IMPACT OF USER CHARACTERISTICS ON ATTITUDES TOWARDS AUTOMATIC ANDROID APPLICATION UPDATES

Arunesh Mathur, Marshini Chetty

@aruneshmathur
Apache Cordova Vulnerability Discovered: 10% of Android Banking Apps Potentially Vulnerable

August 5, 2014 | By Roei Hay Co-authored by David Kaplan

These Android, iOS, and WP8 Apps are Affected by the Heartbleed Bug (Updated)

By Williams Pelgrin — Updated April 15, 2014 8:36 am

How We Discovered The Heartbleed of Vulnerable Android Apps in 1 Day

SESSION ID: HTA-T08

Jaji Montelobano

Will Dormann
IMPORTANT TO APPLY APP UPDATES IMMEDIATELY AND REGULARLY!
Americans and Cybersecurity

Many Americans do not trust modern institutions to protect their personal data—even as they frequently neglect cybersecurity best practices in their own personal lives.

by Kenneth Olmstead and Aaron Smith

4

To Pin or Not to Pin
Helping App Developers Bullet Proof Their TLS Connections

Marten Oltrogge, Yasemin Acar
dseec, Leibniz University Hannover
oltrogge.acar@des.cs.uni-hannover.de

Sergio Dechand, Matthew Smith
USEPA, University Bonn
dechand.1@epa.gov

Seojae Fahl
FKIE, Fraunhofer
fahl@fkie.fraunhofer.de

Abstract

For increased security during TLS certificate validation, a common recommendation is to use a variation of pinning. Especially non-browser software developers are encouraged to limit the number of trusted certificates to a minimum, since the default CA-based approach is known to be vulnerable to security threats.

The decision for or against pinning is always a trade-off between increasing security and keeping maintenance efforts at an acceptable level. In this paper, we present an extensive study on the applicability of pinning for non-browser software by analyzing 639,283 Android apps. Conservatively, we propose pinning as an appropriate strategy for 11,547 (1.8%) apps or 45,247 TLS connections (4.2%) in our sample set.

With a more optimistic classification of borderline cases, we propose pinning for consideration for 58,817 (9.1%) apps or 140,606 (13.8%) TLS connections. This weakens the assumption that pinning is a widely usable strategy for TLS security in non-browser software. However, in a nominal-actual comparison, we find that only 45 apps actually implement pinning. We collected developer feedback from 45 respondents and learned that only a quarter of them grasp the concept of pinning, but still find pinning too complex to use. Based on their feedback, we built an easy-to-use web-application that supports developers in the decision process and guides them through the correct deployment of a pinning-protected TLS implementation.

1 Introduction

Android is the major platform for mobile users and mobile app developers. Many apps handle sensitive information and deploy the transport layer security protocol (TLS) to protect data in transit. Previous research uncovered security issues with TLS in mobile apps [7, 8, 9, 2, 23] that highlight that developers have problems with implementing correct certificate validation while users are challenged by TLS intermediaries. Furthermore, the default TLS implementation on Android receives criticism [24, 18]. Adapted from web-browsers, default TLS certificate validation relies on a large number of root CAs pre-installed on all Android devices [24]. Hence, all Android apps suffer from the same issues as web-browsers. A single malicious CA is able to conduct Man-In-The-Middle attacks (MITM) against all apps trusting the respective certificate.

To make things even worse, Fahl et al. [8] uncovered that in 97% of all cases where developers implemented their own certificate validation strategy, they turned off validation entirely and left their apps vulnerable to MITM attacks with arbitrary certificates. I.e., every active network attacker was able to attack successfully.

Pinning is often recommended as a general countermeasure to tackle the weakest link in the CA-based infrastructure [1, 14, 17, 8]. We use the term pinning in this paper to include both pinning the complete X.509 certificate or only the certificate's public key. Instead of trusting a large set of root CAs that come pre-installed with the operating system, software limits the set of certification it trusts to pins, which can be single leaf certificates, single root CA certificates or a set of certificates. Pinning is a straightforward mechanism and its deployment does not require changes to the current CA infrastructure. However, pinning has not found widespread adoption yet. While limiting the number of trusted certificates drastically increases security, pinning doesn’t come for free. Embedding trusted certificates into an app requires app updates whenever the pins change. Hence, the decision whether
Americans and Cybersecurity

Many Americans do not trust mobile apps to protect their personal data, even if these apps come from developers known to
may be cyber security best practices.

ONLY 16% UPDATED APPS IMMEDIATELY

ONLY 50% USERS UPDATED APPS WITHIN FIRST WEEK
Planet Scale Software Updates

Christos Gkantsidis; Thomas Karagiannis; Pablo Rodriguez; Milan Vojnović

Why Silent Updates Boost Security

Thomas Duebendorfer
Google Switzerland GmbH

Stefan Frei
Swiss Federal Institute of Technology (ETH Zurich)

The Attack of the Clones: A Study of the Impact of Shared Code on Vulnerability Patching

Antonio Nappa, Richard Johnson†, Leyla Bilge‡, Juan Caballero*, Tudor Dumitras†

*IMDEA Software Institute †University of Maryland, College Park
‡Symantec Research Labs §Universidad Politécnica de Madrid

antonio.nappa@imdea.org, rbjohns8@cs.umd.edu,
leylya_yumer@symantec.com, juan.caballero@imdea.org, tdumitra@umiacs.umd.edu
Enable automatic updates if your vendors offer it; that will ensure your software is always updated, and you won’t have to remember to do it yourself.

Greater use of automatic updating may be one solution to the outdated software problem.

Running out-of-date versions can put you at risk from being exploited by web-based attacks. Select automatic updates wherever possible.
Settings

GENERAL

Notifications
Notify me about updates to apps or games that I downloaded

Auto-update apps

Do not auto-update apps
Auto-update apps at any time. Data charges may apply.
Auto-update apps over Wi-Fi only

Cancel

Set the content filtering level to restrict apps that can be downloaded

Require authentication for purchases
For all purchases through Google Play on this device

ABOUT
What user characteristics differentiate those Android users who avoid auto-updates from those who do auto-update their applications?

What user characteristics explain Android users’ preferences towards auto-updating their applications?
User characteristics?

- Past Negative Software Updating Experience [Vaniea CHI ’14, Vaniea CHI ’16, Forget SOUPS ’16]
- Psychometric Traits [Egelman CHI ’15]
  - Risk Taking
  - Consideration of Future Consequences
  - Curiosity and Inquisitiveness
- Application Specific Factors [Mathur SOUPS ’16]
  - Trust in App
  - Frequency of Use of App
  - Importance of App
  - Satisfaction with App
- Demographics
Survey

Part One:
Psychometric Scales

Part Two:
Update settings & Preferences

Part Three:
Past Update Experiences
Survey

Part One: Psychometric Scales

Part Two: Update settings & Preferences

Part Three: Past Update Experiences
Survey: Part One

- **Psychometric Scales**
  - Domain Specific Risk Taking (DoSpeRT) Scale
  - Need For Cognition (NFC) scale
  - Consideration for Future Consequences (CFC) scale
  - Resistance to Change (RTC) scale

- **Past Security Behavior**
  - Security Behavior Intentions (SeBIS) scale
Survey: Part One

- **Psychometric Scales**
  - Domain Specific Risk Taking (DoSpeRT) Scale
  - Need For Cognition (NFC) scale
  - Consideration for Future Consequences (CFC) scale
  - Resistance to Change (RTC) scale

- **Past Security Behavior**
  - Security Behavior Intentions (SeBIS) scale
Survey

Part One: Psychometric Scales

Part Two: Update settings & Preferences

Part Three: Past Update Experiences
Survey

Part One: Psychometric Scales

Part Two: Update settings & Preferences

Part Three: Past Update Experiences
Survey: Part Two

- Report Android Update Settings
- Using labelled instructions
10. Please report the following update settings for your Android device by following the instructions in the images below.

1. Open the Google Play Store App

2. Touch the menu icon

3.

4.
Survey: Part Two

- Report Android Update Settings
- Using labelled instructions
Survey: Part Two

- Report Android Update Settings
- Using labelled instructions
- Report Installed Android Applications
13. The following is a list of the most downloaded Android apps from the Google Play Store.

From this list, please select **ALL** the ones you have installed on your Android phone. *

<table>
<thead>
<tr>
<th>App Name</th>
<th>Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZEDGE™ Ringtones &amp; Wallpapers</td>
<td><img src="image" alt="ZEDGE" /></td>
</tr>
<tr>
<td>Zombie Tsunami</td>
<td><img src="image" alt="Zombie Tsunami" /></td>
</tr>
<tr>
<td>YouTube</td>
<td><img src="image" alt="YouTube" /></td>
</tr>
<tr>
<td>Yahoo Mail</td>
<td><img src="image" alt="Yahoo Mail" /></td>
</tr>
<tr>
<td>Tango</td>
<td><img src="image" alt="Tango" /></td>
</tr>
<tr>
<td>Super-Bright LED Flashlight</td>
<td><img src="image" alt="Super-Bright LED Flashlight" /></td>
</tr>
<tr>
<td>Skype</td>
<td><img src="image" alt="Skype" /></td>
</tr>
<tr>
<td>Subway Surfers</td>
<td><img src="image" alt="Subway Surfers" /></td>
</tr>
<tr>
<td>Spotify</td>
<td><img src="image" alt="Spotify" /></td>
</tr>
<tr>
<td>Talking Tom Cat 2</td>
<td><img src="image" alt="Talking Tom Cat 2" /></td>
</tr>
<tr>
<td>Temple Run</td>
<td><img src="image" alt="Temple Run" /></td>
</tr>
<tr>
<td>Twitter</td>
<td><img src="image" alt="Twitter" /></td>
</tr>
<tr>
<td>Trivia Crack</td>
<td><img src="image" alt="Trivia Crack" /></td>
</tr>
<tr>
<td>Viber</td>
<td><img src="image" alt="Viber" /></td>
</tr>
<tr>
<td>Temple Run 2</td>
<td><img src="image" alt="Temple Run 2" /></td>
</tr>
<tr>
<td>WhatsApp</td>
<td><img src="image" alt="WhatsApp" /></td>
</tr>
<tr>
<td>WeChat</td>
<td><img src="image" alt="WeChat" /></td>
</tr>
<tr>
<td>My Talking Tom</td>
<td><img src="image" alt="My Talking Tom" /></td>
</tr>
<tr>
<td>Pou</td>
<td><img src="image" alt="Pou" /></td>
</tr>
<tr>
<td>PicsArt Photo Studio</td>
<td><img src="image" alt="PicsArt Photo Studio" /></td>
</tr>
</tbody>
</table>
Survey: Part Two

- Report Android Update Settings
- Using labelled instructions
- Report Installed Android Applications
Survey: Part Two

- Report Android Update Settings
  - Using labelled instructions
- Report Installed Android Applications. For a Maximum of 10 Sampled Applications:
  - Comfort auto-updating security and non-security updates (0 - 100)
  - Importance of, Trust in, Frequency of Use of, and Satisfaction with the Application (1 - 5)
Survey

Part One: Psychometric Scales

Part Two: Update settings & Preferences

Part Three: Past Update Experiences
Survey

Part One: Psychometric Scales

Part Two: Update settings & Preferences

Part Three: Past Update Experiences
Survey: Part Three

- Past Negative Software Updating Experience?
- Across any device, software

- Demographics
- Age, Gender, Education
Survey

Part One: Psychometric Scales

Part Two: Update settings & Preferences

Part Three: Past Update Experiences

Always last
Participants

- Recruited through Amazon Mechanical Turk
- N = 477
- Age: 69.2% between 18-34
- Gender: 62.3% Male
Participants

- Recruited through Amazon Mechanical Turk
- N = 477
- Age: 69.2% between 18-34
- Gender: 62.3% Male
- 67% Reported Auto-updating applications
Question One: What user characteristics differentiate those Android users who avoid auto-updates from those who do auto-update their applications?
Analysis: **Logistic regression**

- **Dependent Variable**: Auto-update or Not
- **Independent Variables**: User characteristics
  - Psychometric scales, SeBIS scores
  - Past Negative Experience with Software Updating
  - Demographics
## Results

**Outcome: Did not Auto-update**

<table>
<thead>
<tr>
<th>Predictor</th>
<th>Odds Ratio</th>
<th>Odds Ratio 95% C.I.</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negative Experience [Yes]</td>
<td>2.81</td>
<td>1.75, 4.56</td>
<td>&lt; 0.0001</td>
</tr>
<tr>
<td>DoSpeRT–Investment</td>
<td>0.79</td>
<td>0.66, 0.94</td>
<td>&lt; 0.01</td>
</tr>
<tr>
<td>DoSpeRT–Ethical</td>
<td>0.75</td>
<td>0.62, 0.91</td>
<td>&lt; 0.01</td>
</tr>
<tr>
<td>SeBIS–Proactive Awareness</td>
<td>1.42</td>
<td>1.01, 2.01</td>
<td>0.04</td>
</tr>
</tbody>
</table>
## Results

Outcome: Did not Auto-update

<table>
<thead>
<tr>
<th>Predictor</th>
<th>Odds Ratio</th>
<th>Odds Ratio 95% C.I.</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negative Experience [Yes]</td>
<td>2.81</td>
<td>1.75, 4.56</td>
<td>&lt; 0.0001</td>
</tr>
</tbody>
</table>

Avoiding Auto-updates is associated with Past Negative Experiences with Software Updates.
<table>
<thead>
<tr>
<th>Negative Experience</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version prior to update worked better</td>
<td>36.4%</td>
</tr>
<tr>
<td>The update introduced new bugs</td>
<td>34.3%</td>
</tr>
<tr>
<td>The update modified the user interface</td>
<td>27.6%</td>
</tr>
<tr>
<td>The update took a long time to install</td>
<td>11.3%</td>
</tr>
<tr>
<td>The update used up a lot of data</td>
<td>10.7%</td>
</tr>
</tbody>
</table>
Results

"P34: Windows 10, or garbage time, breaks pretty much every time it updates.

P145: The update I downloaded made other apps buggy.

P298: The iTunes update deleted my password and I could not get it back and it would not let me know what it was. I also lost all the music I had purchased."
## Results

Outcome: Did not Auto-update

<table>
<thead>
<tr>
<th>Predictor</th>
<th>Odds Ratio</th>
<th>Odds Ratio 95% C.I.</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Negative Experience [Yes]</strong></td>
<td>2.81</td>
<td>1.75, 4.56</td>
<td>&lt; 0.0001</td>
</tr>
<tr>
<td>DoSpeRT–Investment</td>
<td>0.79</td>
<td>0.66, 0.94</td>
<td>&lt; 0.01</td>
</tr>
<tr>
<td>DoSpeRT–Ethical</td>
<td>0.75</td>
<td>0.62, 0.91</td>
<td>&lt; 0.01</td>
</tr>
<tr>
<td>SeBIS–Proactive Awareness</td>
<td>1.42</td>
<td>1.01, 2.01</td>
<td>0.04</td>
</tr>
</tbody>
</table>
## Results

### Outcome: Did not Auto-update

<table>
<thead>
<tr>
<th>Predictor</th>
<th>Odds Ratio</th>
<th>Odds Ratio 95% C.I.</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoSpeRT—Investment</td>
<td>0.79</td>
<td>0.66, 0.94</td>
<td>&lt; 0.01</td>
</tr>
<tr>
<td>DoSpeRT—Ethical</td>
<td>0.75</td>
<td>0.62, 0.91</td>
<td>&lt; 0.01</td>
</tr>
</tbody>
</table>

Avoiding Auto-updates is associated with lower risk taking behavior.
### Results

**Outcome: Did not Auto-update**

<table>
<thead>
<tr>
<th>Predictor</th>
<th>Odds Ratio</th>
<th>Odds Ratio 95% C.I.</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SeBIS—Proactive</td>
<td>1.42</td>
<td>1.01, 2.01</td>
<td>0.04</td>
</tr>
</tbody>
</table>

Avoiding Auto-updates is associated with Greater Proactive Security Behavior.
Question Two: What user characteristics explain Android users’ preferences towards auto-updating their applications?
Analysis: Linear Mixed Effects Model

- **Dependent Variable**: Comfort Score
- **Independent Variables**: User characteristics
  - Psychometric scales, SeBIS scores
  - Past Negative Experience with Software Updating
  - Demographics
  - Importance, Trust, Frequency of Use, Satisfaction
Analysis: Linear Mixed Effects Model

- **Dependent Variable:** Comfort Score
- **Independent Variables:** User characteristics
  - Psychometric scales, SeBIS scores
  - Past Negative Experience with Software Updating
  - Demographics
  - Importance, Trust, Frequency of Use, Satisfaction
## Results

**Outcome: Comfort Score with Auto-updating**

<table>
<thead>
<tr>
<th>Predictor</th>
<th>Estimate</th>
<th>Estimate 95% C.I.</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negative Experience [Yes]</td>
<td>-7.39</td>
<td>-11.49, -3.29</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>Update Type [Security]</td>
<td>6.76</td>
<td>6.03, 7.49</td>
<td>&lt; 0.0001</td>
</tr>
<tr>
<td>Trust</td>
<td>7.29</td>
<td>6.61, 7.96</td>
<td>&lt; 0.0001</td>
</tr>
</tbody>
</table>
**Results**

Outcome: Comfort Score with Auto-updating

<table>
<thead>
<tr>
<th>Predictor</th>
<th>Estimate</th>
<th>Estimate 95% C.I.</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negative Experience [Yes]</td>
<td>-7.39</td>
<td>-11.49, -3.29</td>
<td>&lt; 0.001</td>
</tr>
</tbody>
</table>

Past Negative Experience with Software Updates made Auto-updating Less Comfortable.
### Results

**Outcome:** Comfort Score with Auto-updating

<table>
<thead>
<tr>
<th>Predictor</th>
<th>Estimate</th>
<th>Estimate 95% C.I.</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update Type [Security]</td>
<td>6.76</td>
<td>6.03, 7.49</td>
<td>&lt; 0.0001</td>
</tr>
</tbody>
</table>

### Results

**Outcome: Comfort Score with Auto-updating**

<table>
<thead>
<tr>
<th>Predictor</th>
<th>Estimate</th>
<th>Estimate 95% C.I.</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust</td>
<td>7.29</td>
<td>6.61, 7.96</td>
<td>&lt; 0.0001</td>
</tr>
</tbody>
</table>

Trust in Application Made Auto-updating More Comfortable.
Implication #1

- **Improve Auto-update Interfaces:** Make Update Rollbacks/Recovery More Accessible
  - May increase confidence in auto-updating

**Open Questions:**

- Security vs Non-security updates
- Inform users about effects of rollback
- Rollback until when?
Implication #2

- Examine Update Development Practices:
  - Beyond end-users: How do software developers decide, build and test updates?
  - How do these practices lead to negative experiences for end-users?
Implication #3

- **Improve Auto-update Interfaces**: Design and evaluate messaging using risk-taking traits

  - **Financial risk**: “Not switching auto-updates on for security updates increases the chances of someone gaining access to your bank account or stealing your credit card information”

- **Open Questions:**

  - **Medium, timing of messages & evaluation**
Implication #4

- **Personalize Mobile Auto-update Systems:**
  - Use Trust and Security updates as factors to decide which applications to auto-update

- **Open Questions:**
  - What are some proxies for trust in an application, and can these be inferred?
IMPACT OF USER CHARACTERISTICS ON ATTITUDES TOWARDS AUTOMATIC ANDROID APPLICATION UPDATES

Arunesh Mathur

@aruneshmathur

http://aruneshmathur.co.in