openHPI Course: Digital Identities – Who am I on the Internet?

Identity Theft – Attacks on Digital Identities

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

Identity Theft (1/2)

We can use an Internet service and it resources by means of our digital identity

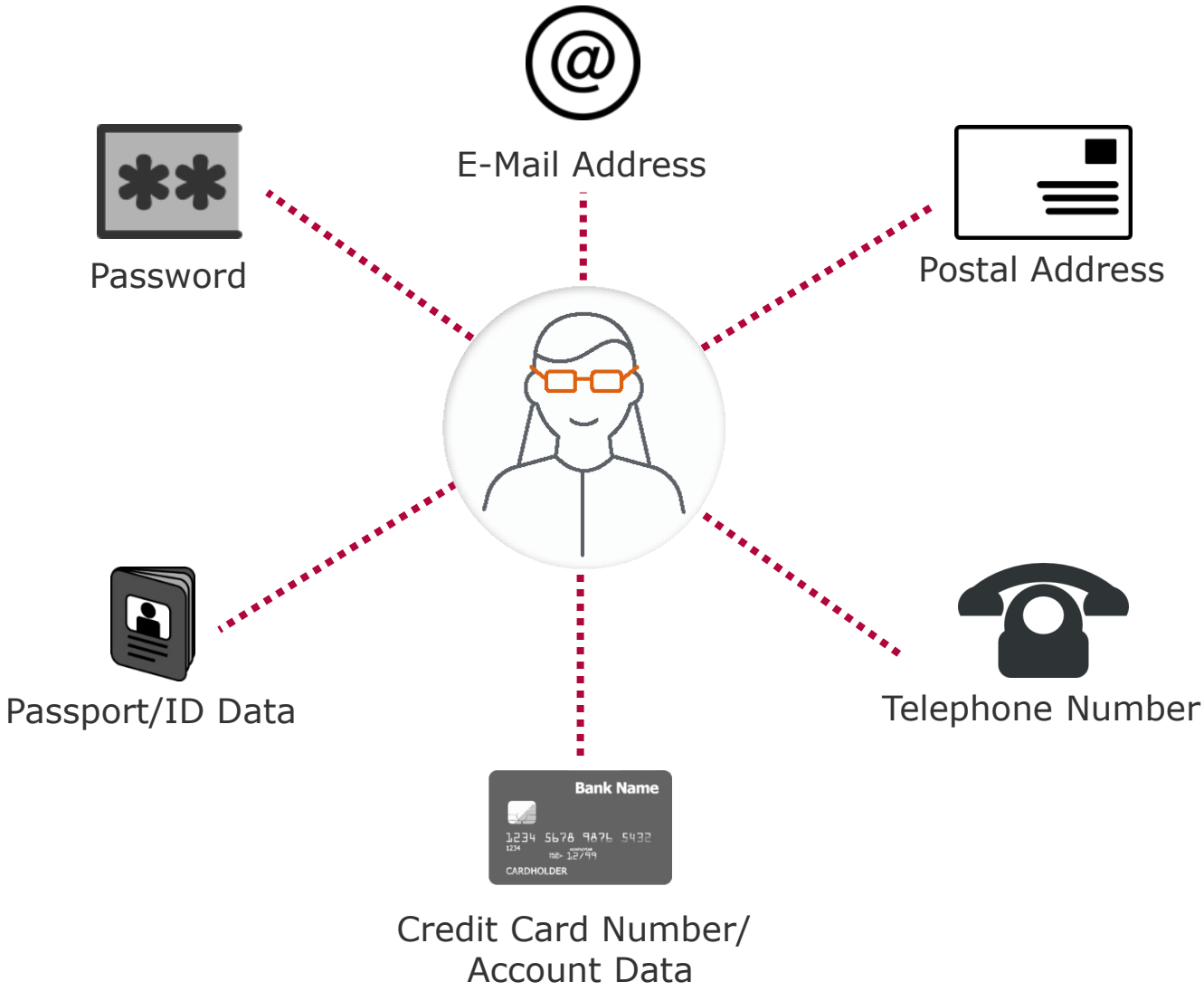
- If we are authenticated, i.e. if the service (or its ID provider) is convinced that a digital identity belongs to us we can use the service
- However, if a third party comes into possession of a user's digital identity, it can use all services and resources in the user's name for which the user is authorized, e.g.
  - online shopping
  - make bank transfers
  - watch videos
  - …
- Unlike physical identities, it is relatively easy to **steal** and **abuse** stolen digital identities

Identity Theft (2/2)

Due to the **high potential for abuse**, identity theft is **very attractive to cybercriminals**:

- With stolen digital identity, the cybercriminal get all rights – **authorization** – of the rightful owner
- Since Internet services authorize on the basis of digital identity alone, thieves can use the services at the expense of the rightful owner

Target: Identity Data



Origin of Stolen Identity Data (1/3)

- Theft of **account/customer databases** of Internet services
  - cybercriminals gain access to the system of an online service provider and copy the database from the provider's authentication system with all identity data
  - often executed by so-called "SQL injection"
- Data theft via **malware**, e.g.
  - "**Spyware**" collects data directly from the user's computer – of particular interest are identity data
  - "**Keyloggers**" read data – especially passwords – directly when entered and transmit them to cybercriminals

Origin of Stolen Identity Data (2/3)

- **Phishing**
  - users are lured in good faith to a malicious website that falsely claims to be a legitimate site
  - there users are asked to enter personal identity data
- Disclosure in **social networks** and **forums**
  - users gullibly post all data about themselves, including identity data, in networks such as Facebook, Twitter, ...
  - anyone registered at those platforms can then view the data and steal it

Origin of Stolen Identity Data (3/3)

- Theft or loss of **data media**
  - storages of personal data are not correctly protected against physical access
  - When such storage media are thieved or lost, all stored identity data falls into the hands of the thief
- **Social engineering**
  - manipulating individuals to disclose sensitive data

Security Incidents – Some Statistics

Verizon publish annual **Security Incident Analysis Reports:**

Incidents in 2019

- 32.002 security breaks
- 3.950 confirmed data thefts

Most common attacks
DoS (Hacking)
Phishing (Social Engineering)
Social Engineering

Most common hacking attacks
1. Usage of stolen access data
2. Advantage of software vulnerabilities
3. Use of backdoor

Most common malware attacks
1. Email link
2. Direct install
3. Download by malware

Most common social engineering attacks
1. Phishing
2. Fake pre-text
3. Other

Was My Digital Identity Stolen?
The HPI Identity Leak Checker (1/2)

You can check with the → **HPI Identity Leak Checker**

Link: https://sec.hpi.de

- Collects leaked user/identity databases published on the Internet and provides a search service

Input:

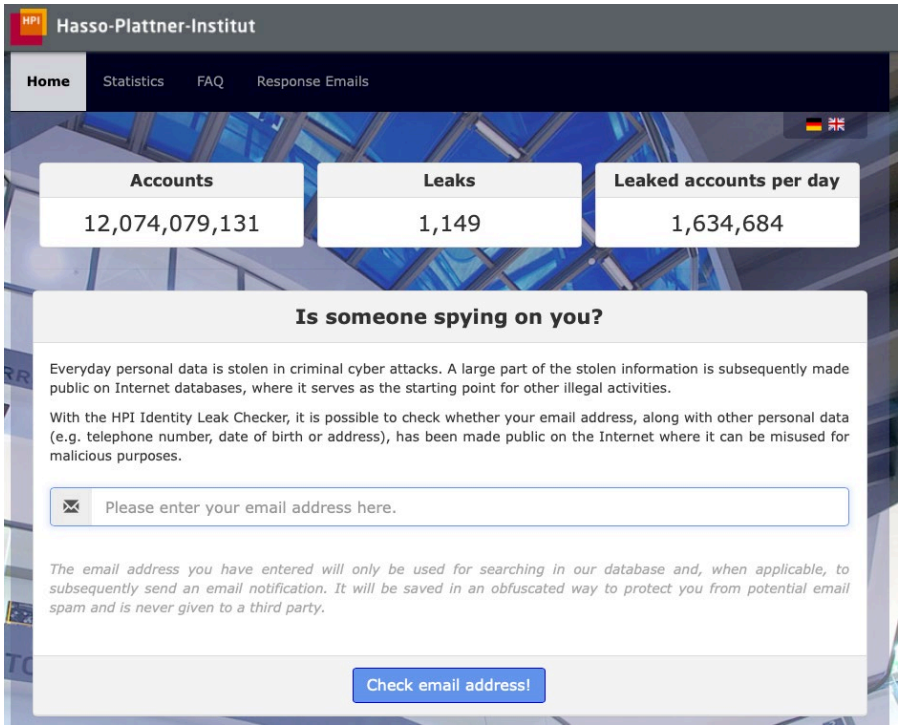
- Your email address (part of the digital identity)

Output:

- **Report with check results is** sent to the provided email address

Additional services:

- Password statistics



Was My Digital Identity Stolen?
The HPI Identity Leak Checker (2/2)

Some statistics on identity theft:

- HPI Identity Leak Checker is online since May 2014

Up to now:

- **12.1 billion** stolen identities recorded from more than 1000 leaks
- **15.3 million** requests
- **3.6 million** people were informed that their identity data is published on the Internet

Leaked user/identity data published on the Internet vary in size. Therefore it has to be normalized before it can be searched within the service

- We found **3,000 further identity leaks with millions of credentials** that have not been normalized yet

Motivation of Identity Theft (1/2)

- **Reputation**
  - cybercriminals want to show what they can do
  - captured data is publicly posted on the Internet as evidence, that a service has been hacked
- **Profit**
  - Data can be sold profitably on the black market
  - Use (by third parties) for criminal purposes
    - sending spam
    - debiting of financial services
    - use of a false identity

Motivation of Identity Theft (2/2)

- **Hacktivism**
  - Fighting for a political / ideological goal
  - damage to the reputation of the victim
    - e.g., Anonymous
- **Revenge**
  - someone has been wronged
  - wants to take revenge by stealing and publishing personal details of this person

Summary: Identity Theft

- Identity theft means that an **attacker takes over the digital identity of a user** so that he/she can use all services and resources for which the user's identity is authorized
- The more information an attacker has about the victim, the easier it is for him to abuse his digital identity
- Attackers have various possibilities to access identity data
  - Theft of password databases
  - Malware
  - Phishing, social engineering, social networks
  - Theft of data media