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

Identity Theft – Social Engineering Attacks on Providers

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

Attacking the Service Provider (1/2)

- Not only users, but also employees of service providers can be attacked by cybercriminals
- Cybercriminals can perform **social engineering attacks on service provider employees** to provoke certain actions, e.g.
  - to take over digital identities of registered users
- Cybercriminal pretends to be the rightful owner of the digital identity
  - the more information the attacker has about the victim, the more credible he appears
- **Victim does not notice** that his digital identity has been stolen

Attacking the Service Provider (2/2)

Typical attack vectors:

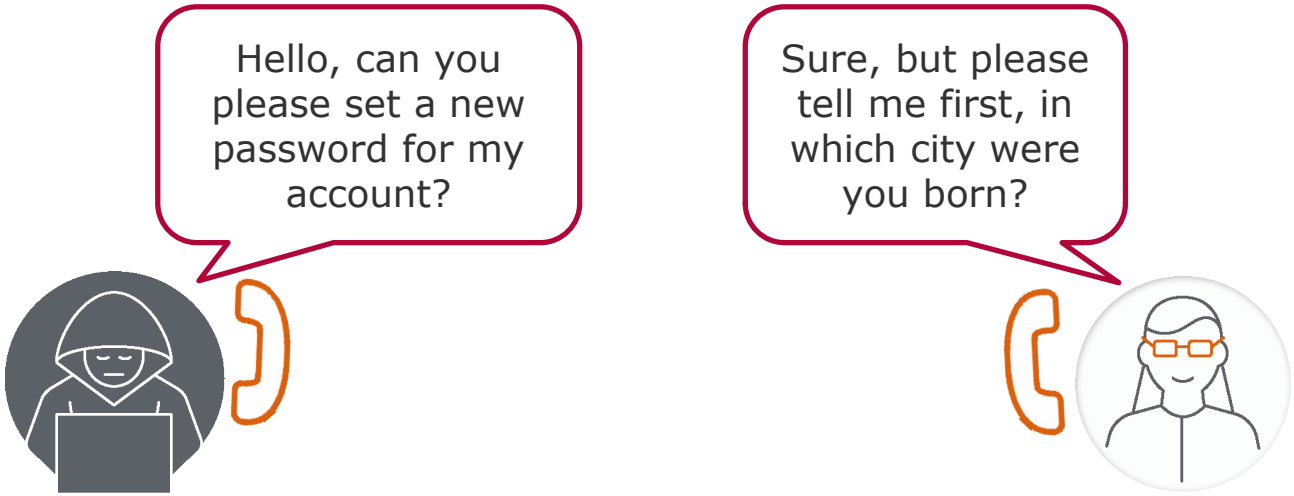
- **Password Reset**
  - Attacker convinces the service provider employees **to reset a password** and hijacks the process to choose a new one
    - service provider wants to help the user quickly
    - identity verification often insufficient
    - usability > security
- **Change in 2FA** (2-factor-authentication)
  - Attacker convinces the service provider employees to **reset the second/third factor of authentication**
    - change the phone number used for SMS-TAN
    - disable the second factor altogether

Password Reset (1/2)

Goal: Gain access to an account via a new password

Attack Methods:

- **Social Engineering**
  - convince service provider employees to reset to a new email address due to "lost email account"
  - easily guessable secret questions are a common vulnerability



Password Reset (2/2)

Goal: Gain access to account via new password

Attack Methods:

- **Man-in-the-Middle**
  - attacker initiates a password reset request
  - forwards any challenges from the website to the victim

Change in 2FA – 2-Factor-Authentication

Goal: Gain access to account via new password

Attack Methods:

- **Social Engineering**
  - convince mobile phone provider to send a new SIM-card due to a lost phone
  - convince service provider employees to send new TANs to that new phone number
- **Man in the Middle**
  - exploit vulnerabilities especially in the mobile phone network protocols (SS7) to intercept SMS-TAN