KIRAS Sicherheitsforschung

secure sba-research.org

COMET

Competence Centers for Excellent Technologies

Guess Who's Texting You?

Evaluating the Security of Smartphone Messaging Applications

Sebastian Schrittwieser

10.05.2012

bmvit Bundesministerium für Verkehr, Innovation und Technologie

bmwfj Bundesministerium für Wirtschaft, Familie und Jugend

Christian Doppler Forschungsgesellschaft

FFG

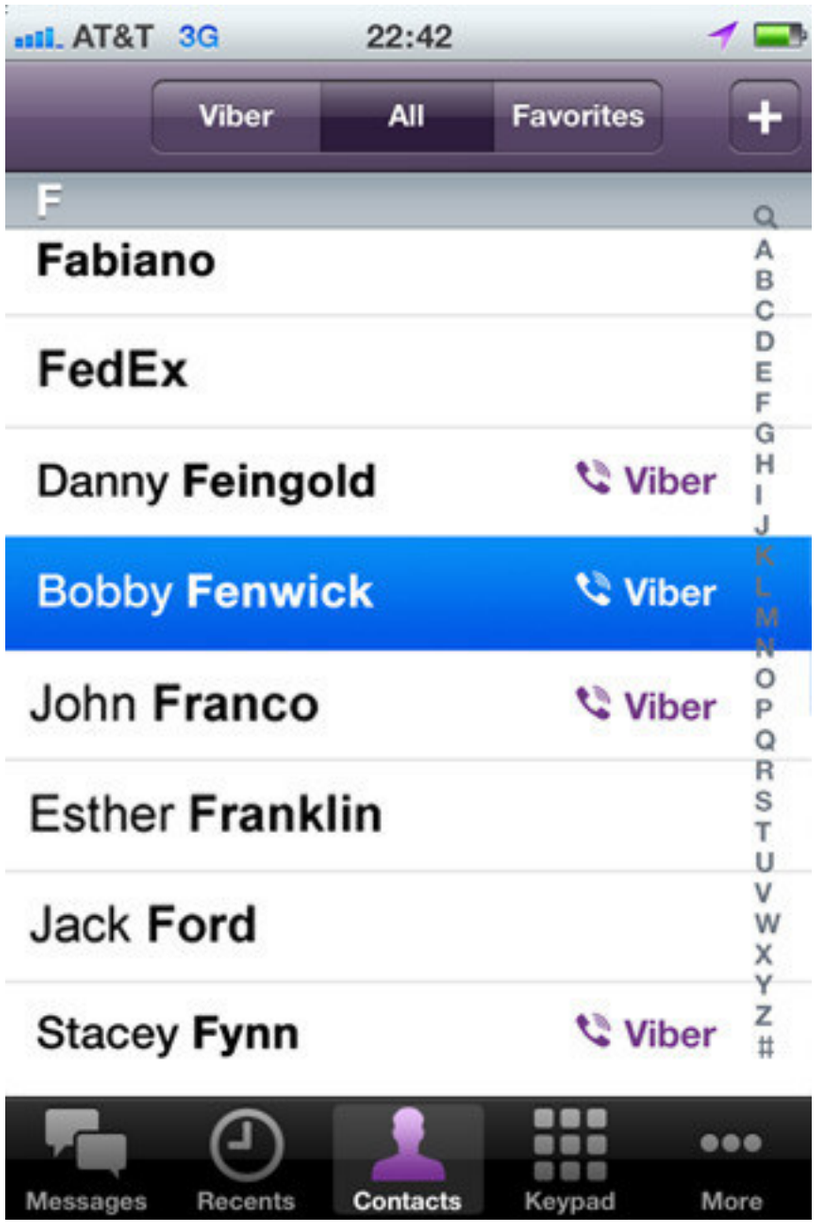
wirtschaftsagentur wien

zit Die Technologieagentur der Stadt Wien

Smartphone Messaging

secure
sba-research.org

COMET
Competence Centers for Excellent Technologies



- Aim at replacing traditional text messaging (SMS) and GSM/CDMA/3G calls
- Free phone calls and text messages over the Internet
- Novel authentication concept
- Phone number used as single authenticating identifier

secure
sba-research.org

COMET

Competence Centers for
Excellent Technologies

Internet

SMS

Telecom infrastructure

Motivation

Competence Centers for Excellent Technologies

	SMS	Messaging Apps
Protocol	proprietary	HTTP(S), XMPP
Security	cryptographically sound authentication (SIM card)	application depended, much weaker authentication (phone number, IMEI, UDID)
Users' perception	SMS	

Evaluation

secure
sba-research.org

COMET
Competence Centers for
Excellent Technologies

Authentication Mechanism and Account Hijacking

Sender ID Spoofing / Message Manipulation

Unrequested SMS / phone calls

User Enumeration

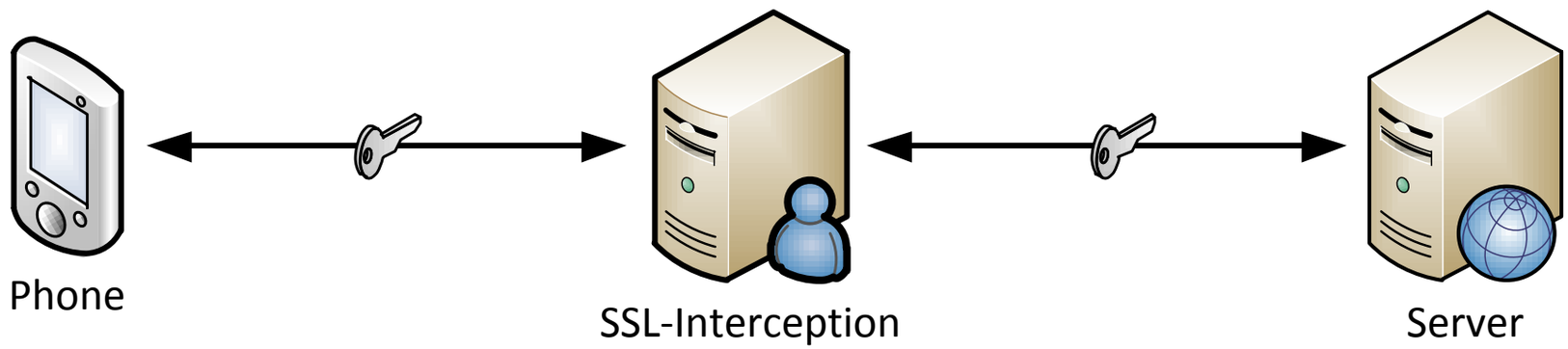
Modifying Status Messages

Experimental Setup

secure
sba-research.org

COMET
Competence Centers for
Excellent Technologies

- Samsung Nexus S running Android 2.3.3 and Apple iPhone 4 running iOS 4.3.3
- SSL proxy to read encrypted HTTPS traffic



- Used to understand the protocol, not for the actual attack (i.e., MITM between victim and server)!

secure
sba-research.org

COMET

Competence Centers for
Excellent Technologies

WhatsApp

eBuddy XMS

WowTalk

Viber

HeyTell

Forfone

Voypi

Tango

EasyTalk

secure
sba-research.org

COMET

Competence Centers for
Excellent Technologies

WhatsApp

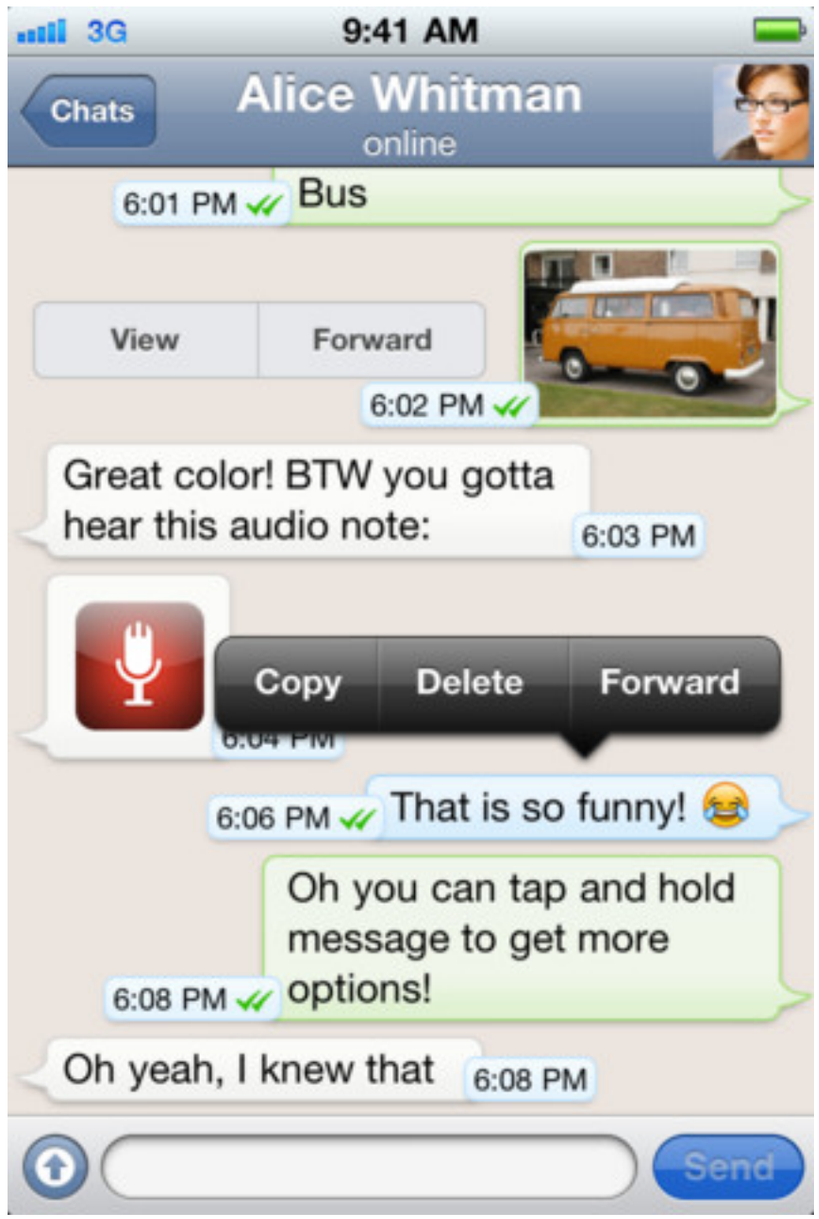
Paper:
Guess who's texting you? Evaluating the Security of Smartphone Messaging Applications
Schrittwieser, S., Frühwirt, P., Kieseberg, P., Leithner, M., Mulazzani, M., Huber, M., Weippl, E.,
NDSS 2012

WhatsApp

secure
sba-research.org

COMET
Competence Centers for
Excellent Technologies

- Instant Messaging
- Status messages
- 23+ million users worldwide (estimation)
- > 1 billion messages per day
- Clients available for Android, iOS, Symbian and Blackberry

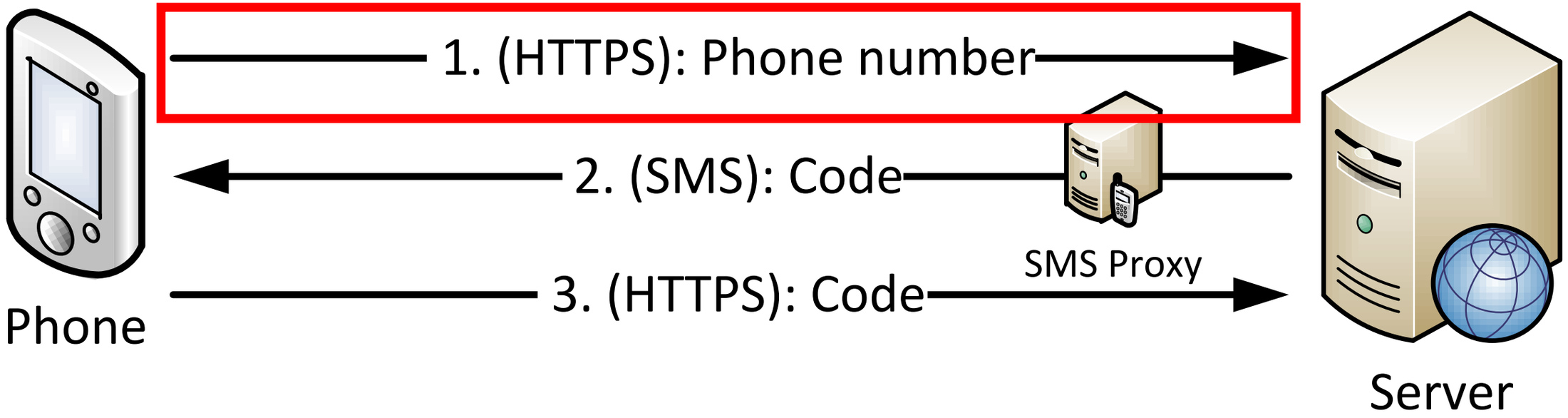


Authentication in WhatsApp

secure sba-research.org

COMET

Competence Centers for Excellent Technologies



Charles 3.5.2 – WhatsApp

Structure | Sequence

- http://crt.tcs.terena.org
- https://s.whatsapp.net
  - client/
    - iphone/
      - smsproxy.php?to=
      - d.php?num=4369
      - smsproxy.php?to=

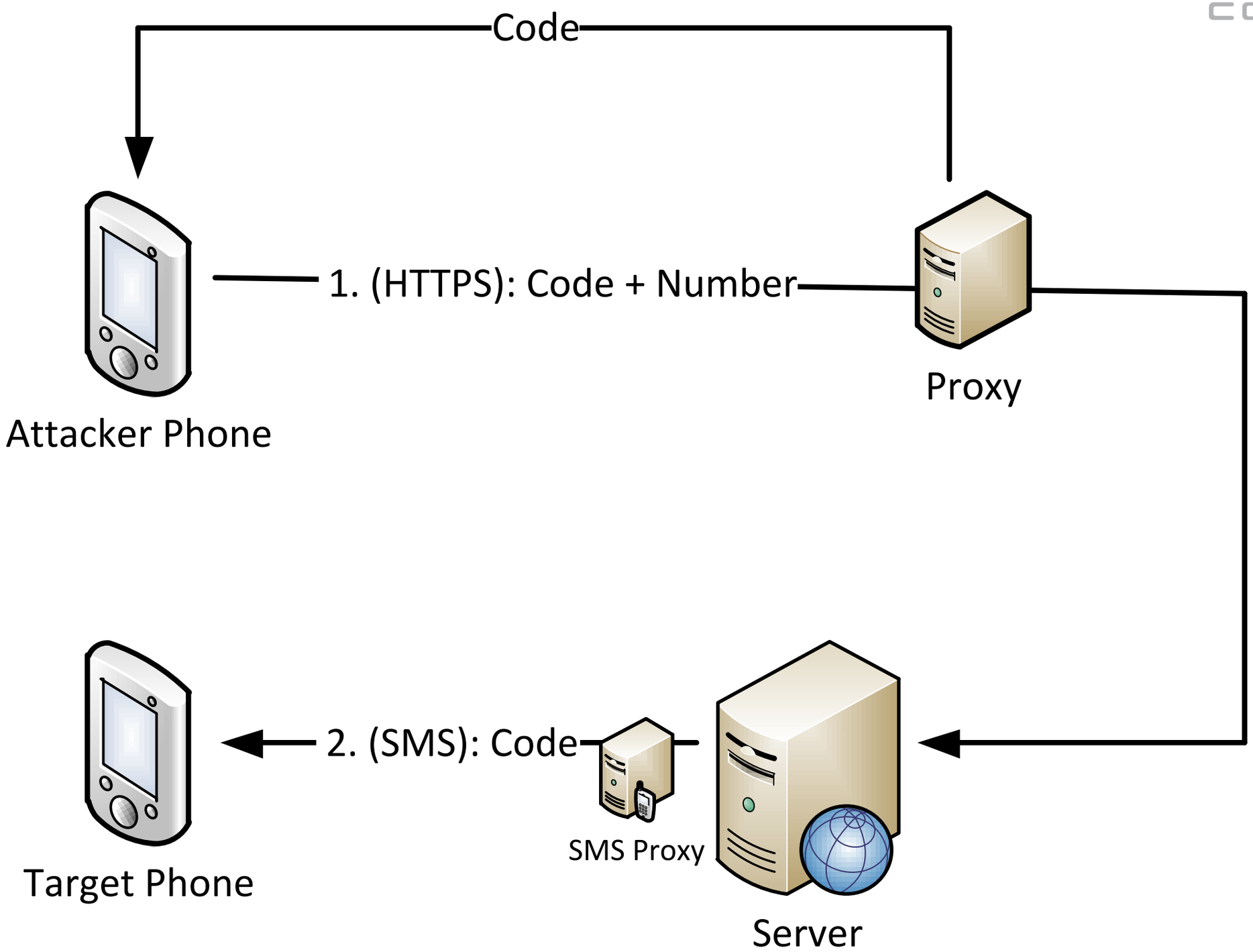
Overview | Request | Response | Summary | Chart | Notes

to	43699
auth	716
in	69
code	43
udid	

Headers | Query String | Raw

Recording Stopped

Breakpoints


Code
1. (HTTPS): Code + Number
Attacker Phone
Proxy
2. (SMS): Code
Target Phone
SMS Proxy
Server

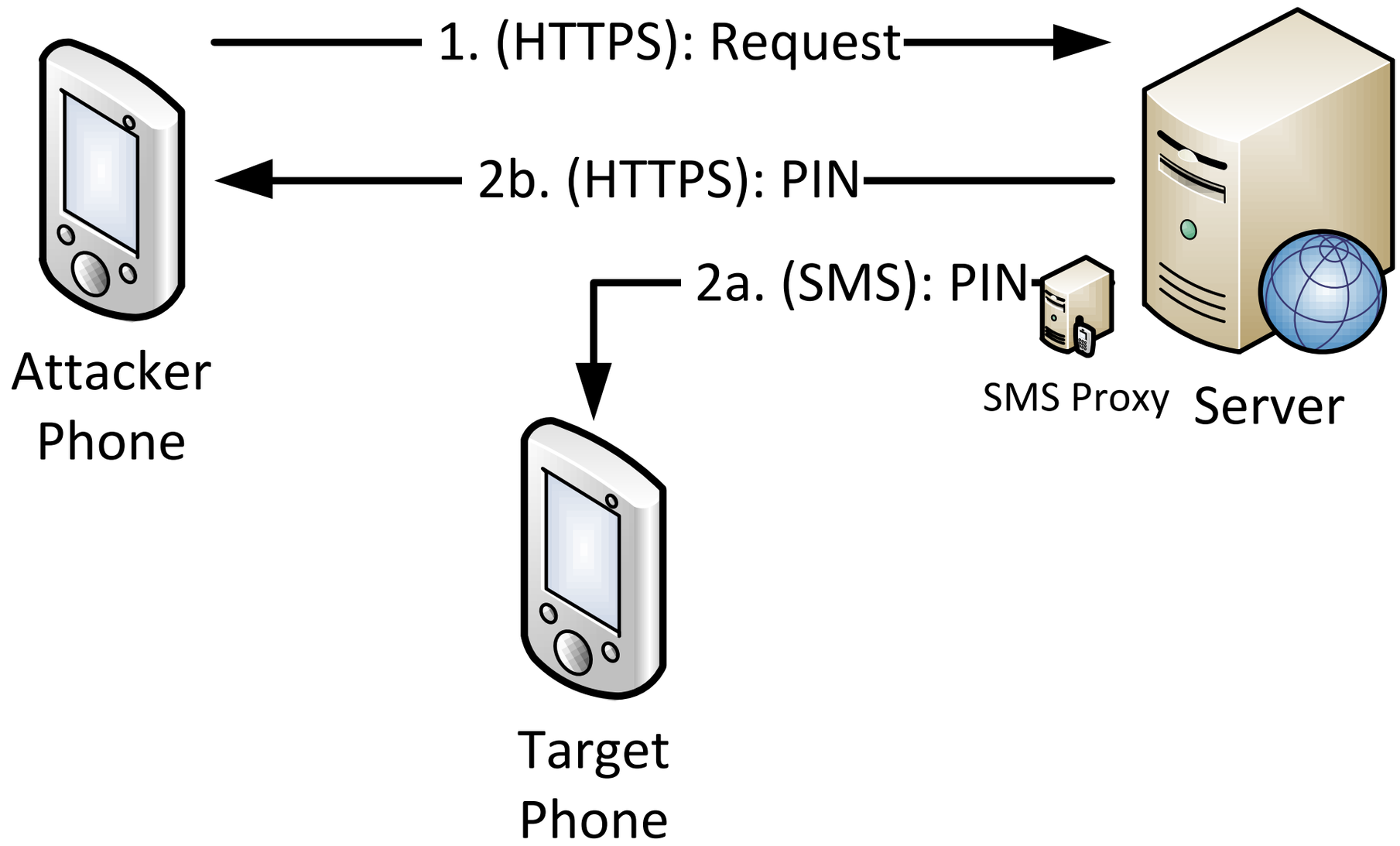
Attack against authentication

- Intercepting the connection between the server and the attacker's phone
- The victim's phone isn't involved in the attack at all
- Similar attacks successful in 6 out of 9 tested applications

secure
sba-research.org

COMET
Competence Centers for
Excellent Technologies

WowTalk



Free SMS

secure
sba-research.org

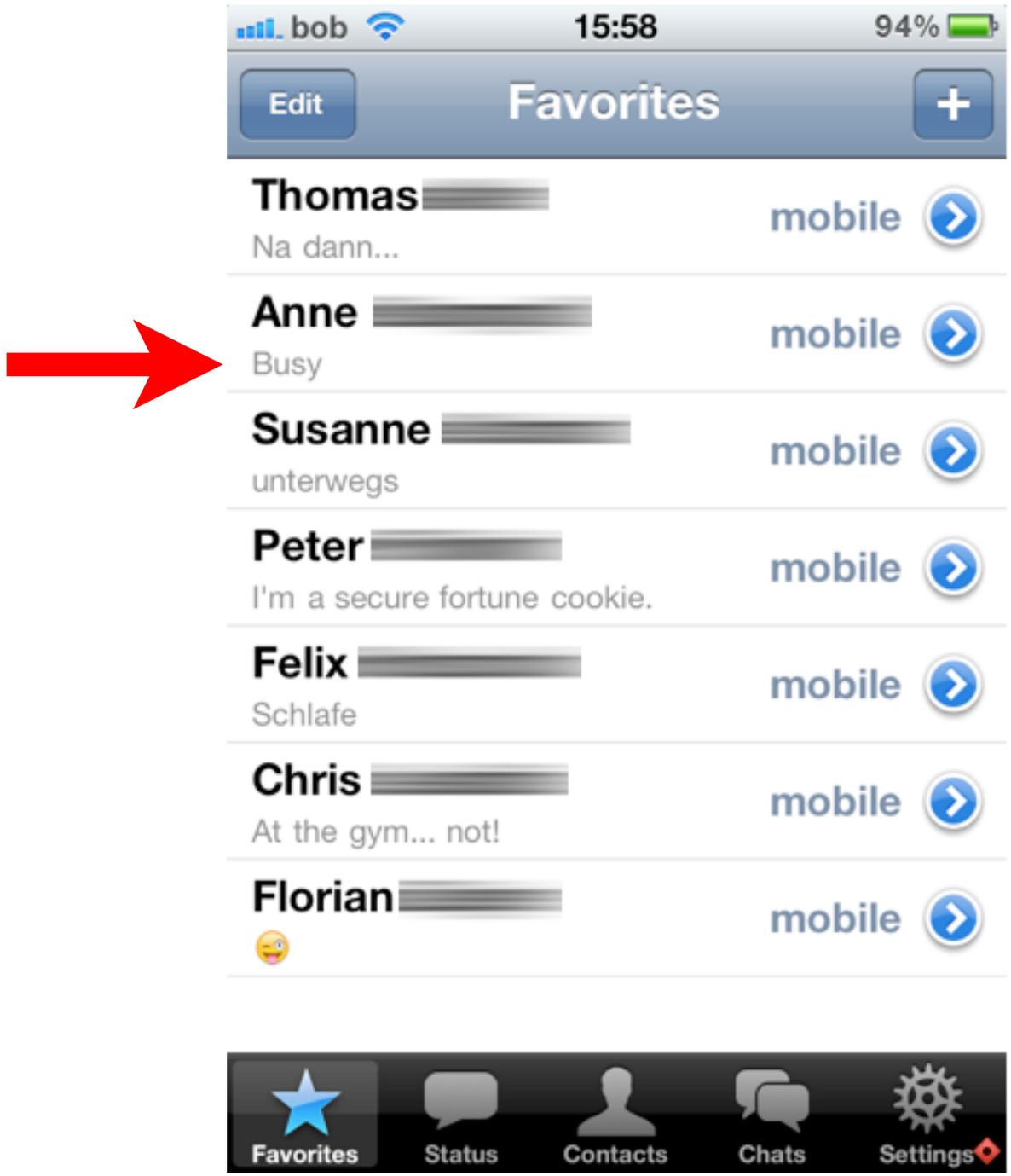
COMET
Competence Centers for
Excellent Technologies

- Authentication code in HTTPS request can be replaced with arbitrary text
- No server-side validation (command injection?)
- Forwarded to SMS proxy and sent via SMS
- Can be misused for sending free SMS

secure
sba-research.org

COMET
Competence Centers for
Excellent Technologies

Status Messages



Charles 3.5.2 – WhatsApp

Structure | Sequence

- http://crt.tcs.terena.org
- https://s.whatsapp.net
  - client/
    - iphone/
      - smsproxy.php?to=
      - d.php?num=4369
      - smsproxy.php?to=
      - u.php
    - tropo/
- https://xmpp-reg.whatsapp.
- https://sro.whatsapp.net

Overview | Request | Response | Summary | Chart | Notes

cc	43
me	+43680
s	Sleeping

cc 43
me +43680
s Sleeping

Headers | Text | Hex | Form | Raw

Recording Stopped

Breakpoints

secure
sba-research.org

COMET

Competence Centers for
Excellent Technologies

```
https://s.whatsapp.net/client/iphone/u.php?
cc=countrycode&me=phonenumber&s=statusmessage
```

User Enumeration

secure sba-research.org

COMET Competence Centers for Excellent Technologies

- Applications upload the user's address book to the server
- Server compares the contained phone numbers to already registered phone numbers
- Server returns a subset list containing only phone numbers that are registered
- Entire user base enumeration?

Austria

secure
sba-research.org

COMET
Competence Centers for
Excellent Technologies

- A1, Orange and T-Mobile
- Number ranges
  - +43664XXXXXXX
  - +436991XXXXXXX
  - +43676XXXXXXX
- 30 million (possible) phone numbers
- WhatsApp returned a subset containing 182.793 (active) phone numbers

secure
sba-research.org

COMET

Competence Centers for
Excellent Technologies

Gerade beim nix tun!!! ;-)

Bei der Arbeit

@ kiino mit schattz <3

Meditation

Schlafe

beim Golfen

Und wieder Training...
Bin so brav hi :-p

Klimakonferenz

In Mondsee
auf Urlaub

Results

secure sba-research.org

COMET Competence Centers for Excellent Technologies

	Account Hijacking	Spoofing/ Manipulation	Unrequested SMS	Enumeration	Other Vulnerabilities
WhatsApp	yes	no	yes	yes	yes
Viber	no	no	yes	yes	no
eBuddy XMS	no	no	yes	yes	no
Tango	yes	no	yes	yes	no
Voypi	yes	yes	yes	yes	yes
Forfone	no	yes	yes	yes	no
HeyTell	yes	no	no	limited	no
EasyTalk	yes	no	yes	yes	no
Wowtalk	yes	no	yes	yes	yes

Responsible Disclosure

secure sba-research.org

COMET

Competence Centers for Excellent Technologies

- Research between spring and fall 2011
- Vendors notified in November 2011
- Vulnerabilities weren't made public until NDSS
- WhatsApp fixed some vulnerabilities:
  - Account hijacking & free SMS
  - (Modifying status messages)

TEST

Schwere Sicherheitslücken in Messenger-Apps

Messenger-Apps wie WhatsApp können ein großes Sicherheitsrisiko für deren Benutzer darstellen. Forschern des SBA Research haben in einem Vergleichstest neun Apps untersucht und konnten nicht nur Accounts übernehmen, sondern auch SMS auf Kosten von WhatsApp verschicken.

07.02.12, 20:00
futurezone

1

Das Wiener Institut SBA Research hat in einem Vergleichstest massive Sicherheitslücken in aktuellen Messenger-Apps wie WhatsApp entdeckt. WhatsApp ist derzeit allein in Österreich auf über 180.000 Geräten installiert, wies aber im Test erhebliche Mängel auf. So konnten die Forscher nicht nur den Account übernehmen, sondern auch kostenlose SMS vom Server von WhatsApp verschicken. Dasselbe war

Conclusions

secure
sba-research.org

COMET
Competence Centers for
Excellent Technologies

- 6 out of 9 tested applications have broken authentication mechanisms
- Many other vulnerabilities
- All identified flaws stem from well-known software design and implementation errors
  - Trusting the client
  - No input validation
  - No/weak authentication mechanisms