific service
- Goal: Termination of the functionality of the service

IP Address Spoofing:

- An attacker posing as a trusted sender generates and sends data packets with a faked IP sender address to his/her victim

Amplification Attacks:

- Goal: Power of any attack is increased with low effort
- Usually via exploitation of specific vulnerabilities or properties of protocols or software to increase impact of attack

GitHub DDoS Attack 2/3: Memcached, UDP

Memcached: open source software for faster access to data that is frequently used, e.g. website data

- Usually behind firewalls, **not** reachable via public Internet

UDP: Lightweight, connectionless protocol

- No sender-receiver handshake in the beginning
- Provides no guarantee that data is delivered

Amplification Attack:

- The attacker finds publicly reachable Memcached instances (often due to misconfiguration of instance)
- Attacker requests **large** content with a **small** UDP package
 - Attacker forges client IP address of request with target IP of **victim** and server will send response to **victim** IP
- → Memcached replies **large** content to **victim** IP

Github DDos Attack 3/3: Attack Details

GitHub: World's largest community of developers with over 80 million repositories with (open) source code of software

On February 28, 2018 **GitHub** was unavailable for some minutes

Attack:

- **DDoS attack** from over 10.000 unique endpoints worldwide
- Attackers used amplification attack via publicly reachable memcached instances
 - Amplification factor of up to **51.000!**
 - **1 Byte** sent by attacker = **51KB** sent to sender
 - At maximum, **1.35TBps / 126.9 million packets per second** were sent to GitHub

Mitigation:

- Routing to GitHub changed to identify and block attackers

Ransomware - Effective Protection

Preventing infection

- Always be careful with email attachments
- Keep systems updated to prevent infection while surfing
- Use current antivirus software (does not always help!)

Regular data backup

- If the infection is successful, the system must be reinstalled completely
- Regular backups protect against data loss
- Backup should be done on external medium
 - Connect the USB hard disk only for backup, then disconnect
 - use special software when backing up network shares, do not permanently embed share as network drive

Ransomware – To Pay or Not To Pay?

There is no comprehensive answer to this question as so many aspects must be considered case-by-case

- German government cybersecurity agency BSI generally advises against payment
 - Payment supports criminal business model
 - Data is not always decrypted despite payment
 - Instead: Take screenshots and report incident to police
 - Store any encrypted data for later decryption attempts
- Cases are also known where the data has been decrypted after payment
 - A Los Angeles hospital paid \$ 17,000 US for decryption of patient records
 - Where the value of the decrypted data exceeds extorted amount, payment then makes economic sense

Mobile Security: Vulnerabilities

Smartphones and their operating systems, just like "normal" computers, have specific vulnerabilities

- Modern smartphones are computers with a specially adapted operating system and specific applications:
 - Android: Based on GNU/Linux
 - iOS: Uses common core with Mac OS X from Apple
- Linux and OS X vulnerabilities can thus also affect other smartphone versions ...

Mobile Security:

Spectacular Vulnerability Stagefright

Reminder: Stagefright is a library for viewing and processing multimedia (video and audio) on Android systems

- Vulnerability in Stagefright library was announced on July 27, 2015:
 - applies to ~ **1** billion Android phones (Versions 2.2 - 5.1)
 - exploit can be installed in any multimedia file, for example:
 - mobile phone receives an MMS (default settings allow automatic downloading of MMS)
 - exploit is executed, attacker gets full control of the cell phone and deletes the MMS message
 - switching off MMS reception does not work as Exploit can also be run with **any other** applications that work with multimedia: browser, email, Facebook app, etc.

Mobile Security:

Stagefright Update Timeline

Original bug fixes by July 2015

- **But:** But updates themselves were flawed, so there was a new update in August 2015
- In October 2015 Stagefright 2.0 was released
- In the following years (2016 – 2018), many more critical Android vulnerabilities were detected in the Stagefright library (concerning all modern Android versions)

➔ **Stagefright vulnerabilities have been around for many years and still pose a persistent problem**

Basically, install latest updates as soon as they are available

But for many older smartphones with an adapted Android variant, new updates are often not applicable

- Switch off automatic MMS reception in the messaging application settings
- Do not use applications on Android mobiles/ tablets (except recent version of Firefox) if no current update has been installed
 - remove applications like email, Twitter, Facebook, etc., which can process multimedia data from the Internet - or refrain from using it
- If you can not do without these applications, buy a new smartphone or switch to updated version of LineageOS (not for all devices available, change at your own risk!)

Hardware Security: Background

Background: An Operating System manages computer hardware (CPU, memory) and controls applications, however, at the end, the program code together with other programs is executed on the hardware

- **Low-level access to the hardware allows an attacker to ignore all security mechanisms on the OS level**
- Intel and AMD CPUs have an autonomous computer inside, which runs even when main computer is turned off
 - Intel Management Engine could be used for remote management of the PC
 - A portion of network traffic goes to Intel ME before the main operating system
- Hardware vulnerabilities can be exploited to get such low-level access

Hardware Security: CPU vulnerabilities

January 2018: The hardware vulnerabilities Meltdown and Spectre in branch prediction mechanism (used for higher CPU performance) got a lot of attention in the media

→ **Already discussed in Excursion 2 of Week 6**

Some other CPU vulnerabilities were not so much discussed:

- May 2017: Vulnerability in Intel Active Management Technology (based on the Intel Management Engine) allows a network attacker to get full control over the computer
 - since 2011 it affects many computers with Intel CPUs
- November 2017: Two more vulnerabilities published
- March 2018: Vulnerabilities published for AMD Platform Secure Processor (analog of Intel ME)

Hardware Security:

Measures Against CPU vulnerabilities

Stay updated

- However, updating operating system and software seems to be not enough anymore
 - regularly checking news and advisories on your hardware (not only including CPU) is recommended
 - in case of Intel Active Management, Intel offers a tool to check for the vulnerability:

<https://downloadcenter.intel.com/download/27150>
 - motherboard manufacturers are responsible for providing updates

For some Intel CPUs, a number of tools (me cleaner) or instructions are available to remove/disable/damage Intel ME

- Removal can be technically very complicated and/or can damage your PC!