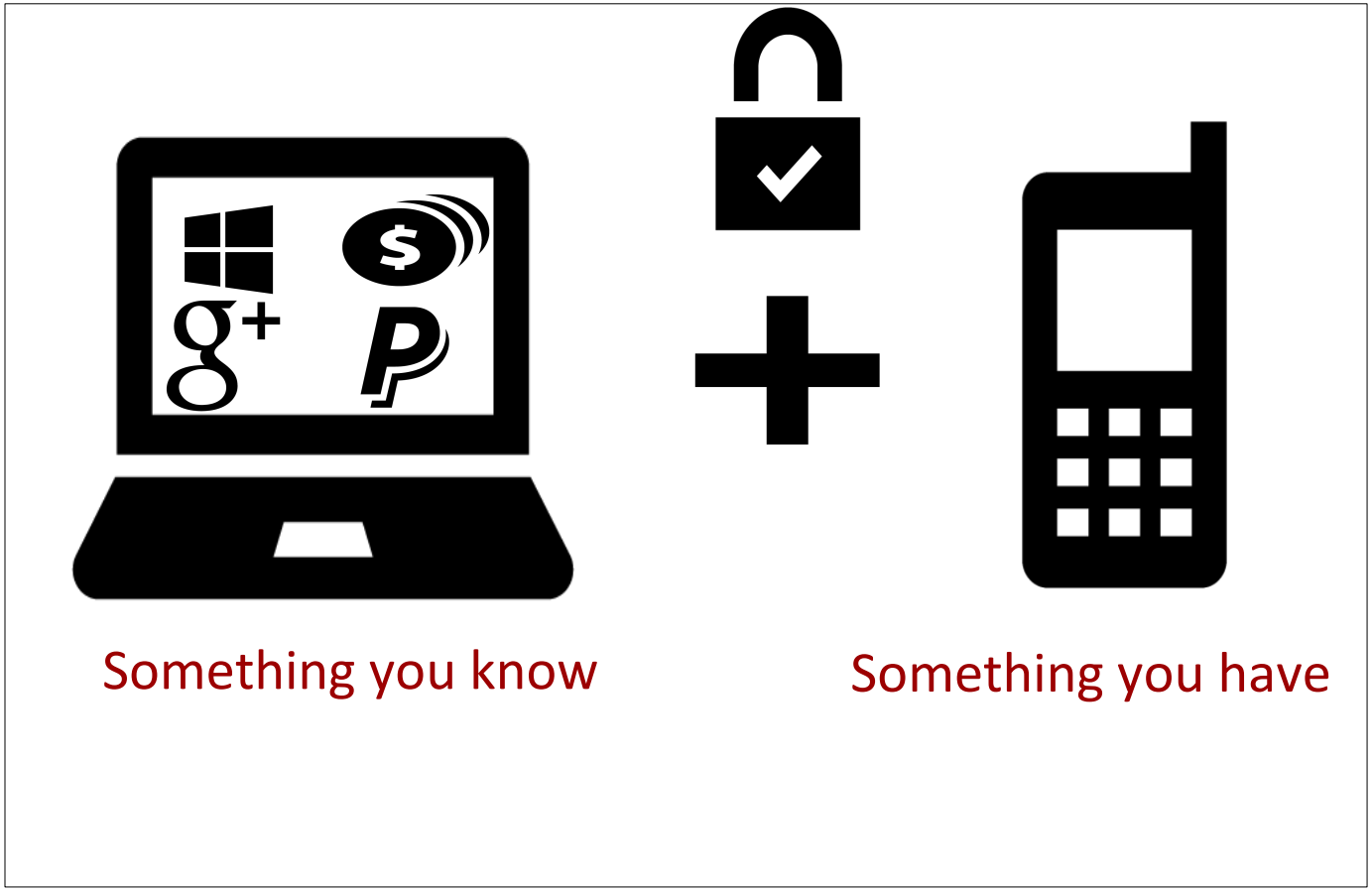
SMS-Based One-Time Passwords: Attacks and Defense

Collin Mulliner*, Ravishankar Borgaonkar, Patrick Stewin, and Jean-Pierre Seifert

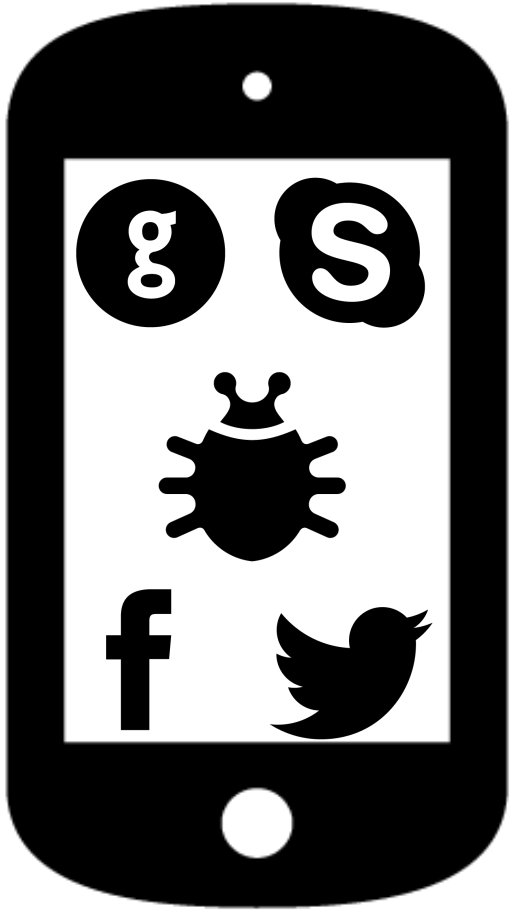
(*Northeastern University)

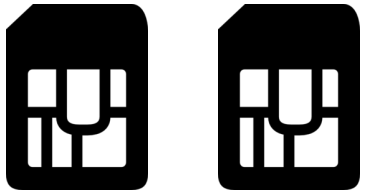
DIMVA 2013 - 19 July, 2013 - Berlin Germany.

One Time Passwords – SMS



Attacks against SMS OTP





Mobile Phone Trojans

July 9th, 2011, 10:55 GMT · By Lucian Constantin

Zbot Targets Android Users

SHARE: +1 0 Like 5 Send Tweet 36 Adjust text size:

Security researchers have identified a Zbot component designed for Android which steals mobile transaction authentication numbers send by banks via SMS.

POLIZEI BERLIN

Pressemeldung

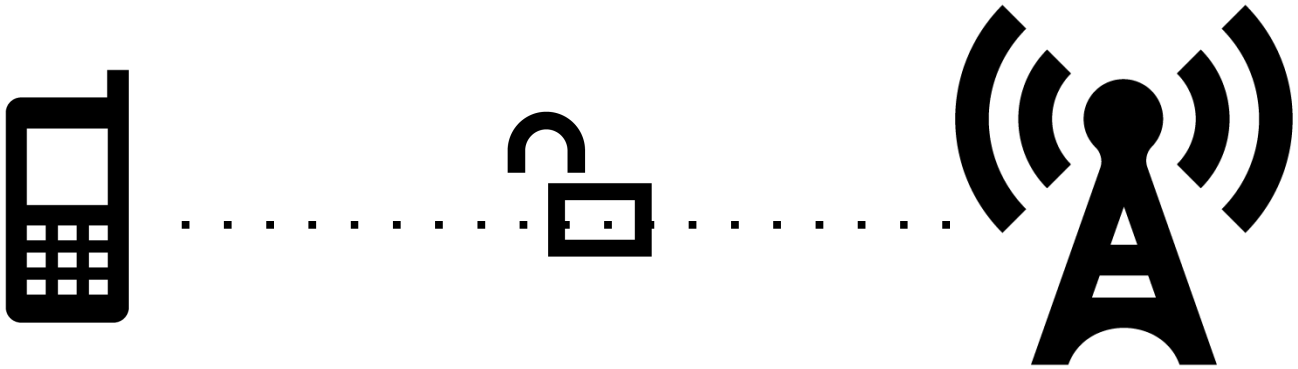
Eingabe: 13.11.2012 - 10:50 Uhr

Präventionshinweis für Onlinebanking im mTAN-Verfahren

3628

Wireless Interception Attacks

GSM



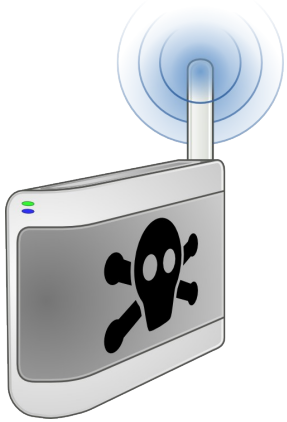
No Mutual Authentication

Weak Encryption Algorithm

Wireless Interception Attacks

3G Femtocell

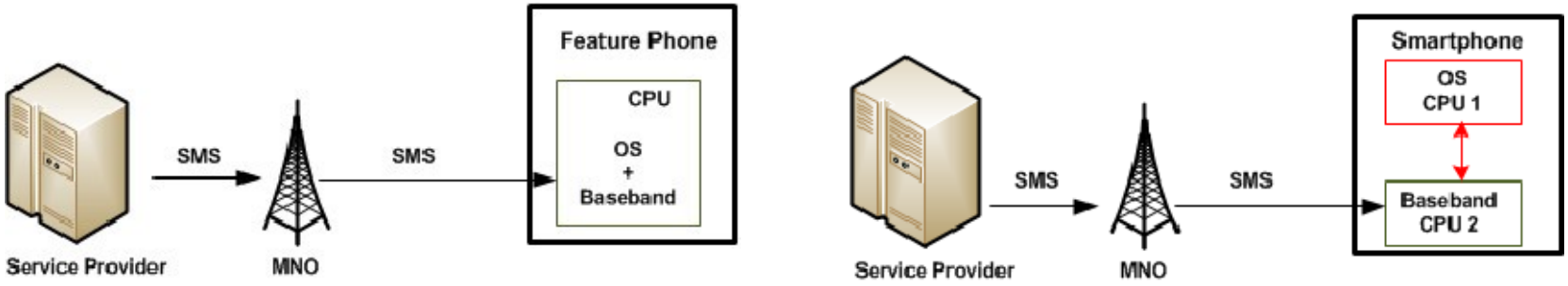
- Architecture Vulnerability
- SMS Traffic Interception



```
▷ TP-Originating-Address - (DB Mobile)
▷ TP-PID: 0
▷ TP-DCS: 0
▷ TP-Service-Centre-Time-Stamp
  TP-User-Data-Length: (90) depends on Data-Coding-Scheme
▽ TP-User-Data
    SMS text: Your activation code is: 779495. Please enter this code in the Online-Banking application.
```

SMS OTP Attack Analysis

- **Mobile phone design issues**

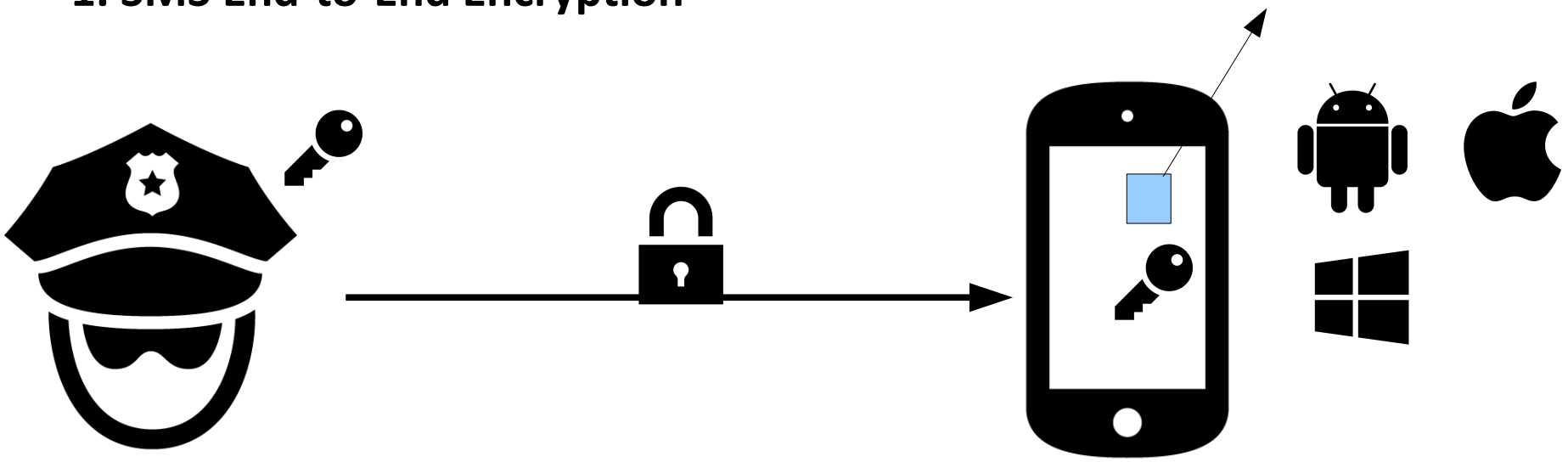


- **Relies on security of cellular networks**
  - **No End-to-End encryption**

Defending SMS OTP

Goal: Minimal Support of OTP providers, MNO, Mobile OS

1. SMS End-to-End Encryption



No eavesdropping

Malicious App can not access

SMS OTP – Our Solution

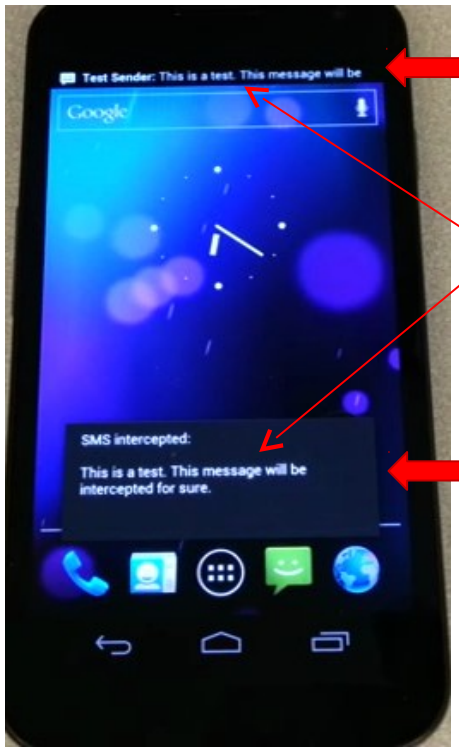
- Incoming SMS message is broadcasted through the system
  - any app w/ SMS read permission has access, that's why SMS Trojans work in the first place!

- Main idea: change SMS routing **inside** the smartphone
  - a "virtual channel" inside the phone to protect SMS OTP messages
  - "Special" SMS messages are directly delivered to special app
    - No broadcast no interception possibilities!

- Implementation: Proof-of-Concept for Android
  - Keyword filter that matches SMS message body
    - Keywords: OTP, Token, mTAN, Password, …
  - Matching SMS message is delivered to our own SMS inbox app

SMS OTP: Implementation

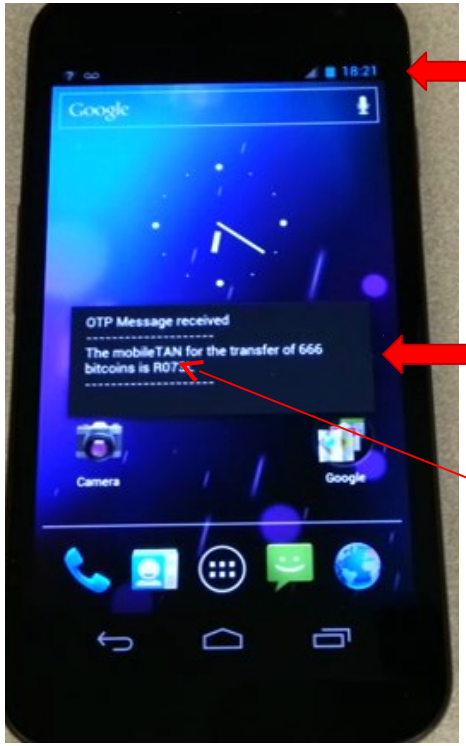
Device is running our Virtual SMS Channel



SMS app gets message (any “normal” SMS)

SMS message received by both

PoC Trojan gets SMS



SMS app does NOT see OTP message!

OTP Message app is the only app that sees this message (keyword: mobileTAN)

Summary

- Studied various SMS OTP attacks
- Identified root-causes
  - Mobile phone design issue
  - MNO network insecurities
- Defending attacks
  - End-to-End encryption
  - Virtual dedicated SMS channel
    - Implemented message filter-based channel

Thank you!