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

Introduction: Digital Identities

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

openHPI Course: Digital Identities
Physical Identity vs. Digital Identity

Before we can use a Web service on the Internet, we have to **identify** ourselves towards the service such that the service can

- **„recognize"** who we are and
- **„remember"** which permissions we have

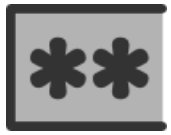
In the physical world we identify ourselves through our outer appearance

- **physical identity**

But how can we identify ourselves on the Internet?

- We can't identify ourselves through our physical presence, but through a collection of electronic data
  - **digital identity**

openHPI Course: Digital Identities
Attributes (Examples)



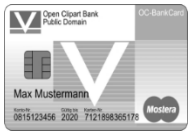
Password

Address

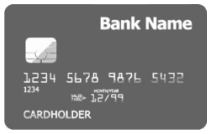
E-Mail Address

Telephone Number

Passport/ID Data



Account Data



Credit Card Number

…and how can we prove that we own a digital identity?

There are numerous ways to provide a proof:

- **knowledge**, e.g. password, pin, …
- **ownership**, e.g. smartcard, token, …
- **Biometric characteristics**, e.g. fingerprint, face,
- …

Most common and simplest method is the use of passwords

- easy to implement
- little effort for the user

But: The use of passwords for authentication is quite unsecure and holds great dangers ...

Passwords must be stored in the **database of the service** so that the password can be verified during the login process

- Attackers can attack services and try to steal there user data, e.g.
  - by **exploiting software vulnerabilities** or through **social engineering attacks** on the service administrator

Stolen identity data can be misused to assume a digital identity

→ Identity theft

Recent case:

- Under the name "Collections #1 - #5", records were published on the Internet in January 2019 that contained a total of **2.1 billion (!) email addresses with the corresponding passwords in plain text**
- In some cases, the exact services from which the identity data was stolen were specified
- Attackers can quickly test the identity/access data for different platforms

Extremely dangerous for the persons effected, as their digital identities remain vulnerable as long as the stolen passwords are valid

More examples:

- In December 2018, data and documents of roughly 1000 politicians and celebrities were published on the Internet
- The data records included internal and personal documents as well as contact data such as email addresses, addresses and telephone numbers of the celebrities concerned

Generally: The more identity data about a person icomes in the hands of cybercriminals, the more easily their identity can be misused

openHPI Course: Digital Identities
Course Overview – First Week

This course is all about the topic:

„**Digital Identities – Who am I in the Internet?**“

- In the **first course week**, we consider how a digital identity is defined and the different ways of managing digital identities

  → **Identity Management**

  … and how to prove that one has a certain digital identity

  → **Authentication methods**

openHPI Course: Digital Identities
Course Overview – Second Week

This course is all about the topic:

„**Digital Identities – Who am I in the Internet?**“

- In the **second course week** we deal with question which **attacks on digital identities** are possible and how to best protect your digital identities
- In addition, we look at the problem of **"weak passwords"** and give advice on how to choose **strong passwords** and what influence strong passwords have on possible attacks

openHPI Course: Digital Identities
Introduction of the Teaching Team

Prof. Dr. Christoph Meinel

- Institute Director and Dean of the Hasso Plattner Institute
- Head of the Chair "Internet Technologies and Systems"
- Research focus: Security Engineering, Learning and Knowledge Engineering, Digital Education, Innovation Research

openHPI Course: Digital Identities
Introduction of the Teaching Team

Alexander Mühle

- Secure Identity
- Peer-to-Peer Applications

Chris Pelchen

- Security Engineering
- Identity on the Internet