Is Security an Afterthought when Designing Apps?

SBA Research – Vienna University of Technology
Edgar R. Weippl

Apps, Mobile Devices, Cloud Services

- So many new opportunities
- Building on experience of previous decades
- Things can only get better
- Really?

Data Storage

Simple systems

- FTP, WebDAV, NFS

A little more complex

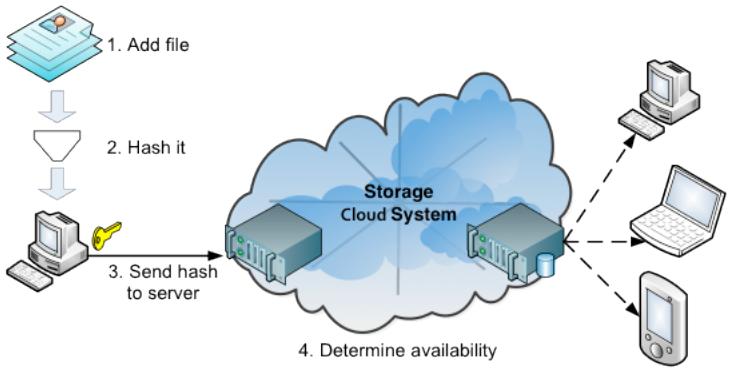
- Delta sync
- P2P

More complex systems

Name	Protocol	Encrypted transmission	Encrypted storage	Shared storage
Wuala	Cryptree	yes	yes	yes
SpiderOak	proprietary	yes	yes	yes
Ubuntu One	u1storage	yes	no	yes
Dropbox	proprietary	yes	no	yes

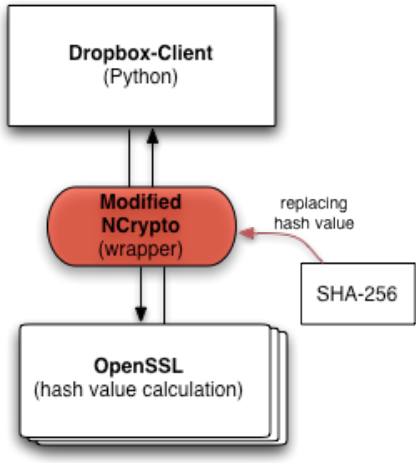
Data Deduplication

- At the server
  - Same file only stored once
  - Save storage space at server
- At the client
  - Calculate hash or other digest
  - Reduce communication



Attacks

- Hash manipulation
- Stolen Host ID
- Direct Up-/Download
  - Uploading without linking
  - Simple HTTPS request https://dl-clientXX.dropbox.com/store



Evaluation

Time until (hidden) chunks get **deleted**:

- Random data in multiple files
- Hidden upload: at least 4 weeks
- Regular upload: unlimited undelete possible (> 6 months)

Popular files on Dropbox:

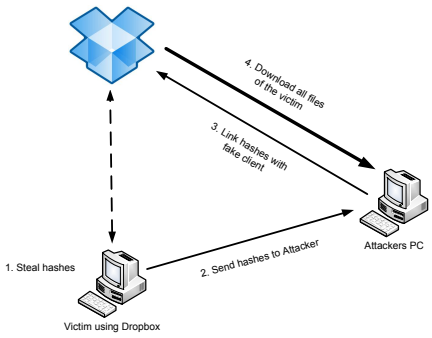
- thepiratebay.org Top 100 Torrent files
- Downloaded copyright-free content (.sfv, .nfo, ...)
- 97 % (n = 368) were retrievable
- 20 % of torrents were less than 24 hours old

Interpretation:

- At least one of the seeders uses Dropbox

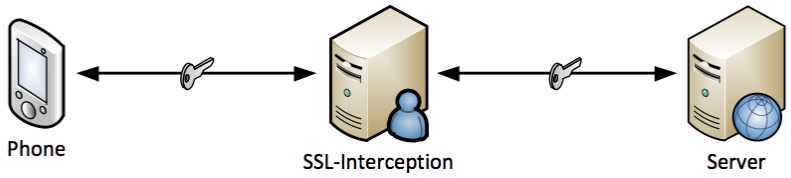
Solutions

- Aftermath – Dropbox fixed the flaws
  - HTTPS Up-/Download Attack
  - Host ID is now encrypted
  - No more client-side deduplication
    - Proof of ownership
    - Take down notice

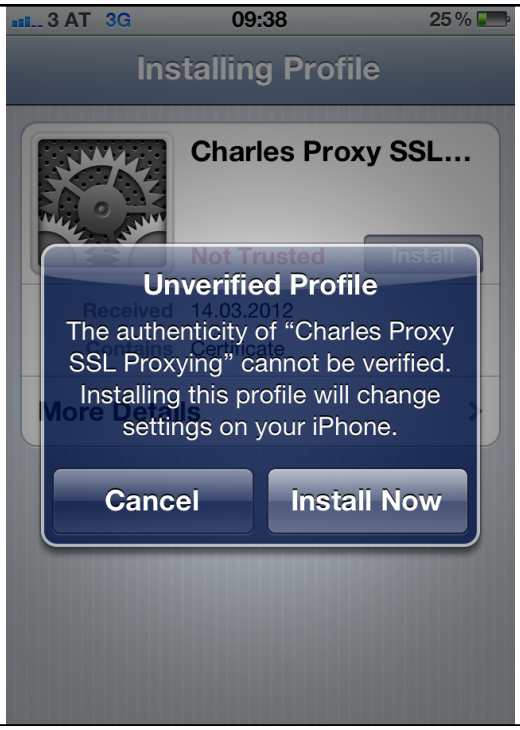


WhatsApp

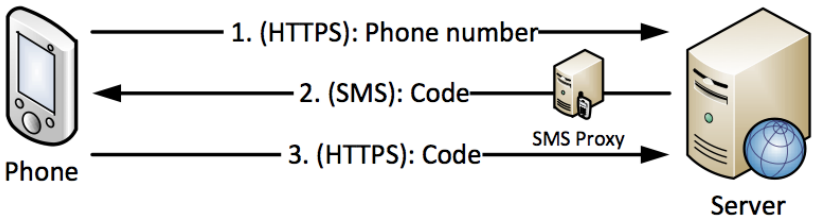
Man-in-the-Middle

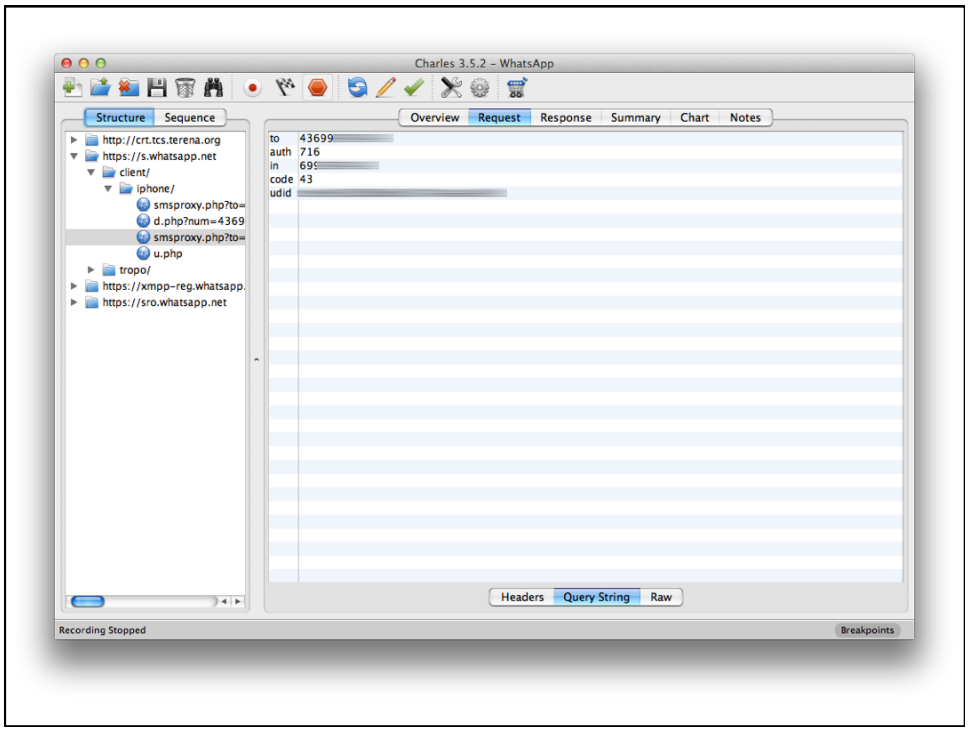


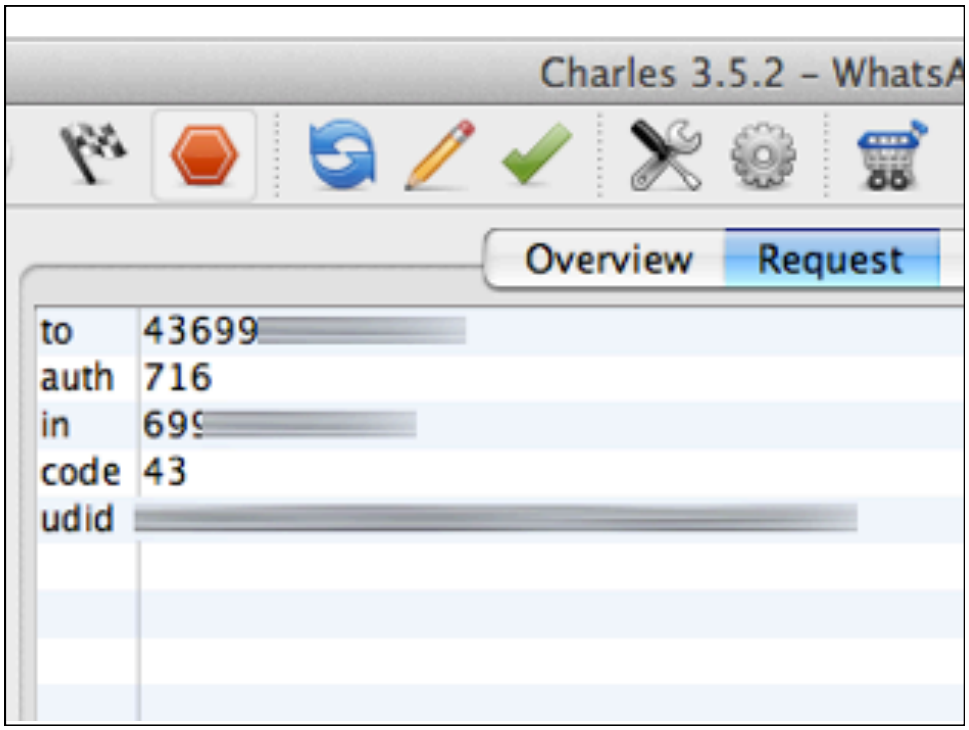
Certificates?



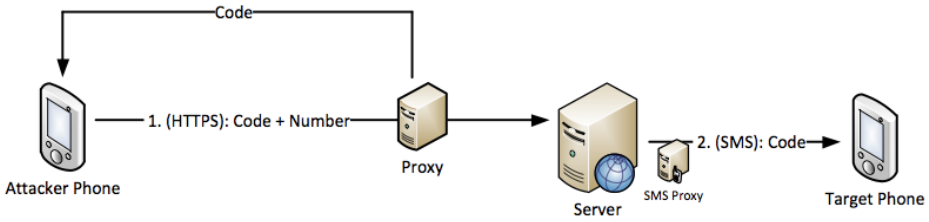
Authentication



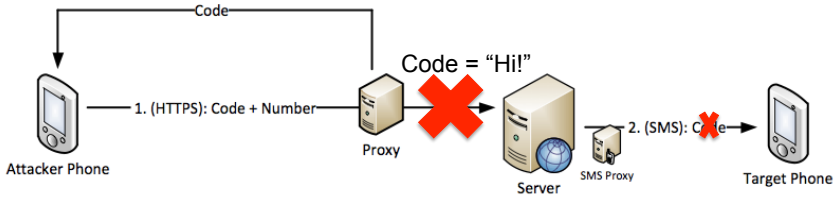

Charles 3.5.2 – WhatsApp
Structure
Sequence
http://crt.tcs.terena.org
https://s.whatsapp.net
client/
iphone/
smsproxy.php?to=
d.php?num=4369
smsproxy.php?to=
u.php
tropo/
https://xmpp-reg.whatsapp.
https://sro.whatsapp.net
Overview
Request
Response
Summary
Chart
Notes
to 43699
auth 716
in 69
code 43
udid
Headers
Query String
Raw
Recording Stopped
Breakpoints


Charles 3.5.2 – WhatsA
Overview
Request
to 43699
auth 716
in 69
code 43
udid

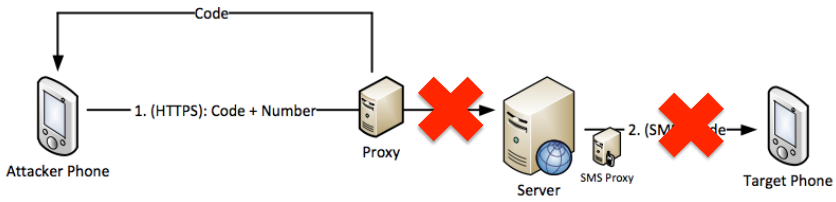
In Reality



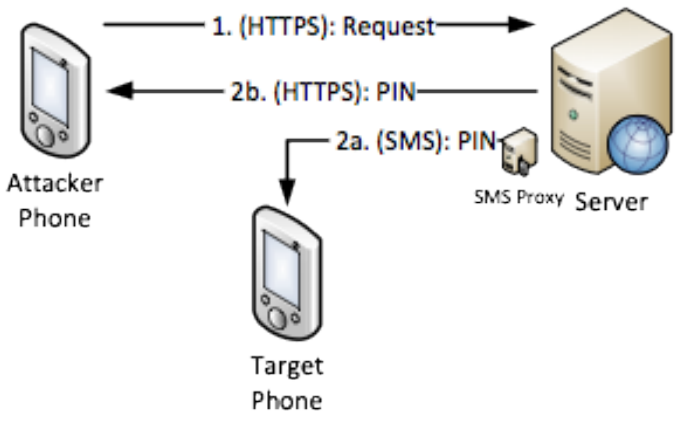
Even Worse



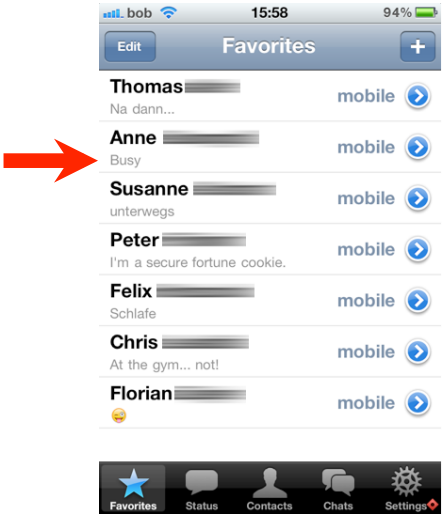
Completely Stealthy

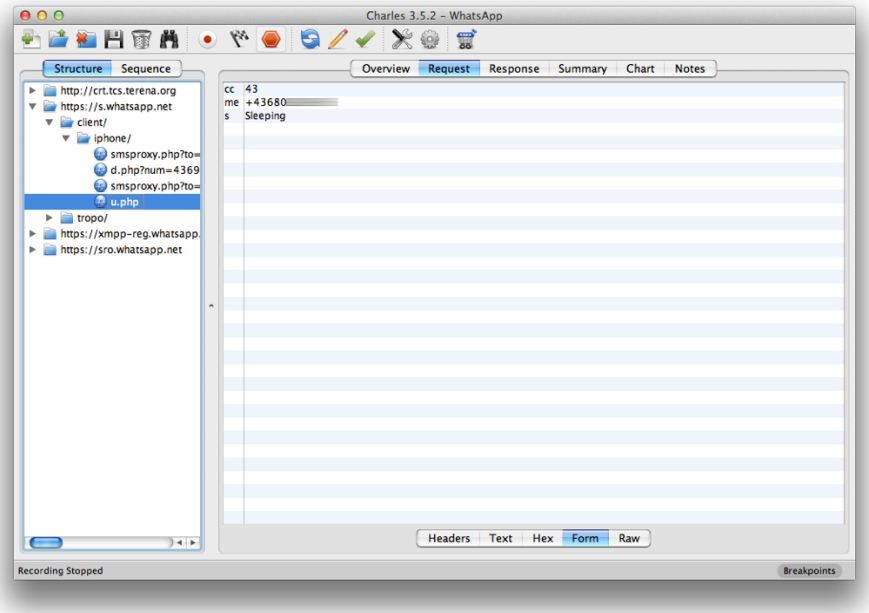


WowTalk



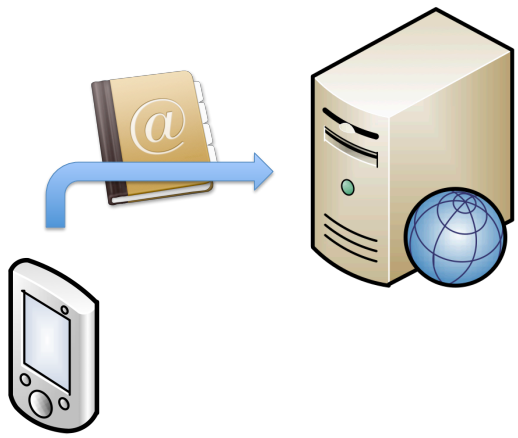
Status Messages



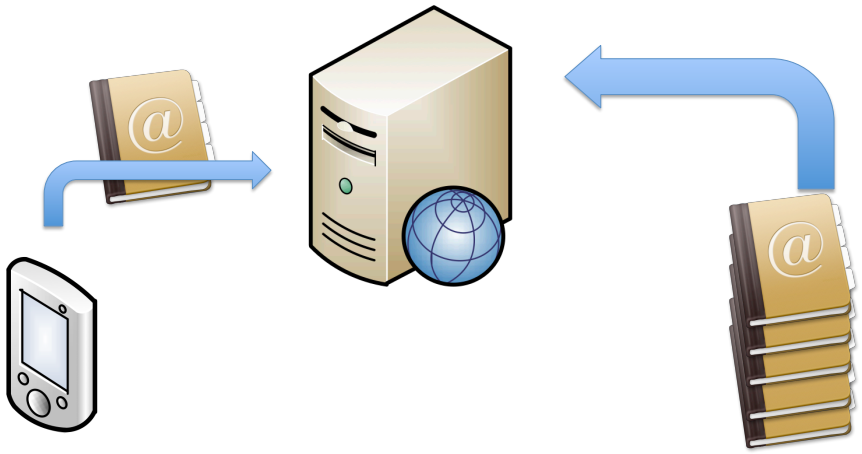


https://s.whatsapp.net/client/iphone/u.php?cc=countrycode&me=phonenumber&s=statusmessage

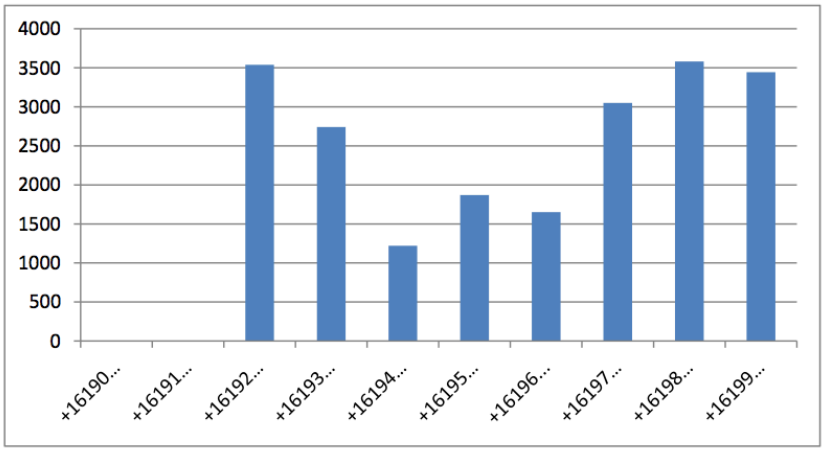
Enumeration Attack

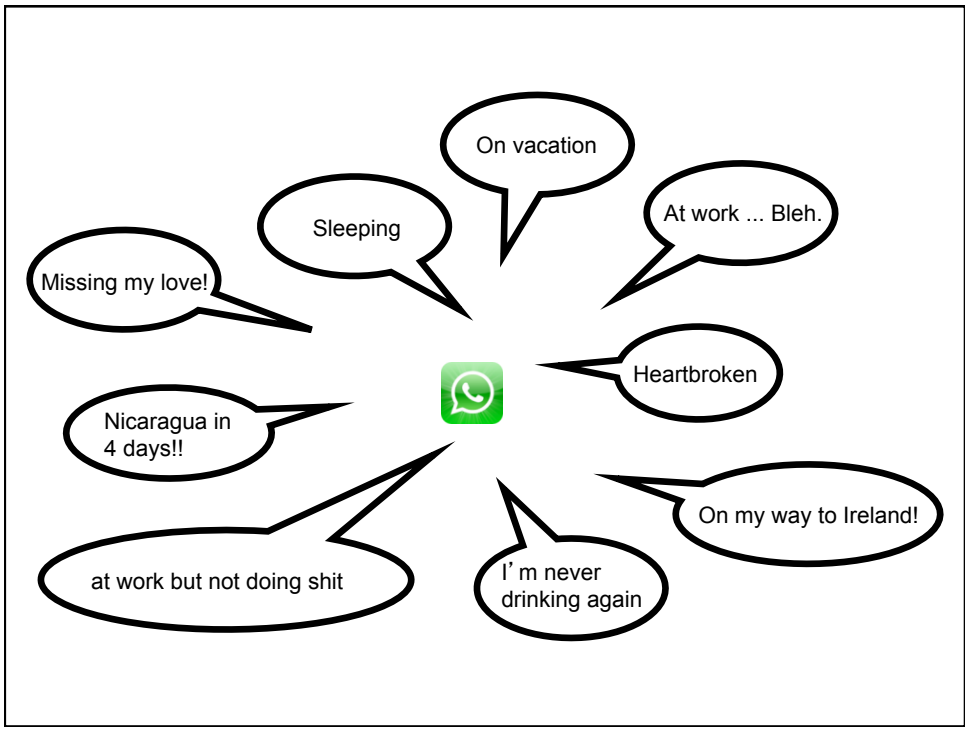


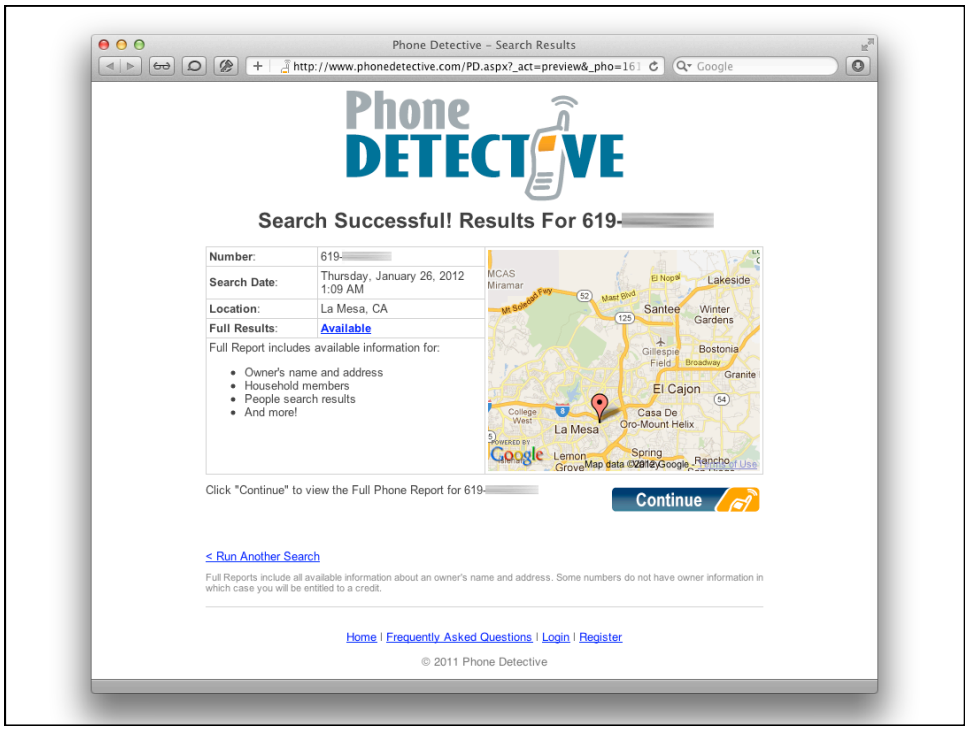
Enumeration Attack

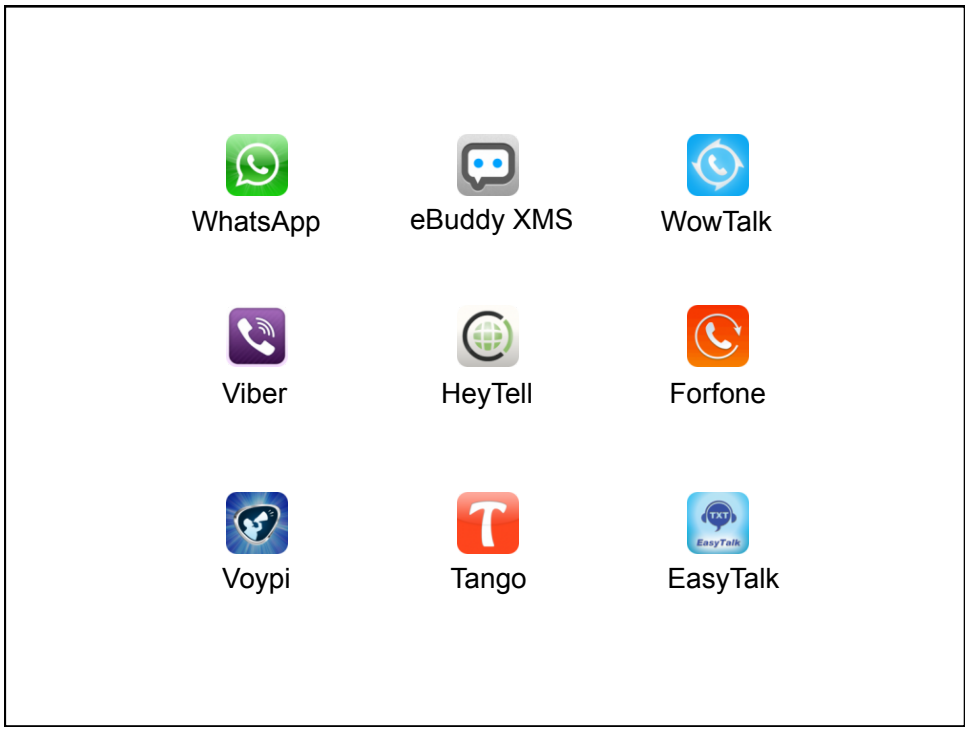


Enumeration Attack




On vacation
Sleeping
At work ... Bleh.
Missing my love!
Heartbroken
Nicaragua in 4 days!!
On my way to Ireland!
at work but not doing shit
I' m never drinking again


Phone Detective - Search Results
http://www.phonedetective.com/PD.aspx?_act=preview&_pho=161
Google
Phone DETECTIVE
Search Successful! Results For 619-
Number: 619-
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!
MCAS Miramar
Lakeside
Santee
Winter Gardens
Bostonia
Granite
El Cajon
Casa De Oro-Mount Helix
La Mesa
Lemon Grove
Spring
Rancho
Google
Click "Continue" to view the Full Phone Report for 619-
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.
Home | Frequently Asked Questions | Login | Register
© 2011 Phone Detective



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

Summary

- Authentication protocols: 6 out of 9 similar applications had the same problems
- Unintended use (reverse hash in Dropbox)
- Trust in client application
- Missing input validation
- Everything you should learn in Security 101

Contact Information

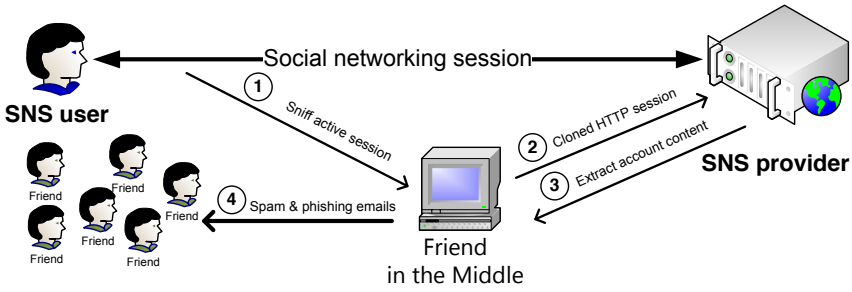
Martin Mulazzani, Sebastian Schrittwieser, Manuel Leithner, Markus Huber, and Edgar R. Weippl. **Dark clouds on the horizon**: Using cloud storage as attack vector and online slack space. In USENIX Security, 8 2011.

Markus Huber, Martin Mulazzani, Manuel Leithner, Sebastian Schrittwieser, Gilbert Wondracek, and Edgar R. Weippl. **Social snapshots**: Digital forensics for online social networks. In Annual Computer Security Applications Conference (ACSAC), 12 2011.

Sebastian Schrittwieser, Peter Fruehwirt, Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Markus Huber, and Edgar R. Weippl. **Guess who is texting you**? evaluating the security of smartphone messaging applications. In Network and Distributed System Security Symposium (NDSS 2012), 2 2012.

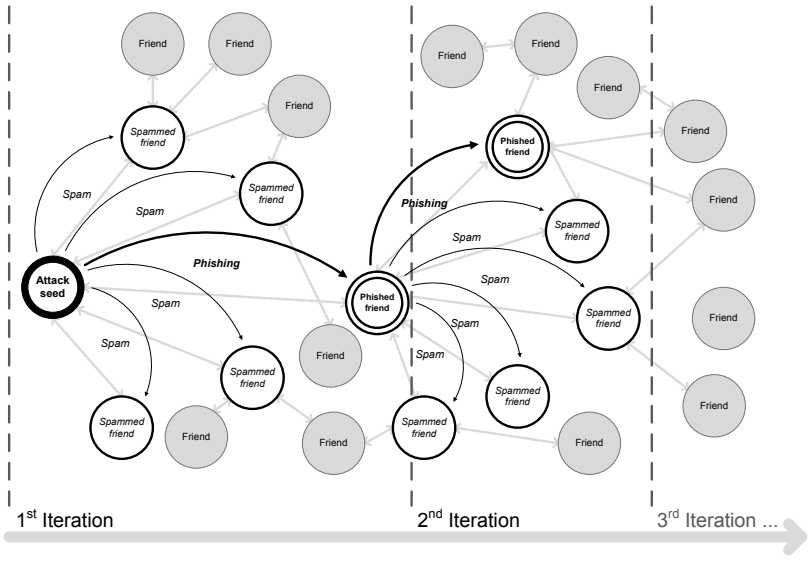
Edgar Weippl
www.sba-research.org

Friend-in-the-middle (FITM) attacks



- Hijack social networking sessions
- Attack surface: unencrypted WLAN traffic, LAN, router etc.
- User impersonation

Attack scenario



Fast Access to Data