White Rabbit in Mobile

Effect of Unsecured Clock Source in Smartphone OS and Apps

Shinjo Park [1]
Altaf Shaik [1]
Ravishankar Borgaonkar [2]
Jean-Pierre Seifert [1]

[1]TU Berlin / Telekom Innovation Labs

[2]Oxford University

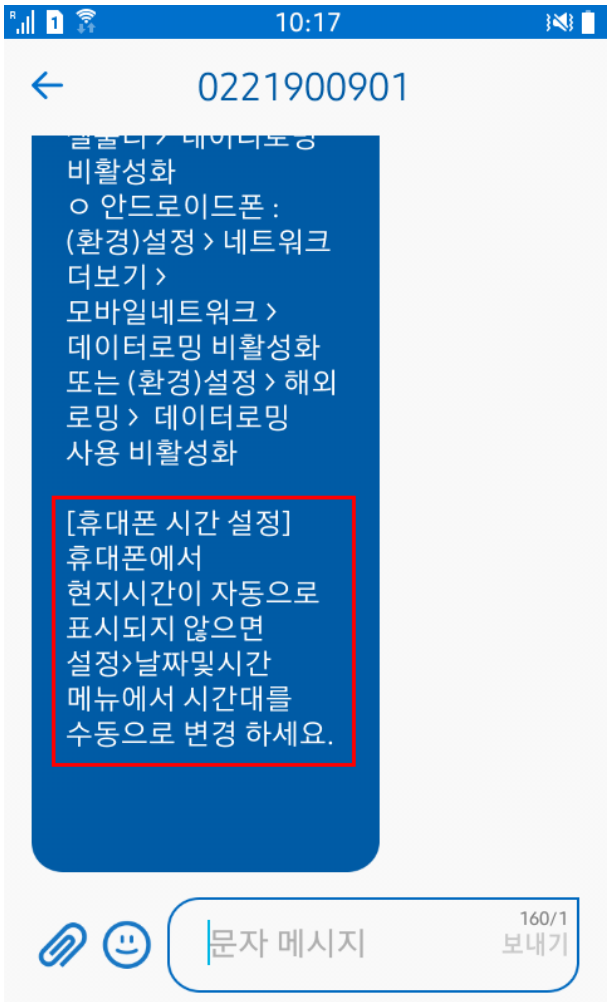
PoC 2016, 2016. 11. 11

SECT

Contents

- Introduction to clock sources on smartphones
- Security analysis and attack on NITZ and NTP
- Effect of attack on smartphone OS and apps
- Conclusion and future work

How Smartphones Set Clock?

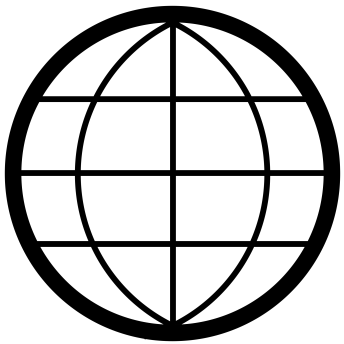


- Roaming information SMS from KT
- Highlighted text says: “If your clock is incorrect, please manually set your current time zone”
- Why KT is sending this SMS?

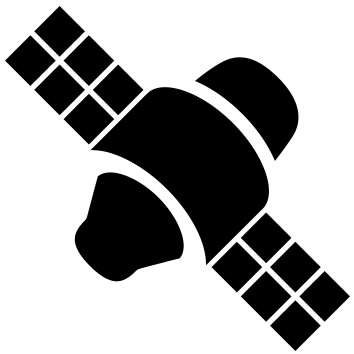
How Smartphones Set Clock?

- Smartphones have multiple clock sources such as:

Cellular Network: NITZ



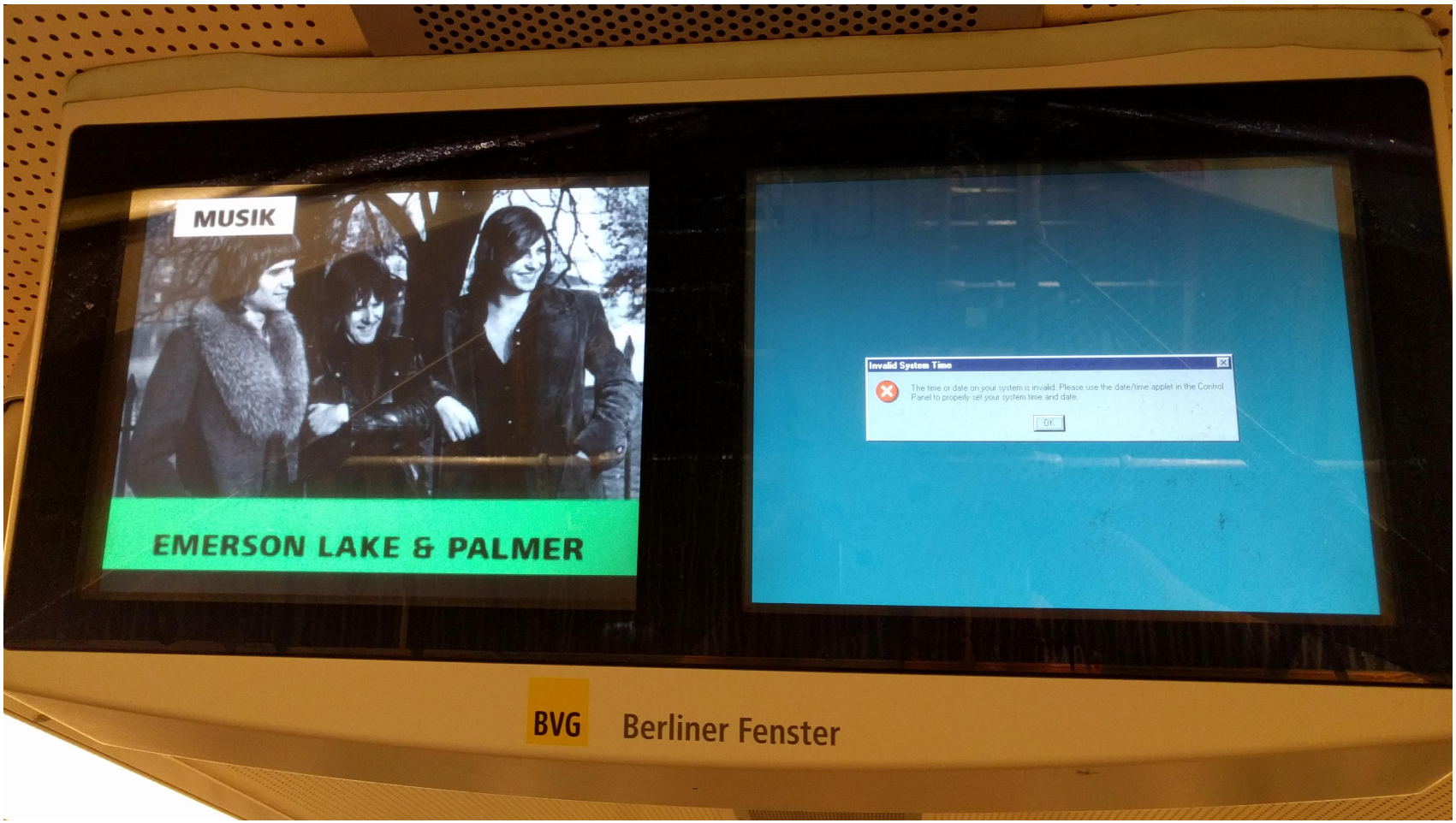
Internet: NTP



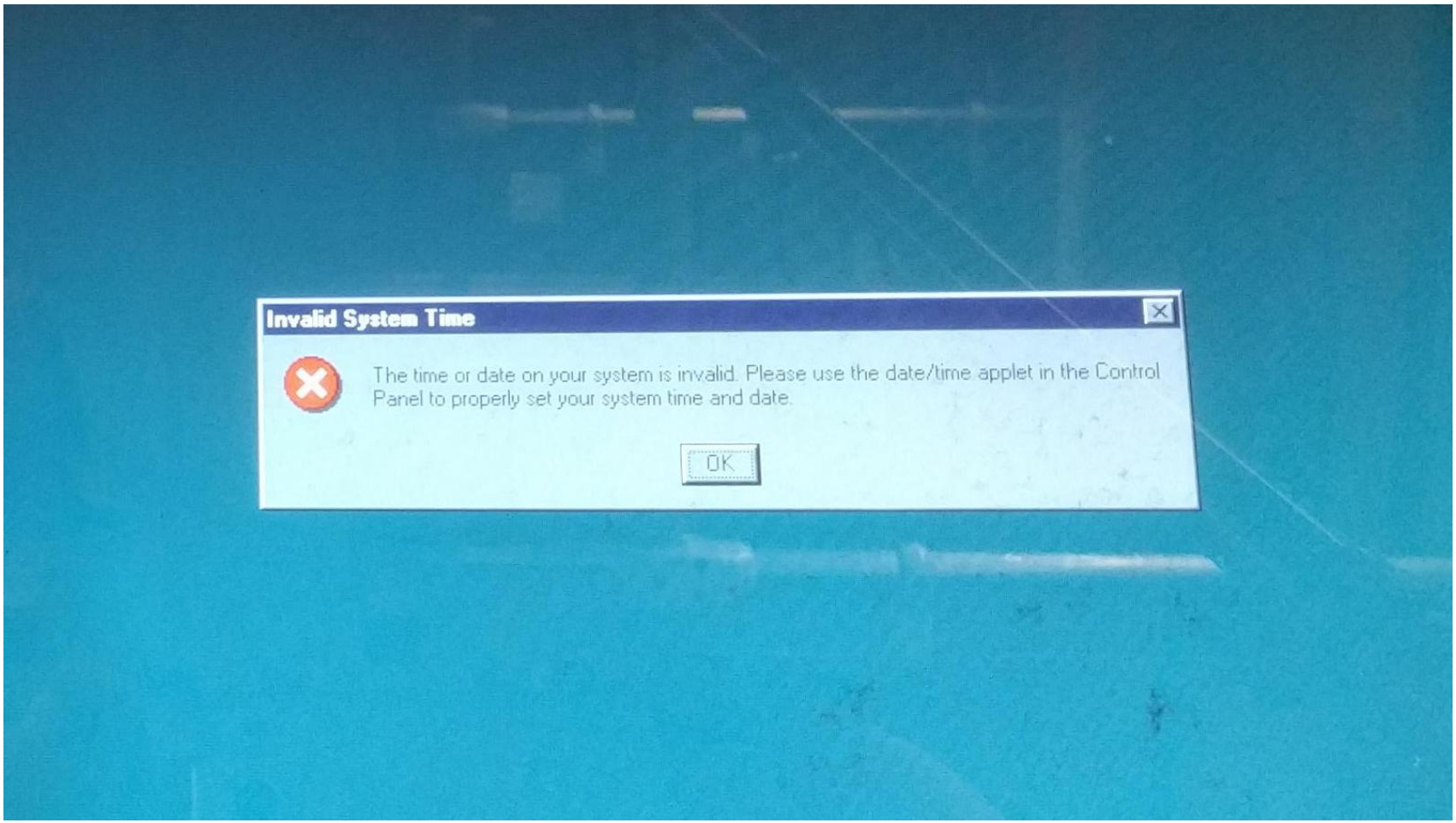
Satellite Navigation: GPS

- We cover NITZ and NTP as user interaction not required
- GPS spoofing, NTP attack is well known but NITZ attack is not
- How clock sources interact on smartphones?

Clock Synchronization Problem



Clock Synchronization Problem



Contributions

- Security analysis of NITZ in cellular network standard
- Implementation of NITZ in real networks and related issues
- Clock spoofing attack via NITZ and NTP
- Effect of clock spoofing on mobile OS and apps

NITZ: Clock in Cellular Network

- NITZ is an optional feature to provide accurate clock to the connected devices (smartphones, tables, IoT devices, etc.)
- Frequency of NITZ message is up to operator configuration
  Analysis of signaling messages during automated call

Operator (Country)	**2G/3G**	**4G**
T-Mobile (US)	✓	✓
KT (KR)	✓	✓
Vodafone (IS)	✓	·
E-Plus (DE)	▲	▲
Telekom (DE)	·	·

- ✓– sent after every attach
- ▲– sent spontaneously
- · – not sent at all

NITZ: Clock in Cellular Network

- NITZ must be accepted after mutual authentication in:

2G (GSM)	3G	4G
✗	✓	✓

- 2G CDMA do not use separate clock information; system clock is synchronized with GPS
- Roaming from network with NITZ to without NITZ cause clock synchronization issue
  - Example: T-Mobile USA (with NITZ) to Telekom Germany (no NITZ)
  - Recall the SMS in the previous slide!
  - Manual update still possible

NITZ vs. NTP: Multiple Clock Sources

- There is no single policy on prioritizing clock sources
- Mobile OS usually prefer NITZ, as cellular network is more trusted than Wi-Fi
  - Stock Android prefer NITZ
  - Windows 10 Mobile, Tizen, BlackBerry 10 has equal priority
  - Apple iOS
- Other observed behaviors
  - Apple iOS later than 9.3
  - Some Android modification puts equal priority on NITZ and NTP

Clock Source of Operators

- Around year 2010–2011: GPS jamming attempt of North Korea
- Operators using GPS as sole clock source are affected, providing inaccurate NITZ
- Securing clock source is important for operators

Attack Model and Setup

- Attacker operating fake base station and Wi-Fi access point – allowing everyone nearby can connect to it
- Fake base station (2G/3G/4G) is transmitting inaccurate NITZ
- Fake Wi-Fi access point is connected to the fake NTP server

Experimental Results

- Most of phones accepted inaccurate clock on fake 2G network
- For 3G/4G, some phones accepted clock without mutual authentication
- Phones prioritizing NITZ accepted NTP clock information only in absence of NITZ

Phone	**NTP → NITZ**	**NITZ → NTP**
Google Nexus 5	NITZ	NITZ
HTC One M9	NITZ	NTP
BlackBerry Z10	NITZ	NTP
Microsoft Lumia 950	NITZ	NTP
Samsung Z1	NITZ	NTP

Experimental Results

- Android will issue NTP request no more than once a day
- Automatic clock synchronization is hindered when real network does not send NITZ
  - NITZ is prioritized over NTP $\rightarrow$ NTP will not override NITZ

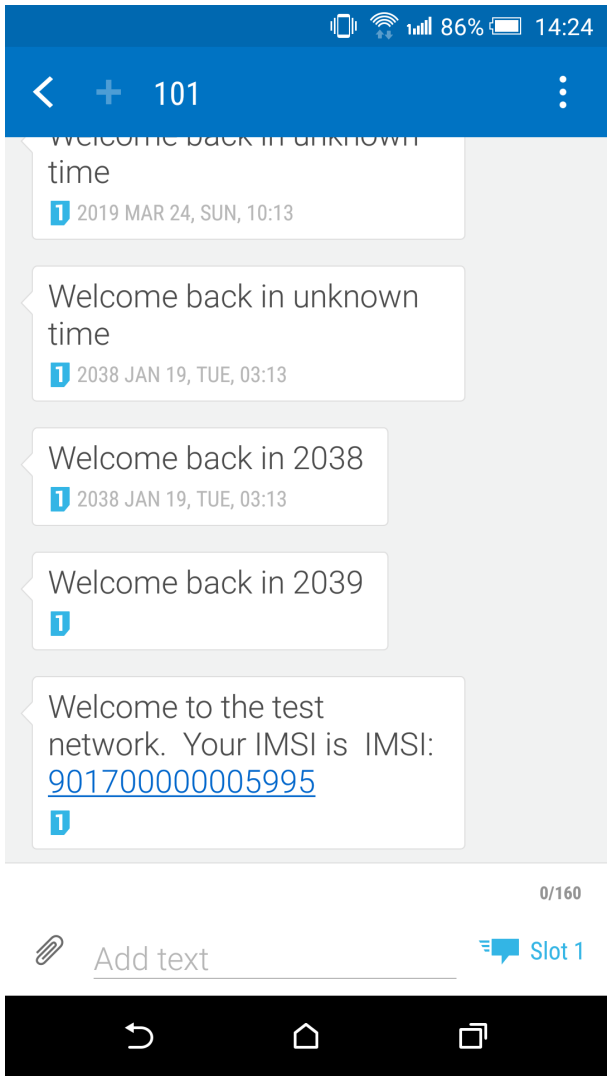
Mobile Network Operation

- None of 3G/4G signaling messages carry clock information, except NITZ message itself and SMS
- Operator internal clock management causes error on CDR operation

- Received SMS messages carry network clock information

```
GSM SMS TPDU (GSM 03.40) SMS-DELIVER
    0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
    .1.. .... = TP-UDHI: The beginning of the TP UD field contains a Header in addition to the short message
    ..0. .... = TP-SRI: A status report shall not be returned to the SME
    .... 0... = TP-LP: The message has not been forwarded and is not a spawned message
    .... .1.. = TP-MMS: No more messages are waiting for the MS in this SC
    .... ..00 = TP-MTI: SMS-DELIVER (0)
  > TP-Originating-Address - (436601020985)
  > TP-PID: 127
  > TP-DCS: 246
  v TP-Service-Centre-Time-Stamp
      Year: 16
      Month: 10
      Day: 25
      Hour: 7
      Minutes: 46
      Seconds: 18
      Timezone: GMT + 2 hours 0 minutes
    TP-User-Data-Length: (20) depends on Data-Coding-Scheme
  > TP-User-Data
```

Demo 1: SMS Timestamp



- Whether to show network or phone clock information is up to device developer
- Some device showed both, some device showed only network or phone clock information
- Can we inject SMS with fake clock information?

- **Disclaimer:** please do your experiment ethically and do not interfere with commercial service!

Mobile OS Issues

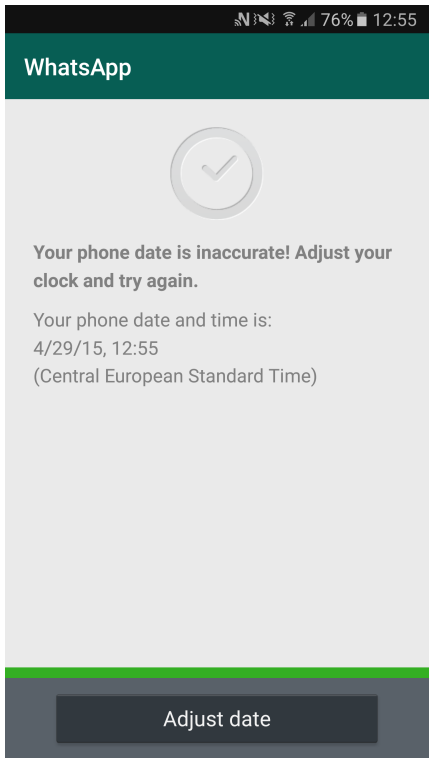
- Mobile OS clock is also used by apps, baseband has separate clock
- Android and iOS use UNIX time: seconds passed since 1970-01-01
- Year 2038 Problem: Signed 32-bit UNIX time will overflow in January 2038
- Android crashes by setting date near overflow point (see also CVE-2016-3831)

Demo 2: Android Crash

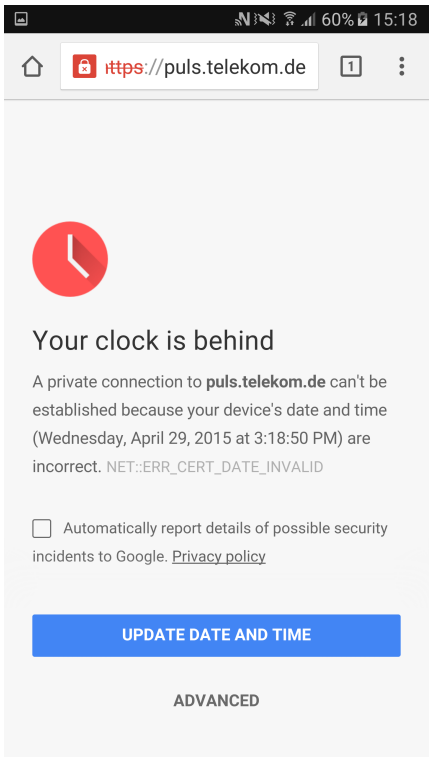
- Fake base station is sending year 2038
- Any 32-bit Android devices with security patch level before 2016-08-01 will crash
- ... which includes Android-based IoT/embedded devices

Mobile Apps and Clock Spoofing

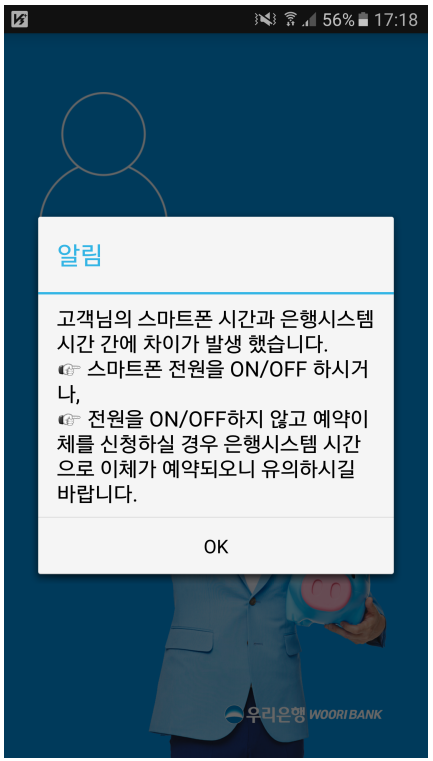
- Apps using clock information locally have no way to check it
- Best practice – explicit indication of clock spoofing



WhatsApp



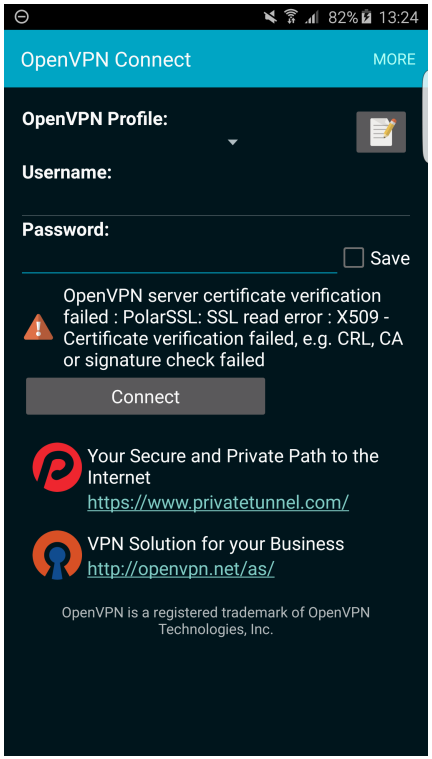
Chrome



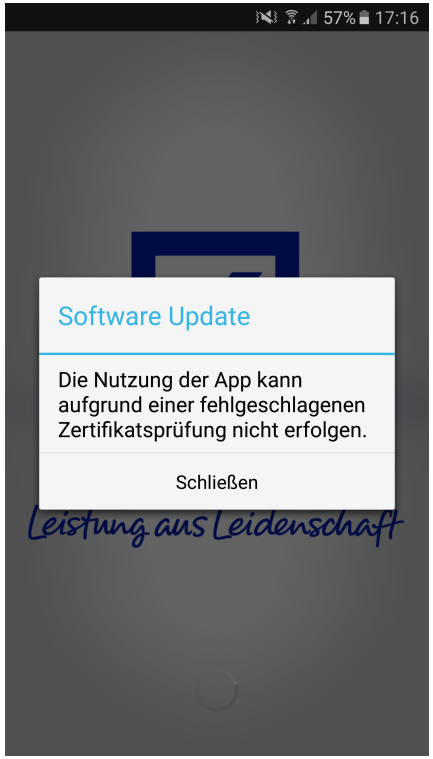
Woori Bank

Mobile Apps and Clock Spoofing

- Common practice – not distinguishing from generic network error
- Some apps did not indicated clock spoofing at all

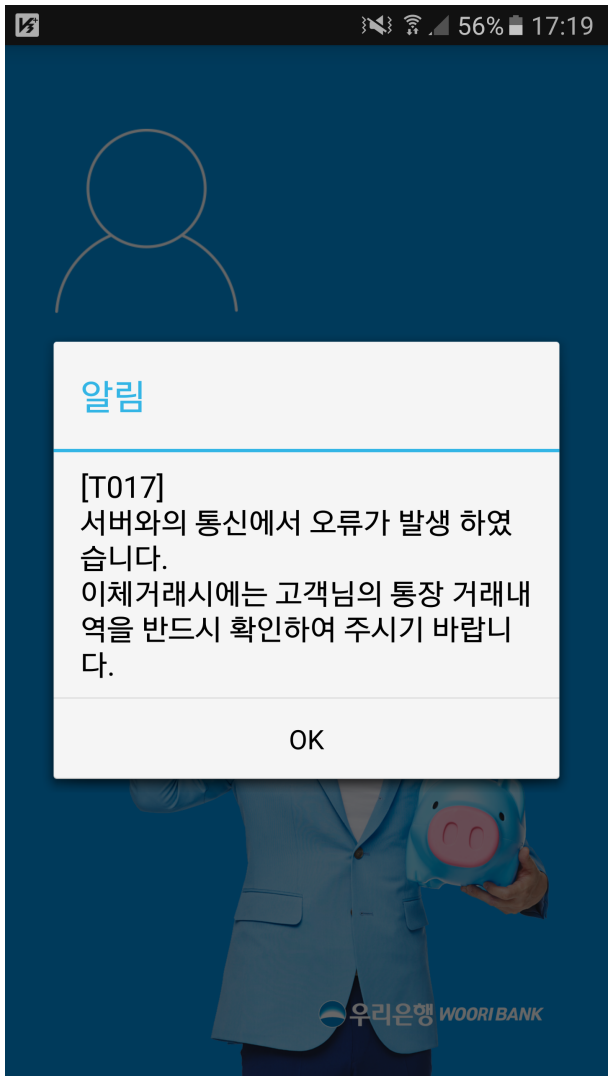


OpenVPN



Deutsche Bank

Demo 3: App Operations



- Affecting app operations by manipulating clock information
- What app will work, what will not?

Mitigations

- Time-critical apps
  - Implementing own NTP server to check clock
  - Example: tickeing apps, banks
- TLS certificate: short validity period, maintenance cost for renewal
- Better clock policy on roaming (operator change)
- Operator: secure clock sources when using NITZ

Conclusion and Takeaway Messages

- Smartphones have two main clock sources: NITZ, NTP
- Many vendors do not have single policy on priority
- Security issues in NITZ specification and incorrect policies allow clock spoofing attack resulting in a DoS
- Mobile OS needs to have consistent and secure clock source policy management

- Clock spoofing attack towards IoT and M2M devices

Thanks!

- Questions and discussions

This research was partly performed within the 5G-ENSURE project of the EU Horizon 2020 and the Software Campus project from DLR.

SECT

References

- 1: https://commons.wikimedia.org/wiki/File:The_White_Rabbit_(Tenniel)_-_The_Nursery_Alice_(1890)_-_BL.jpg
- 4: https://openclipart.org/detail/15868/wireless-access-point, https://openclipart.org/detail/196091/satellite-icon, https://openclipart.org/detail/153895/earth
- 16: https://xkcd.com/607/
- 10: http://thestory.chosun.com/site/data/html_dir/2011/03/07/2011030700944.html
- 17: https://www.flickr.com/photos/46130640@N05/11277918555
- 23: https://commons.wikimedia.org/wiki/File:Alice%27s_Adventures_in_Wonderland_-_Carroll,_Robinson_-_S119_-_%27What_day_of_the_month_is_it%27_he_said,_turning_to_Alice.jpg