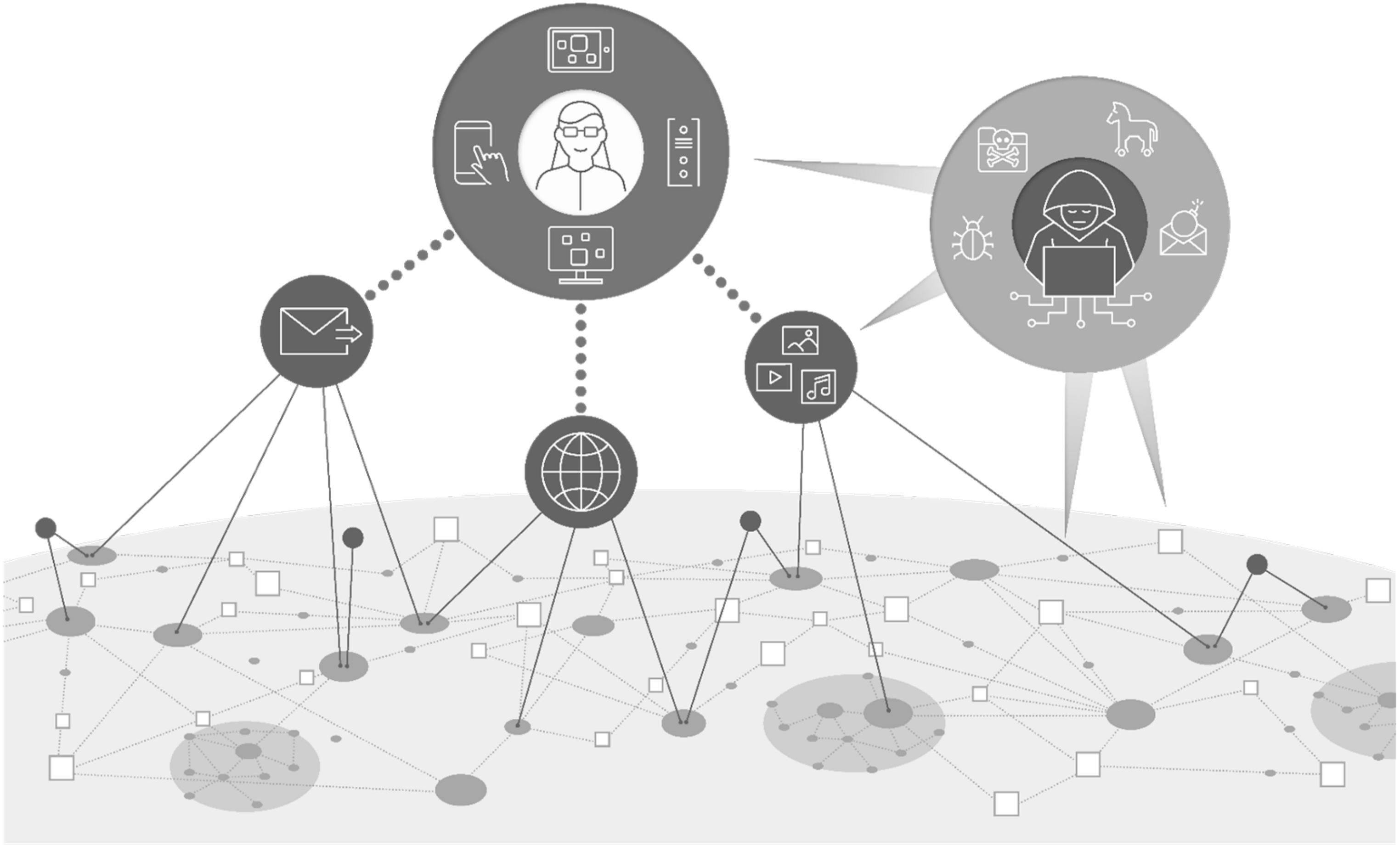
openHPI Course: Cyberthreats by Malware

Attackers and their Motivation

Prof. Dr. Christoph Meinel

Hasso Plattner Institute
University of Potsdam, Germany

Attackers on the Internet and Their Goals



Potential Attackers on the Internet: **Insiders**

Company's own employees could attack or steal company's resources, e.g., confidential document, or servers, misusing their privileges in the company

Motives: curiosity, frustration, revenge, greed, envy, ...

- Insider attacks are particularly dangerous since they are come from inside the company's network – **intranet** (internal company Internet)
- Naivety or carelessness → **social hacking**
- Increased risk due to (faulty) **integration of home offices** and **"Bring Your Own Device (BYOD)"** into the corporate network
- Non-compliance with internal security instructions open doors for attackers

Potential Attackers on the Internet: **Script Kiddies**

Attackers without deep cybersecurity knowledge who launch cyberattacks using hacker tools

Motives: curiosity, just for fun, show-off, ...

- Indiscriminate and usually without direct criminal intent
- Mostly young people (pupils, students) starting to learn about cybersecurity
- Many hacking tools are available for download on the Internet
- Especially dangerous: **Denial-of-Service-Attacks** (**DoS**)

Potential Attackers on the Internet: **Hacker**

The term hacker has different interpretations

- The term "**hacker**" was originally used in recognition of particularly creative and talented individuals
- Later hacker has **negative connotation** by the media due to the indiscretions and damages by their cyberattacks
- Mostly referring to people with in-depth technical knowledge
- The “hacker‟ term could be categorized as follows:
  - white hat hacker
  - grey Hat hacker
  - black hat hacker
  - hacktivists

Potential Attackers on the Internet: **White Hat Hacker**

The "good" hackers / ethical hackers

Professional experts who look for security vulnerabilities in computer systems, applications, services, networks, … to help secure the system from future possible attacks

Motives: good samaritan, increase cybersecurity awareness

- Perform **security analysis** and **penetration tests** to detect security gaps in the systems
- Inform authorized owner about discovered security gaps to help to improve the security of computer systems
- Prevent future attacks on the systems by cybercriminals

Potential Attackers on the Internet: **Black Hat Hacker** (1/2)

The "evil" hackers / cybercriminals

Mostly professional computer experts who hack the computer systems to do criminal activities out of self-interest and greed for profit

Motives: money, power, blackmail, notoriety, ...

- Exploit discovered security gaps to gain authorized access to computer systems
- Aim is to launch crimes, such as data theft, identity theft, service destruction, …
- For own benefits or on behalf of others
- In most cases, discovered security gaps are kept secret and shared with other **black hat hackers**, e.g. in the Darknet, to exploit other computer systems

Potential Attackers on the Internet: **Black Hat Hacker** (2/2)

Black hat hackers could sell the **stolen information** to the public (usually in Darknet), for example:

- Email accounts: $0.70 - $2.30
- Driving license information: $20
- Credit card details: $8,00 - $22,00
- Medical records: Up to $1000

They also provide **services and tools** for various illegal activities, such as:

- Tool to hack Facebook accounts: $19.99 (3 months)
- Ratings on Google and co.: $3 - $350
- Access to special user accounts: $90 - $350

Source: https://www.keepersecurity.com/how-much-is-my-information-worth-to-hacker-dark-web.html, https://www.businessinsider.com/9-things-you-can-hire-a-hacker-to-do-and-how-much-it-will-generally-cost-2015-5?r=DE&IR=T

Potential Attackers on the Internet: **Grey Hat Hacker**

Intermediate group of benign and malicious hackers

Mostly professional computer experts who have both benign and malicious / selfish goals

- Exploit found security gaps in computer systems
- Possibly launch criminal activities **for their own profit**
- Publish found security gaps to increase security awareness

Potential Attackers on the Internet: **Hacktivist**

Hacker + activists

Individuals or groups who hack computer systems for ideological, social, political, or religious reasons

Motives: raise awareness, self ego, political goals, …

- Launch attacks to computer systems to highlight issues to the public
- Believe they contribute to higher cause
- Do not shy away from criminal activities
- May influence the media and public opinion with false reports and confusing ideological phrases

Known group, e.g. **Anonymus**

Potential Attackers on the Internet: **“Common" Criminals**

Criminals who use the Internet for their activities

Traditional criminals and organized crime have recognized the potential of the Internet as global marketplace for their criminal activities

- Use the Internet for criminal activities, e.g. drugs and arms trafficking, extortion, computer fraud, ...
- Authorities could have more difficulties to enforce the law and investigate the criminal activities on the Internet than in the physical world
  - □ **therefore**: governments might be interested to install "backdoors" in cryptographically protected systems

Potential Attackers on the Internet: **Secret Services & Espionage**

Extensive possibilities of the Internet offer high potentials for spies and secret services

- Economic crime: stealing confidential information and spying on competitors
- Espionage: spying on politically interesting actors in other countries
- Politically or economically motivated cyber attacks on services and computer systems

Example: Stuxnet

- Malware attacking Windows networks and proprietary programmable systems of nuclear plants with the aim of destroying Iranian uranium enrichment plants
- Exploits used multiple (!) zero-day vulnerabilities