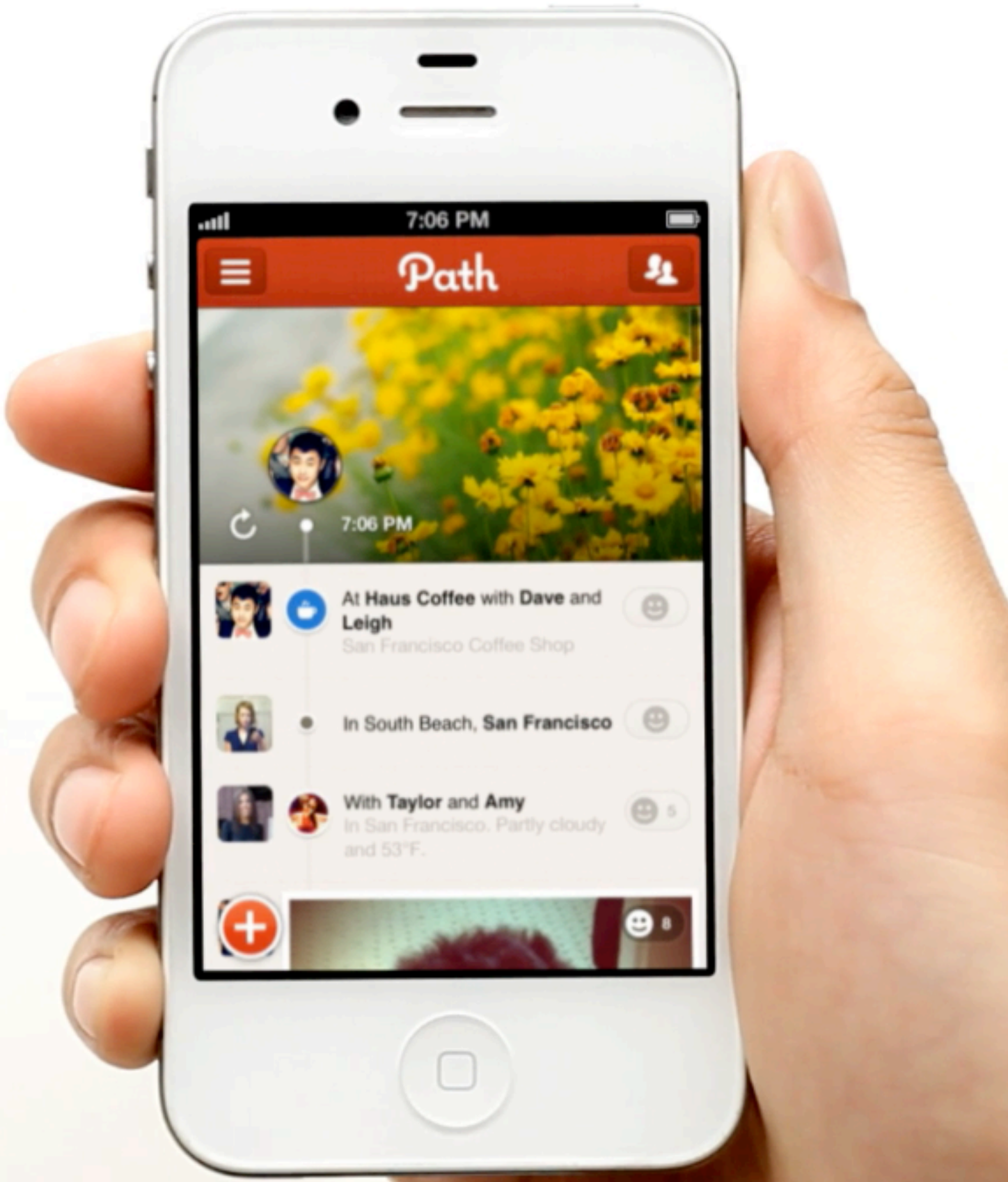
TelcoSecDay @ Troopers · 3/20/12 · Heidelberg, Germany

Guess Who's Texting You?

Evaluating the Security of Smartphone Messaging Applications

Sebastian Schrittwieser

SBA Research, Vienna, Austria



Source: path.com

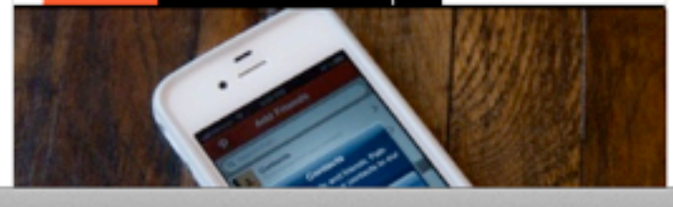
APPLE APPS & SOFTWARE

71 COMMENTS

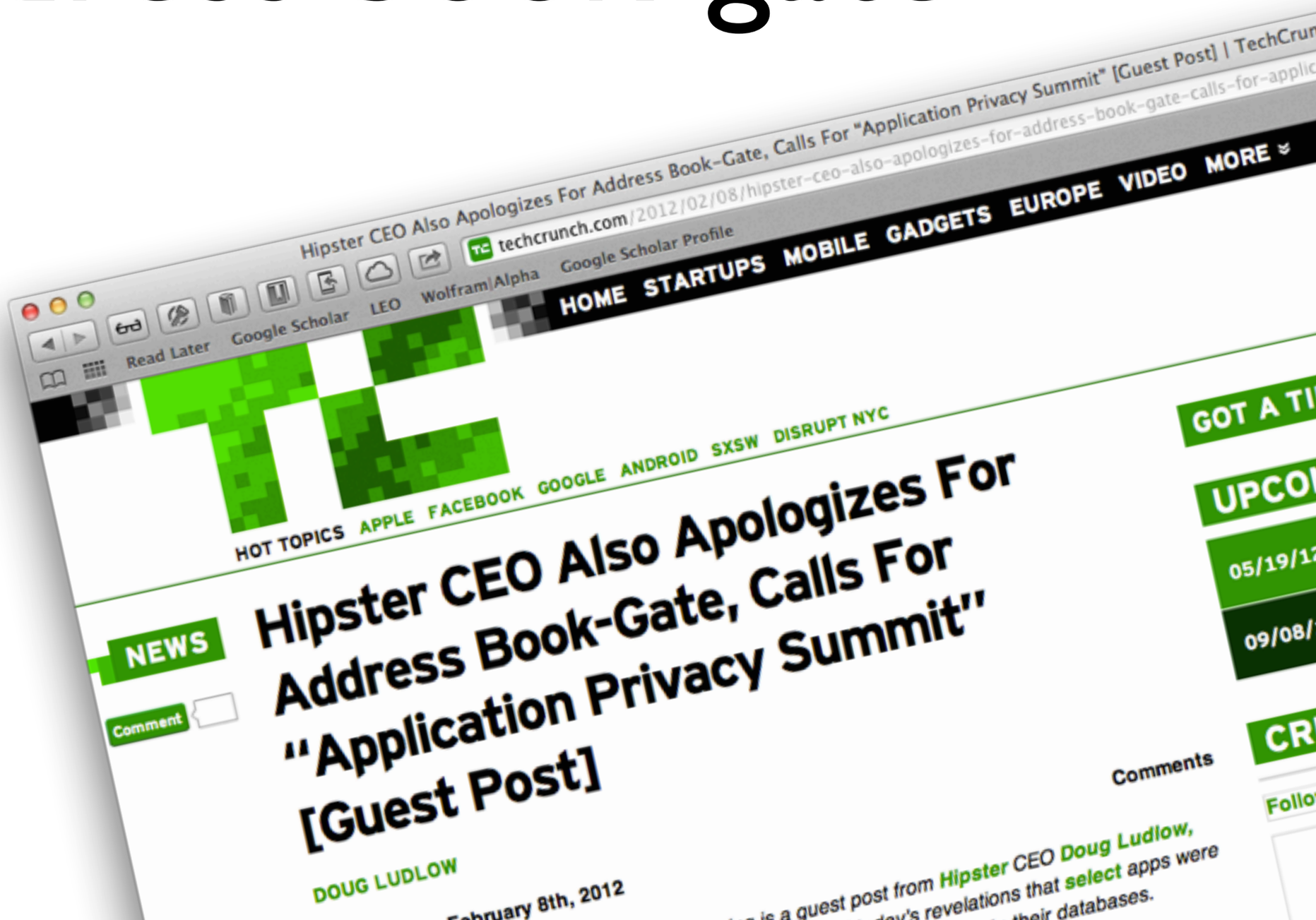
Path iOS app uploads your entire address book to its servers

By Adi Robertson on February 7, 2012 06:18 pm

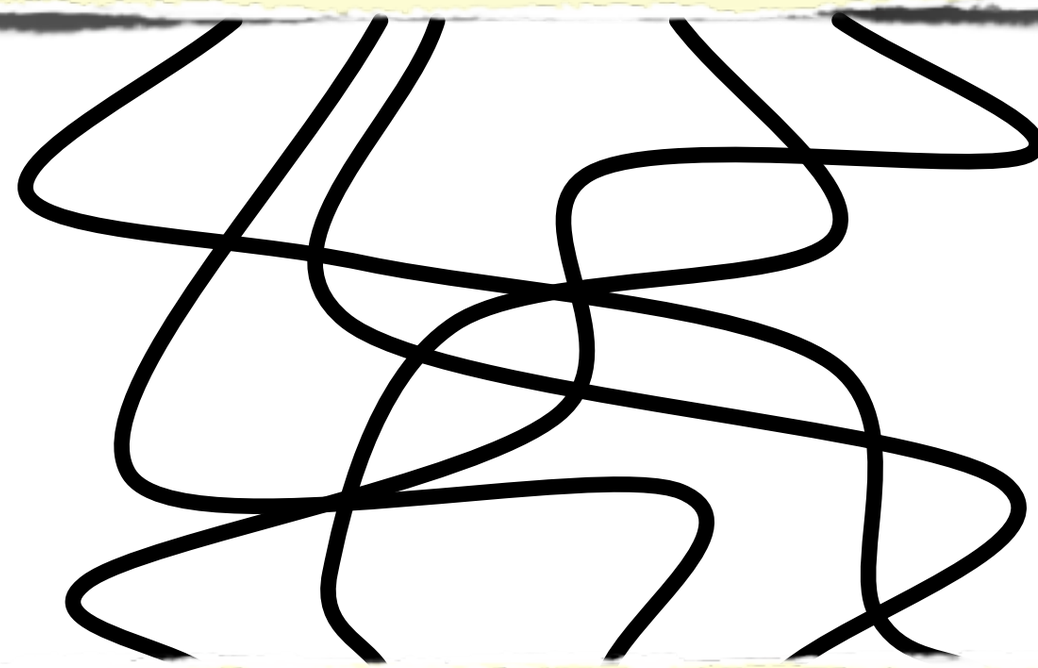
PART OF THIS STORYSTREAM 1



address book-gate



android.permission.READ_CONTACTS
android.permission.READ_CALENDAR

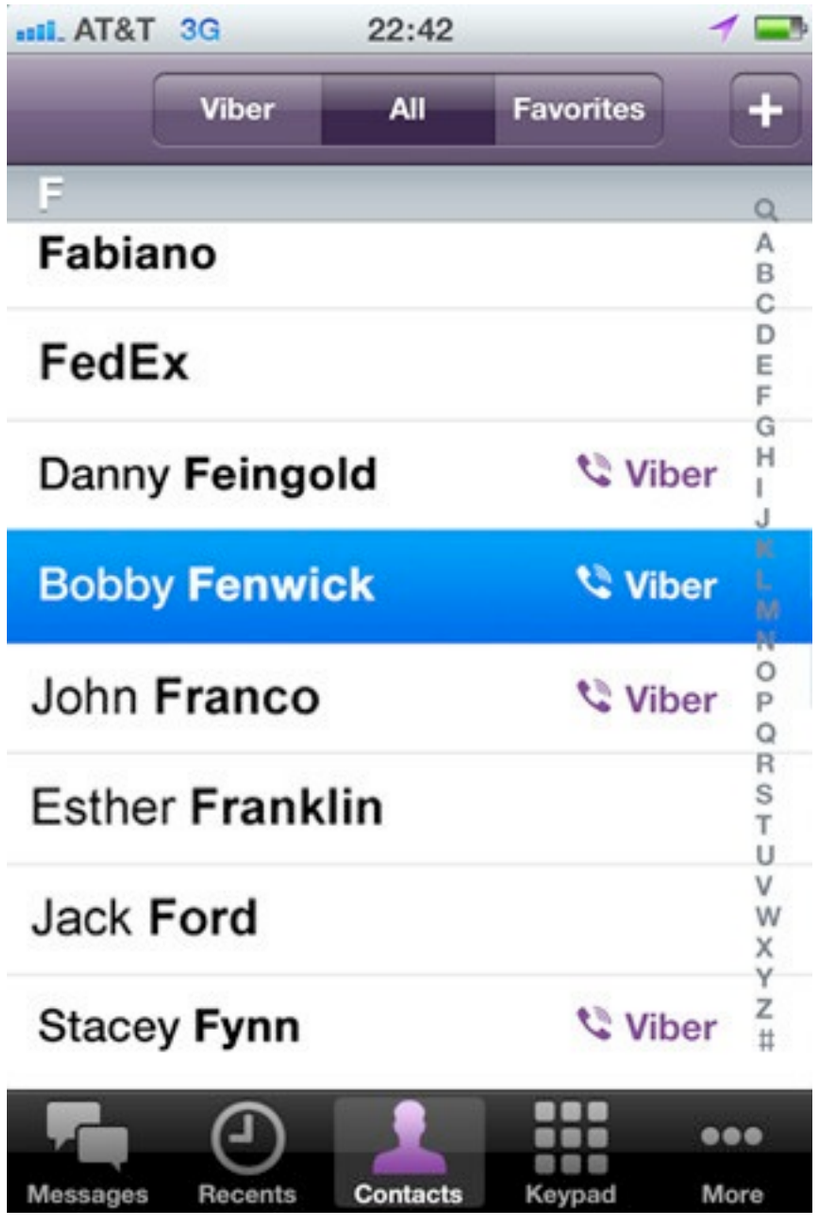


android.permission.INTERNET

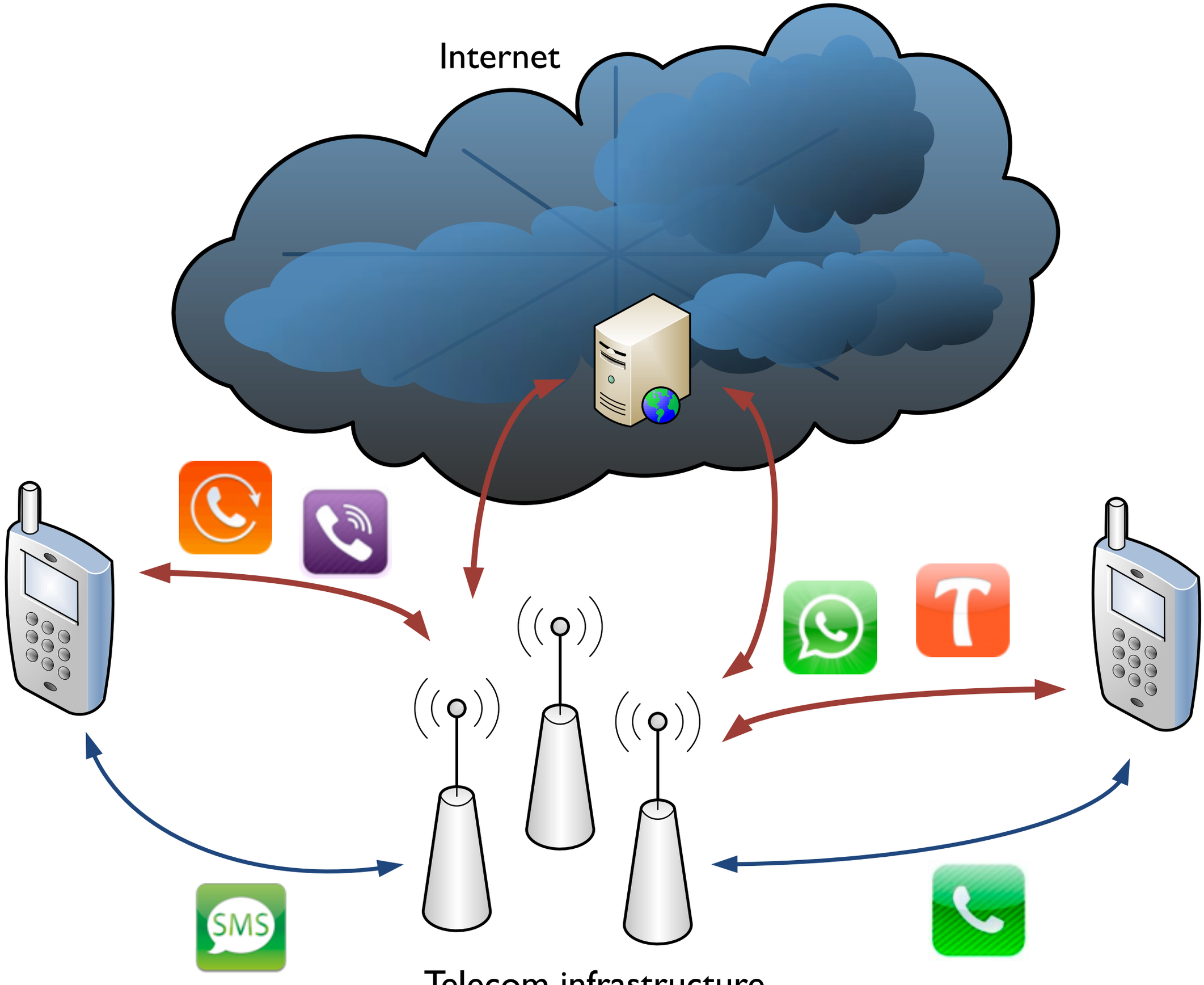
Analyzing network traffic of smartphones

- Data flow analysis
- Security evaluation
- Example: Smartphone Messengers

Smartphone Messaging



- 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


Internet
SMS
Telecom infrastructure

Motivation

	Traditional SMS/talk	Messenger/VoIP Apps
Protocol	proprietary	HTTP(S), XMPP
Security	cryptographically sound authentication (SIM card)	application depended, much weaker authentication (phone number, IMSI, UDID)
Users' perception	SMS/talk	

Evaluation

Authentication Mechanism and Account Hijacking

Sender ID Spoofing / Message Manipulation

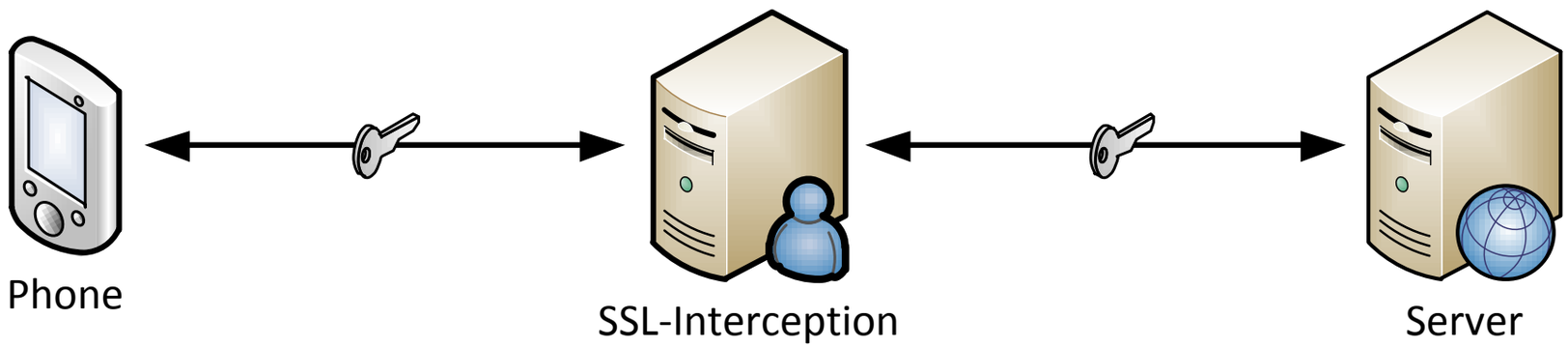
Unrequested SMS / phone calls

User Enumeration

Modifying Status Messages

Experimental Setup

- 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)!

Certificates?


3 AT 3G
09:38
25 %
Installing Profile
Charles Proxy SSL...
Not Trusted
Install
Unverified Profile
Received 14.03.2012
The authenticity of “Charles Proxy SSL Proxying” cannot be verified.
Contains Certificate
Installing this profile will change settings on your iPhone.
More Details
Cancel
Install Now

WhatsApp

eBuddy XMS

WowTalk

Viber

HeyTell

Forfone

Voypi

Tango

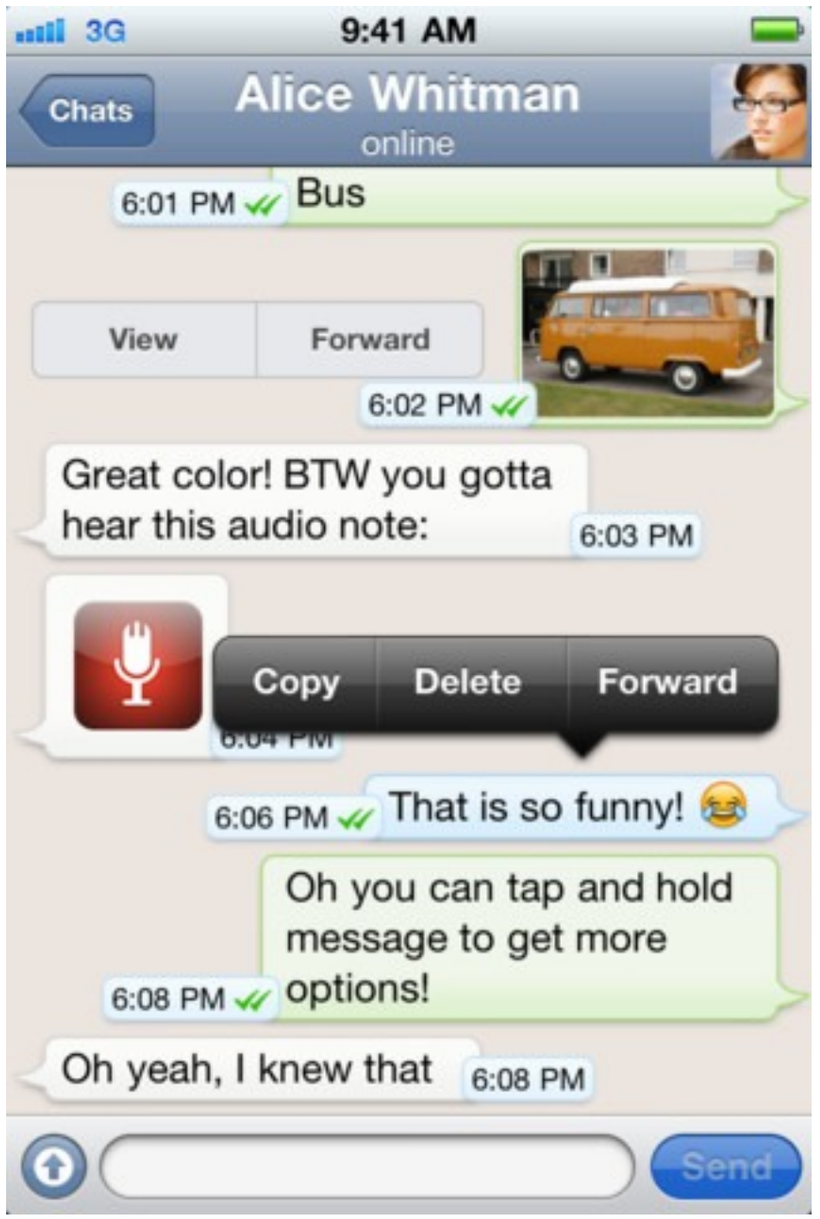
EasyTalk

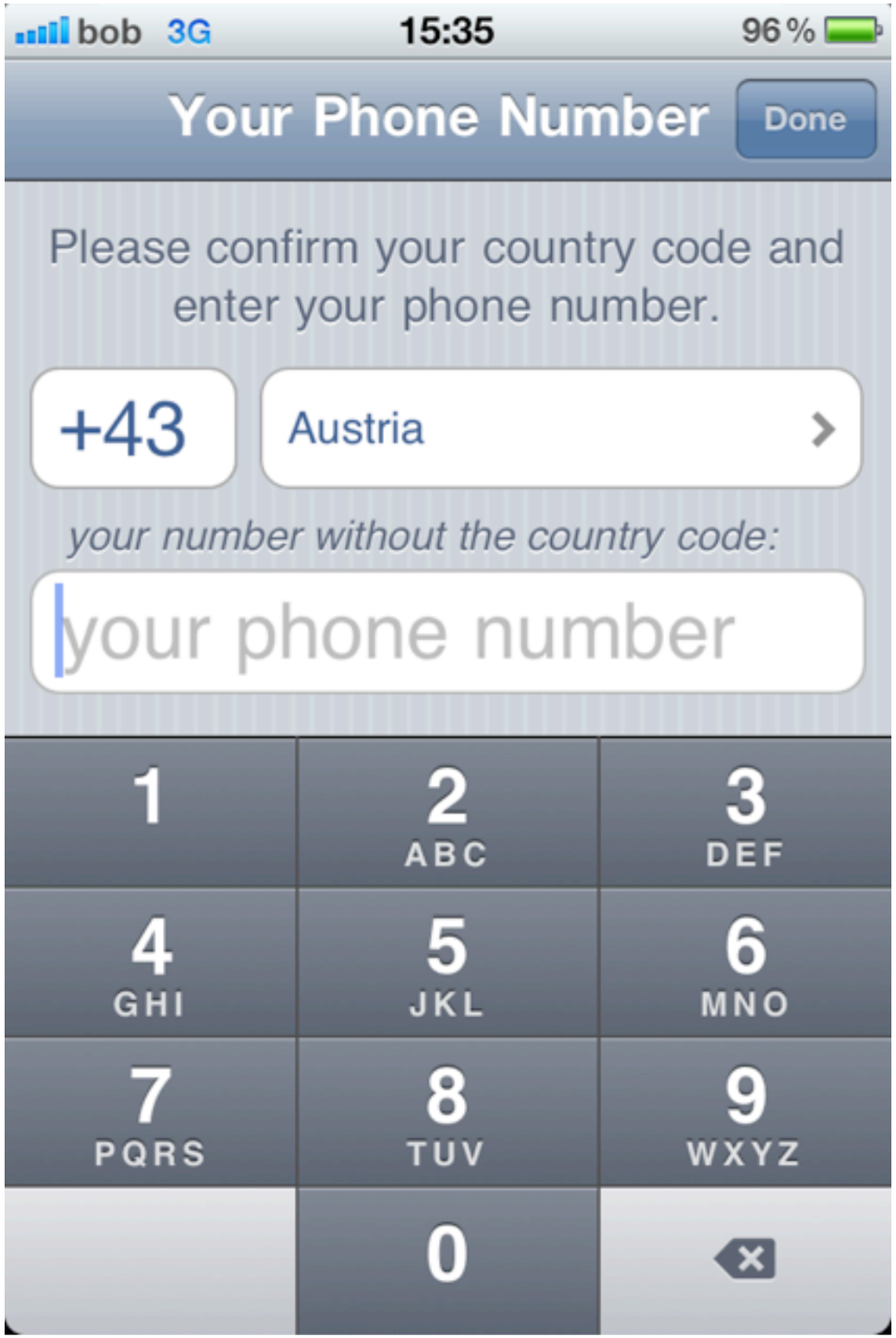
WhatsApp

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

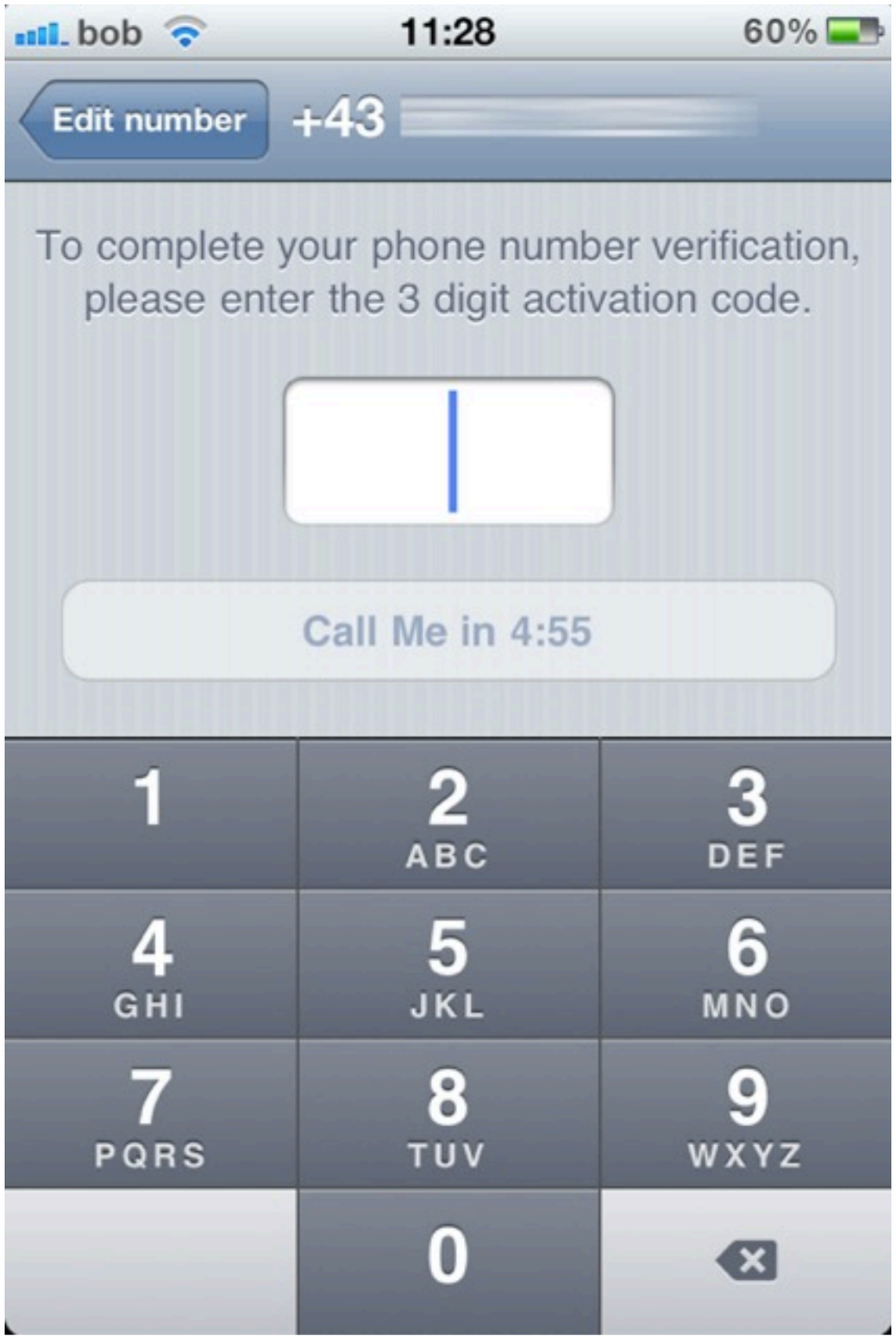
WhatsApp

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

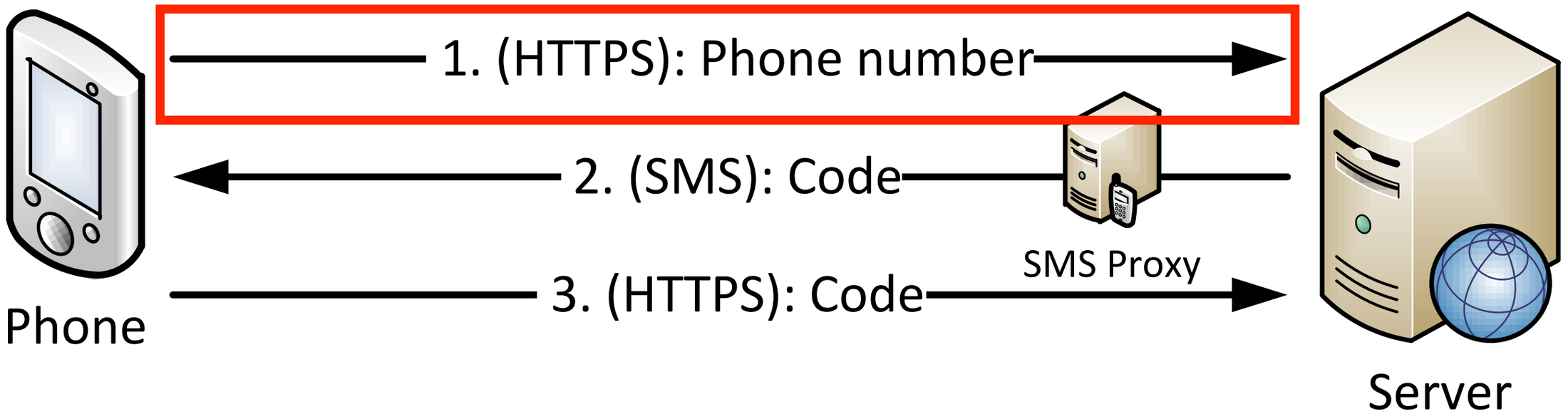



bob 3G
15:35
96 %
Your Phone Number
Done
Please confirm your country code and enter your phone number.
+43
Austria
your number without the country code:
your phone number
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0


bob 3G
15:42
95 %
Messages
+41 79 807 30…
Edit
Call
FaceTime
Add Contact
Text Message
11.07.2011 15:19
WhatsApp code 393
Text Message
Send


bob
11:28
60%
Edit number
+43
To complete your phone number verification, please enter the 3 digit activation code.
Call Me in 4:55
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0

Authentication in WhatsApp



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

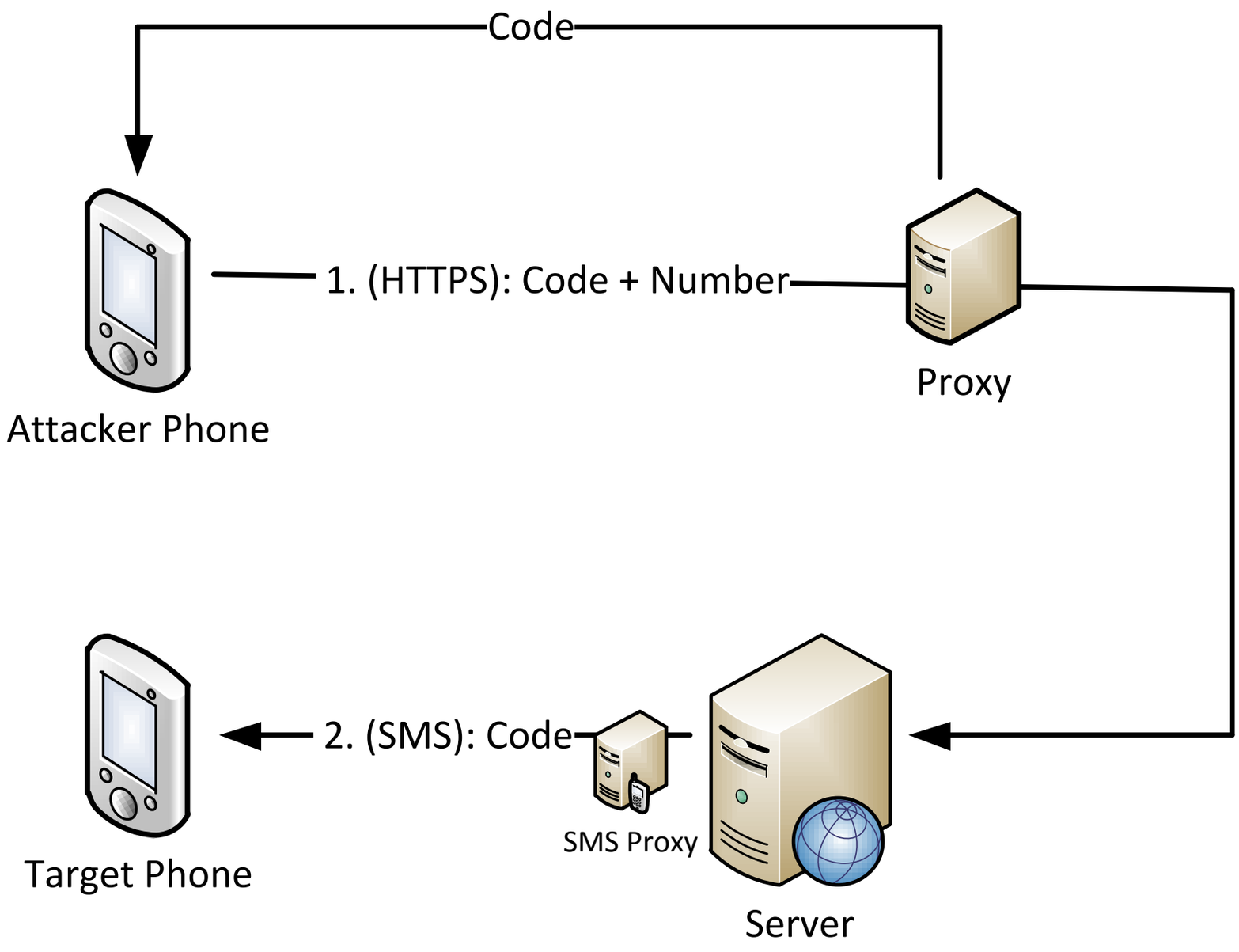
to	43699
auth	716
in	69
code	43
udid	

Headers | Query String | Raw

Recording Stopped

Breakpoints

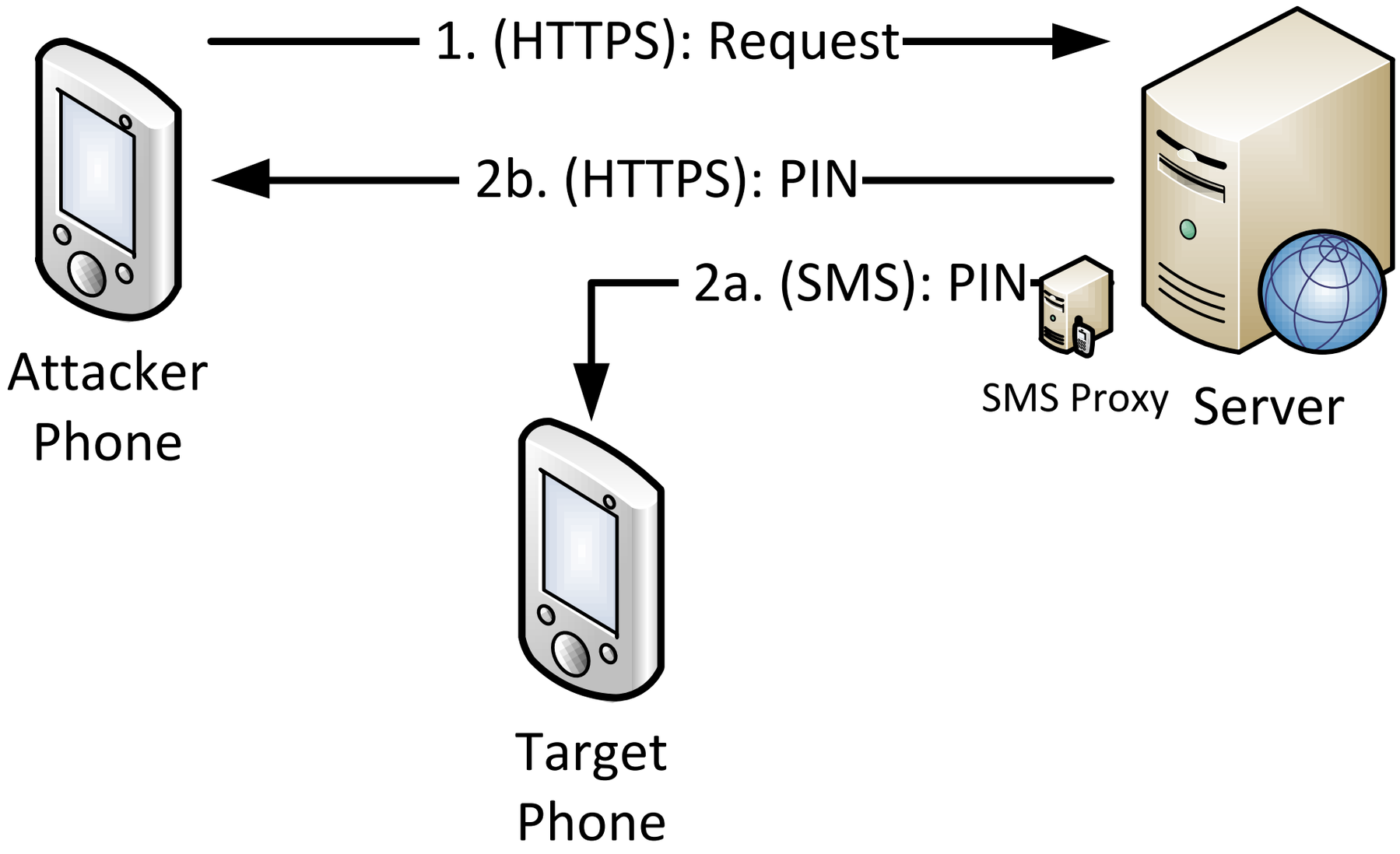
Attack against authentication



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

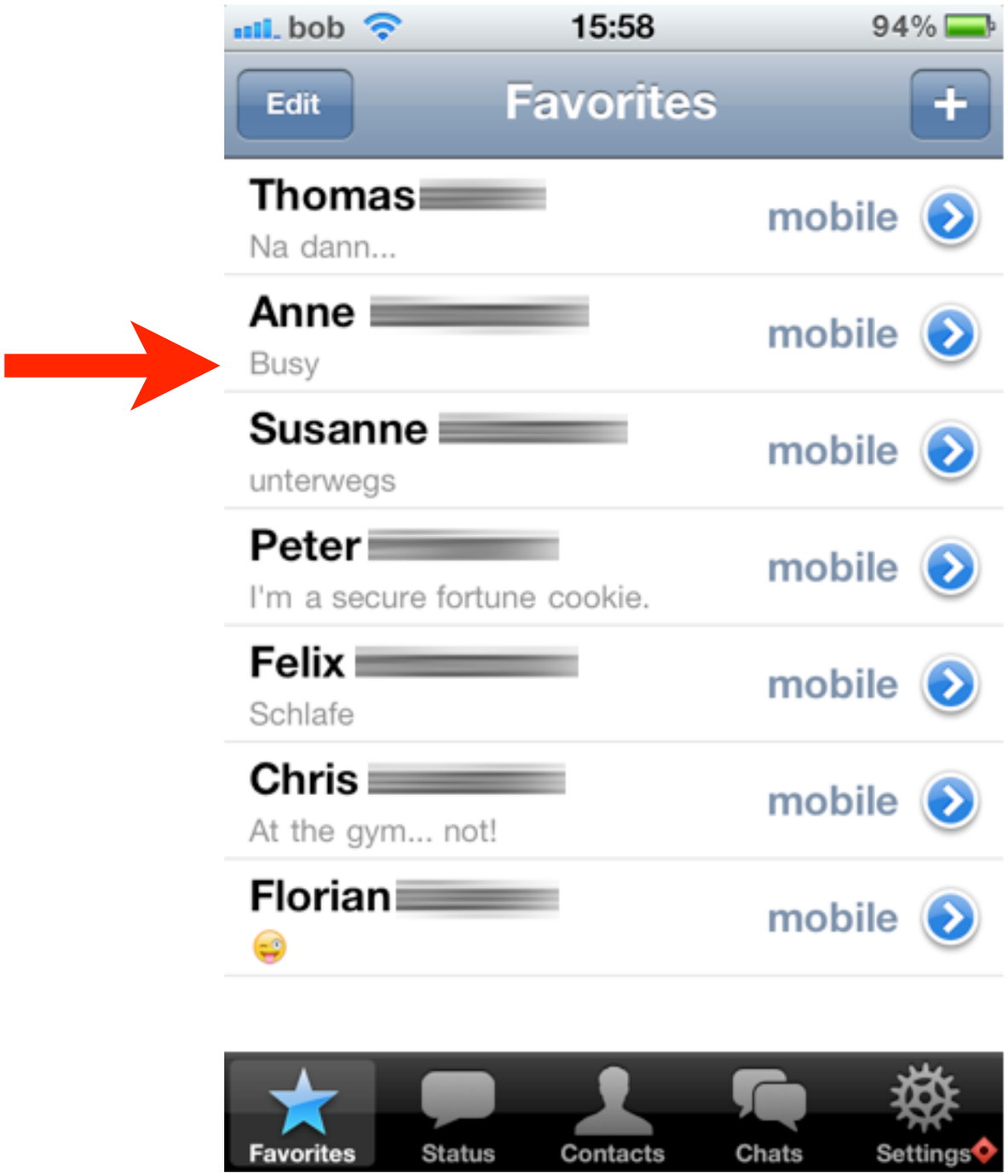
WowTalk


1. (HTTPS): Request
2b. (HTTPS): PIN
2a. (SMS): PIN
Attacker Phone
Target Phone
SMS Proxy
Server

Free SMS (WhatsApp)

- 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

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

Headers | Text | Hex | Form | Raw

Recording Stopped

Breakpoints

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

Sender ID spoofing

- Example: Forfone
  - Messages are authenticated by IMSI (Android) or UDID (iOS)
  - Both numbers can be accessed by 3rd party applications
- Voypi: no authentication at all

User Enumeration

- 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?

User Enumeration

- US area code 619 (Southern San Diego)
- Number range: +1 (619) XXXXXXX
- 10 million possible phone numbers
- WhatsApp returned a subset containing 21.095 (active) phone numbers

On vacation

Sleeping

At work ... Bleh.

Missing my love!

Heartbroken

Nicaragua in
4 days!!

On my way to Ireland!

9420-5794-3731-1793-7083

I’m never
drinking again

Phone DETECTIVE

Search Successful! Results For 619-[redacted]

Number:	619-[redacted]
Search Date:	Thursday, January 26, 2012 1:09 AM
Location:	La Mesa, CA
Full Results:	Available

Full Report includes available information for:

- Owner's name and address
- Household members
- People search results
- And more!

Click "Continue" to view the Full Phone Report for 619-[redacted]

Continue

< Run Another Search

Full Reports include all available information about an owner's name and address. Some numbers do not have owner information in which case you will be entitled to a credit.

User Enumeration

- Entire Austria (population: 8.3 million)
- 4 carriers, 12.3 million SIM cards
- Uploaded entire number range in chunks of 5000 numbers each
- Server returned 182.793 WhatsApp users (phone number + status message) in less than 5 hours

Results

	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

- 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)

Conclusions

- 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

Conclusions

- SSL interception is an easy way for doing data flow analysis in smartphone applications
- Cannot detect well-hidden data leakage
  - Steganography
  - Additional encryption layer on top of SSL
- ... but can help to understand and evaluate software