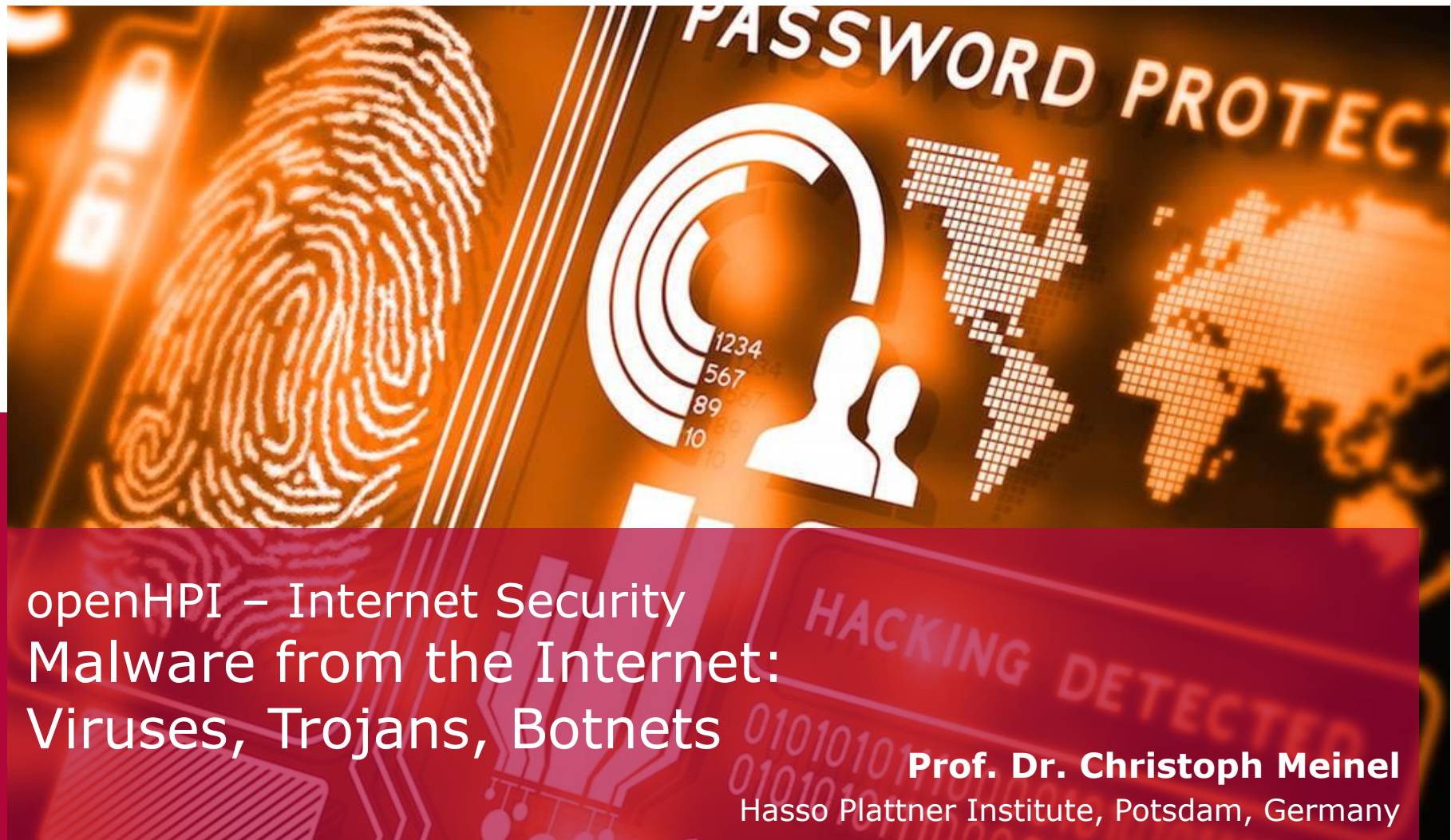




openHPI – Internet Security Malware from the Internet: Viruses, Trojans, Botnets

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

Malware - Malicious Software

Malware - Malicious Software – name for software usually smuggled by hackers onto an unsuspecting user's device via the Internet to enable cyberattacks

Well-known examples of Malware are:

- ❑ Viruses
- ❑ Worms
- ❑ Trojans
- ❑ Botnets
- ❑ Rootkits
- ❑ Adware
- ❑ Spyware
- ❑ ...

Malware: Viruses

Viruses are harmful mini-programs that integrate themselves into existing programs ("host program")

- Falsify or change host program
- Integration sometimes even takes place without changing the size or the last modification date of the host program
- Multiply themselves locally using the host program
 - Reproduction has a particular effect on the performance of the infected system
- Can affect the workability of the system (computer, laptop, smartphone, ...)

Malware: Worms

Worms are malicious programs, which spread themselves independently over the network or via removable media (e.g. USB sticks)

- Can start themselves after further transmission
 - User does not have to expressly agree to execution
 - Often spread faster than viruses
- Work independently, do not need a host program
- Following execution, payload often has devastating effect on the affected system:
 - Impairment of performance,
 - Post-installation of other malware,
 - Opening of backdoors,
 - Infected computer becomes bot in a botnet,
 - ...

Malware: Trojan or Trojan Horse

The term “**trojan**” refers to computer programs with hidden malicious functions masked as useful applications

- When the supposedly benign application is started, the malicious function is automatically executed
 - partly parallel to expected functionality, to remain unnoticed
- Trojans can also camouflage themselves as documents or files
 - Malicious function is executed when the document / file is opened
- **Example:** Fake Facebook app for Android phone to access username / password combination

Malware: Keylogger

A **keylogger** is a mini-program that records all the user's keystrokes

- More powerful variants also capture the contents of the screen
- Recording of the keystrokes is carried out when, for example, a password input field appears on the screen
- The recorded user inputs are then stored in a file accessible to the attacker or sent to the attacker
- An attacker uses these information for
 - identity theft,
 - bank transfers,
 - ...

Malware: Botnets

A **botnet** is a combination of numerous different computer **bots** - typically created without the knowledge of the computer owner

- Central "Command and Control Server" - **C&C Server** - in the hands of an attacker manages, coordinates, and controls the (numerous) bots from a distance
- C&C Server takes control over the bots and sends handling instructions to the bots, which then execute them autonomously, e.g. to start a DoS attack ...
- Botnets with many remote-controlled bots can perform a variety of dangerous attacks with very high computational power ... -> *Stand-alone clip for botnets*

Malware: Rootkit and Backdoor

A **rootkit** is malicious software that allows the attacker continuous access to a compromised system

- Usually installed when a system is breached
- Attempts to conceal its own existence on the system
 - Open connection or certain files are masked
 - Further malicious programs are hidden from user / antivirus

A **backdoor** allows an attacker to gain unauthorized access to a third-party computer

- It is very attractive to cybercriminals to have hidden access to a system

Malware: Adware

Adware is a program that displays advertising in addition to the actual functionality

- Adware can also be integrated into the web browser, which makes it possible to display advertisements on every website
- Malicious software that uses advertising is also referred to as adware, e.g.
 - Browser plugins that embed JavaScript with ads on each page

Malware: Spyware

Spyware is software that sends sensitive data to third parties without the consent of the owner, e.g.

- Software manufacturers, web service providers, government agencies, foreign intelligence services, ...
- Spyware is also referred to as spy software, snooping software, spy programs...
- Data transmission takes place in secret
- Often used to display personalized advertising and follow surfing behavior
- But also used for information retrieval of personal data, e.g.
 - Passwords,
 - Credit card data,
 - ...

Malware: Scareware

Scareware attempts to frighten users by faking error messages, virus infections or other problems

- Often, particularly current or prominent virus and error messages are used to make the threat as dramatic as possible
- Then penalties or repair costs are demanded
- Common approach:
 - Listing legal infringements on the user in the name of the police
 - Demands for a penalty
 - ...



www.webroot.com

Malware: Rogueware / Rogue Antivirus

Rogueware is a stand-alone program that fakes a trustworthy source to get sensitive information or money

- Preventing the cleaning of the computer while introducing malicious programs or stealing data

Rogue Antivirus is a special type of rogueware that camouflages itself as an antivirus program

- "Scans" computers and "finds" various malicious software
- No real scan is performed, but "infections" are reported (even on a fault-free system)
- Users are then prompted to perform a cost-based repair

Malware: Ransomware

Ransomware is a malicious program that prevents the user from accessing his data and extorts money

- Encryption of personal data so that the victim can no longer view and use his / her own data
- Then the victim is offered a decryption of the data at a cost
- BSI advises against payment, since often further requests follow or data is not decrypted despite payment
- Infection is carried out via e-mail attachments, trojans, ...

Prevention:

- Regular back-up of all important data and prevention of initial access to the computer

Malware Today

Nowadays, generally, malicious software (malware) can **no longer** be assigned **explicitly** to one of the named types

- Usually, various malicious functions are used within a malware and in some cases additional components can be uploaded
- **Example:** The well-known **carberp** malware contains various functions of a
 - Trojan
 - Keylogger
 - Rootkit
 - Backdoor
 - ...