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

<table>
<thead>
<tr>
<th>Name</th>
<th>Protocol</th>
<th>Encrypted transmission</th>
<th>Encrypted storage</th>
<th>Shared storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wuala</td>
<td>Crypttree</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>SpiderOak</td>
<td>proprietary</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Ubuntu One</td>
<td>u1storage</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Dropbox</td>
<td>proprietary</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>

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

1. (HTTPS): Phone number
2. (SMS): Code
3. (HTTPS): Code
In Reality

Even Worse
Completely Stealthy

WowTalk
Status Messages

Thomas
No damn....

Anne
Story

Susanne
unavailable

Peter
I'm a secure fortune cookie.

Felix
Schrödinger

Chris
At the gym... not!

Florian


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

Enumeration Attack
Enumeration Attack

[Diagram showing a flow of data from a phone to a server and then to a database]

Enumeration Attack

[Bar chart showing data distribution]
On vacation

Sleeping

At work ... Bleh.

Heartbroken

Nicaragua in 4 days!!

Missing my love!

On my way to Ireland!

I’m never drinking again

at work but not doing shit

12/18/12
### Results

<table>
<thead>
<tr>
<th>App</th>
<th>Account Hijacking</th>
<th>Spoofing/Manipulation</th>
<th>Unrequested SMS</th>
<th>Enumeration</th>
<th>Other Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>WhatsApp</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Viber</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>eBuddy XMS</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Tango</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Voypi</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Forfone</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>HeyTell</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>limited</td>
<td>no</td>
</tr>
<tr>
<td>EasyTalk</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>WowTalk</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>
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


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

1. Social snapshot client
   - Authentication
2. Shared secret
3. Contact list
4. Session secret
5. Crawler data
6. API requests
7. Social data

Third-party application

Social data pool

Web server

Automated web browser