

openHPI course "Digital Identities
Identity thefts -
Attacks on Digital Identities

Prof. Dr. Christoph Meinel

Hasso Plattner Institute, University of Potsdam

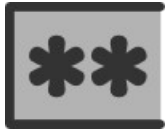
Identity theft (1/2)

- If a third party comes into possession of a user's digital identity, he can use all services and resources on the user's behalf for which the user has an authorization, e.g.
 - shopping, making bank transfers, watching videos,
- Unlike physical identities, it is relatively easy to **misuse** the stolen digital identity

Identity theft (2/2)

- Identity thefts are very attractive for cyber criminals due to their high potential for abuse:
 - With a stolen digital identity, the cybercriminal thief has all the rights (authorization) like the rightful owner
 - Since Internet services authorize solely on the basis of the digital identity, thief can use the services at the expense of the legitimate owner

Target: Identity Data



password



address



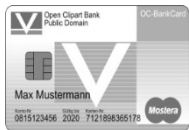
Email Address



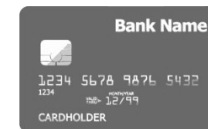
telephone number



Passport/ID card data



account details



credit card details

Origin of stolen identity data (1/5)

- Theft of the **password database** of Internet services
 - Cybercriminals gain access to the system of an Internet service provider and copy the database of its authorization system with all identity data.
 - Frequently executed by so-called "SQL Injection"
- Data theft using **malware**, e.g.
 - "Spyware" collects data directly from the user's computer - of particular interest are the identity data
 - "Keyloggers" read data - especially passwords - directly when they are entered and transmit them to cybercriminals.
- ...

Origin of stolen identity data (2/5)

■ **phishing**

- Users are lured in good faith to a malicious web site that falsely claims to be a legitimate site
- There, users are requested to enter personal identity data.

■ Revelation in **social networks** and **forums**

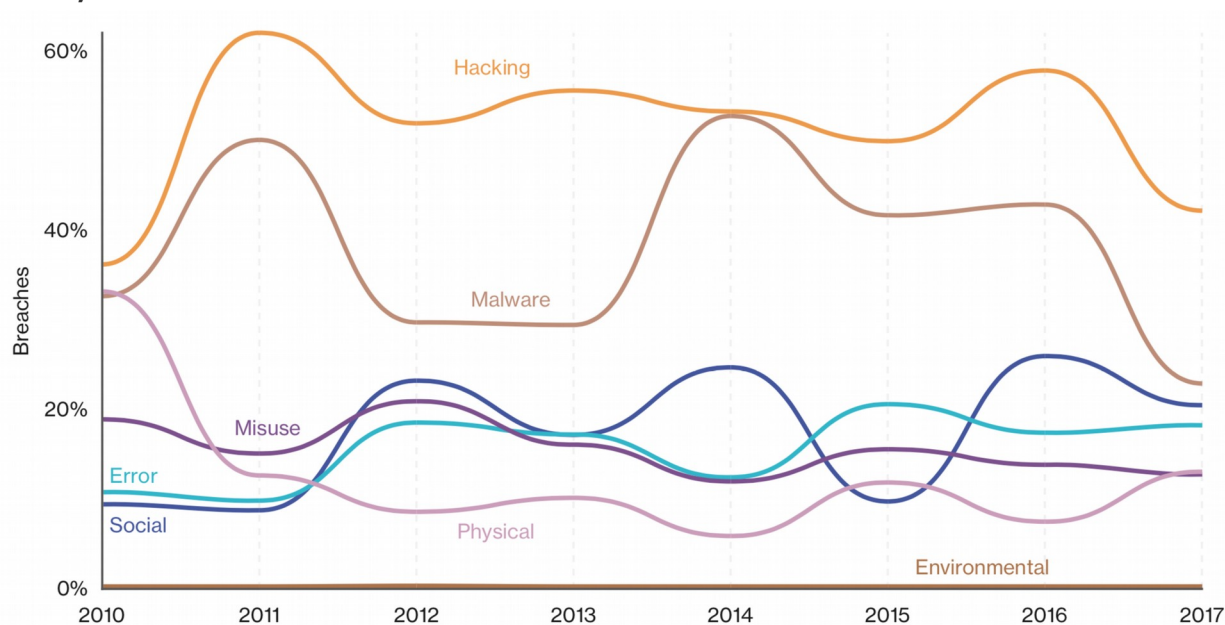
- Users gullibly disclose all data about themselves, including the identity data, in networks such as Facebook, Twitter, ...
- Anyone registered there can then view and steal the data

Origin of stolen identity data (3/5)

- Theft or loss of **data media**
 - stored personal data is not properly secured against physical access
 - in the event of theft or loss of storage media, all identity data also falls into the hands of the thief
- **social engineering**
 - Manipulation of persons to disclose sensitive data
- ...

Origin of stolen identity data (4/5)

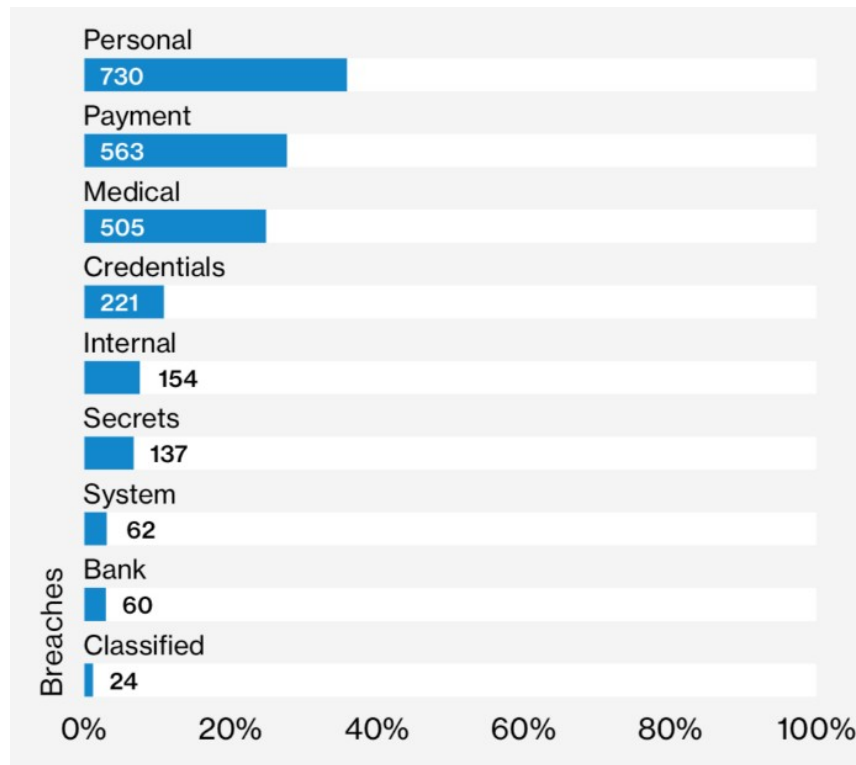
- Every year **Verzion** publishes an analysis of security incidents
- Incidents in 2017
 - 53,000 security incidents
 - 2,216 confirmed data thefts



Source: 2018 Data Breach Investigations Report (Verizon)

Origin of stolen identity data (5/5)

- Every year **Verzion** publishes an analysis of security incidents
- Incidents 2017 by data type



Source: 2018 Data Breach Investigations Report (Verizon)

HPI Identity Leak Checker (1/3)

Identity Leak
Checker
by Hasso-Plattner-Institut



- Internet service of the Hasso Plattner Institute, which searches for freely accessible identity databases ("leaks") illegally published on the Internet.
- Developed by HPI researchers at my Chair of "Internet Technologies and Systems" with the goal of alerting users when their identity data is freely accessible on the Internet and can be abused by anyone.
- Start: May 2014, available at <https://sec.hpi.de>

HPI Identity Leak Checker (2/3)



- Enter your e-mail address at <https://sec.hpi.de>
- Shortly thereafter, you will receive an email stating whether your identity data was found in an unlawfully published identity database collected by HPI.

The screenshot shows the HPI Identity Leak Checker website. At the top, there's a navigation bar with 'Start', 'Statistiken', 'FAQ', and 'Antwort-E-Mails'. Below this, three white boxes display statistics: 'Nutzerkonten' (8.165.169.702), 'Leaks' (810), and 'Geleakte Accounts pro Tag' (882.733). The main section is titled 'Wurden Ihre Identitätsdaten ausspioniert?' and contains a paragraph about identity theft. Below the text is a text input field with a placeholder 'Bitte geben Sie hier Ihre E-Mail-Adresse ein.' and a blue button labeled 'E-Mail-Adresse prüfen!'. A small disclaimer at the bottom states that the email address is only used for searching the database and is stored in an encrypted form.

Nutzerkonten	Leaks	Geleakte Accounts pro Tag
8.165.169.702	810	882.733

Wurden Ihre Identitätsdaten ausspioniert?

Täglich werden persönliche Identitätsdaten durch kriminelle Cyberangriffe erbeutet. Ein Großteil der gestohlenen Angaben wird anschließend in Internet-Datenbanken veröffentlicht und dient als Grundlage für weitere illegale Handlungen.

Mit dem HPI Identity Leak Checker können Sie mithilfe Ihrer E-Mailadresse prüfen, ob Ihre persönlichen Identitätsdaten bereits im Internet veröffentlicht wurden. Per Datenabgleich wird kontrolliert, ob Ihre E-Mailadresse in Verbindung mit anderen persönlichen Daten (z.B. Telefonnummer, Geburtsdatum oder Adresse) im Internet offengelegt wurde und missbraucht werden könnte.

✉ Bitte geben Sie hier Ihre E-Mail-Adresse ein.

Die von Ihnen eingegebene E-Mail-Adresse wird lediglich zur Suche in unserer Datenbank und das anschließende Versenden einer Benachrichtigungs-E-Mail benutzt. Sie wird von uns in verschlüsselter Form gespeichert, um Sie vor E-Mail-Spam zu schützen. Die Weitergabe an Dritte ist dabei ausgeschlossen.

E-Mail-Adresse prüfen!



Experiences from the project

- Since May 2014 we have more than **7.000 Identity Databases** freely accessible on the Internet
- Of these, the largest databases have more than 2 billion identity records
- We currently collect around 8.2 billion data records from more than 800 freely available leaked databases on the Internet
- The most frequently leaked data types are:
 - E-mail address, passwords, address, telephone, ...

Motivation of identity theft (1/2)

■ **standing**

- Cyber criminals want to show what they can do
- captured data is publicly posted on the net as proof that a service has been cracked

■ **gain**

- Data can be profitably sold on the black market
- Use (by third parties) for criminal purposes
 - Sending Spam
 - Direct debiting of financial services
 - Use of a false identity

Motivation of identity theft (2/2)

- **hacktivism**

- Fight for mostly quashed political / ideological goal
- Damage to the reputation of the victim
- e.g. Anonymous

- **revenge**

- someone has been wronged.
- wants to take revenge by theft and publication of personal details of this person

- ...

Summary: identity thefts

- Identity theft means that an attacker takes over a user's digital identity so that he or she can use all the services and resources for which the user is authorized on his or her behalf.
- The more information an attacker has about the victim, the easier it is for him to misuse his digital identity.
- Attackers have several ways to gain access to stolen identity data
 - Theft of password databases
 - malware
 - Phishing, Social Engineering, Social Networks
 - theft of data media

Summary: identity thefts

- Identity theft means that an attacker takes over a user's digital identity so that he or she can use all the services and resources for which the user is authorized on his or her behalf.
- The more information an attacker has about the victim, the easier it is for him to misuse his digital identity.
- Attackers have several ways to gain access to stolen identity data
 - Theft of password databases
 - malware
 - Phishing, Social Engineering, Social Networks
 - theft of data media