Why Eve and Mallory Love Android
An Analysis of Android SSL (In)Security

Sascha Fahl

Marian Harbach

Thomas Muders

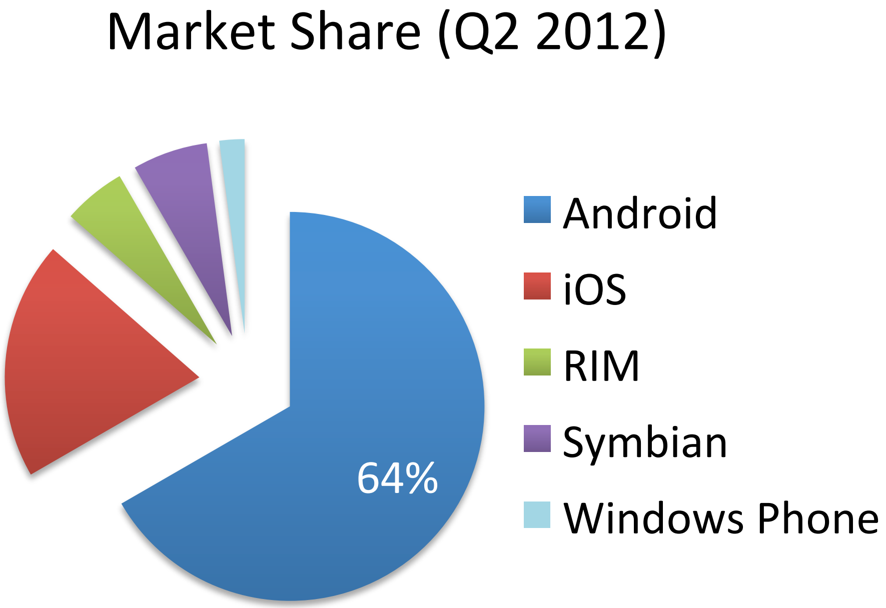
Lars Baumgärtner

Bernd Freisleben

Matthew Smith

Some Android Facts

- 330 million devices (as of Q1 2012)
- 930,000 activations per day (as of Q1 2012)
- 450,000 apps (as of June 2012)



Sascha Fahl, 20.11.2012

Appification

- There's an App for Everything

What do Most Apps Have in Common?

They share data over the Internet

Most of them secure transfer of sensitive data using

SSL

(Secure Sockets Layer protocol)

(Transport Layer Security **(TLS)** protocol)

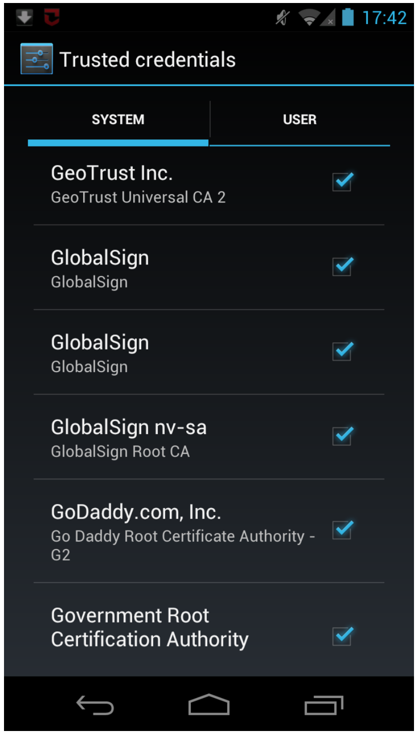
SSL Usage on Android

The default Android API implements correct certificate validation.

What could possibly go wrong?

SSL Usage on Android

- A server needs a certificate that was signed by a trusted Certificate Authority
- ~130 pre-installed CAs
- For non-trusted certificates a custom workaround is needed



GeoTrust Inc. ☑
GeoTrust Universal CA 2

GlobalSign ☑
GlobalSign

GlobalSign ☑
GlobalSign

GlobalSign nv-sa ☑
GlobalSign Root CA

GoDaddy.com, Inc. ☑
Go Daddy Root Certificate Authority - G2

Government Root Certification Authority ☑

What about using a non-trusted certificate?

Q: Does anyone know how to accept a self signed cert in Java on the Android? A code sample would be perfect.

A: Use the EasyX509TrustManager library hosted on code.google.com.

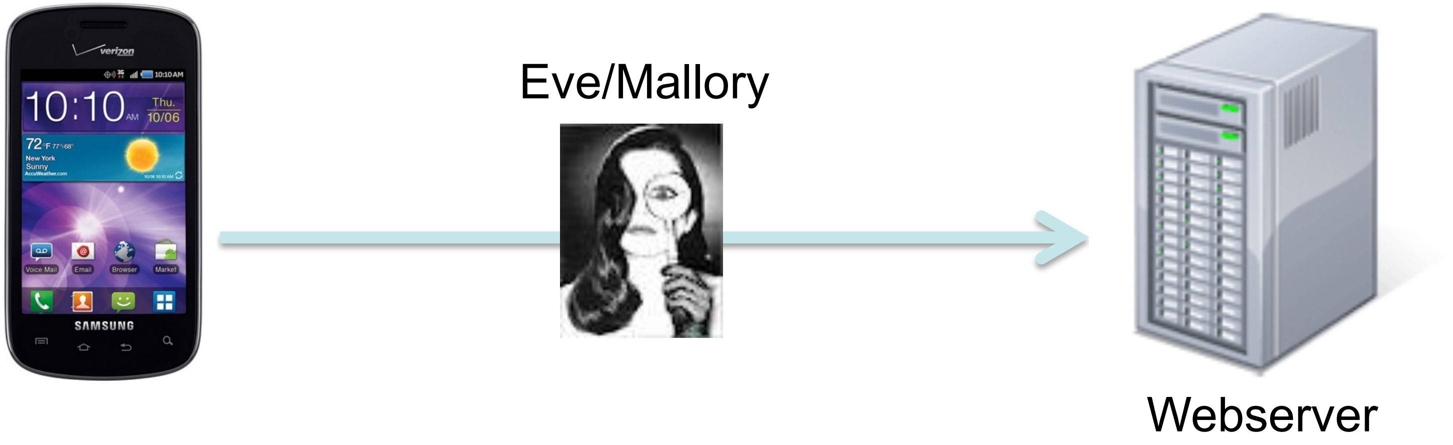
Q: I am getting an error of „javax.net.ssl.SSLException: Not trusted server certificate“. I want to simply allow any certificate to work, regardless whether it is or is not in the Android key chain. I have spent 40 hours researching and trying to figure out a workaround for this issue.

A: Look at this tutorial [...]

stackoverflow.com

Our Analysis

- downloaded 13,500 popular and free Apps from Google’s Play Market
- built MalloDroid which is an androguard extension to analyze possible SSL problems in Android Apps
  - broken TrustManager implementations
  - accept all Hostnames

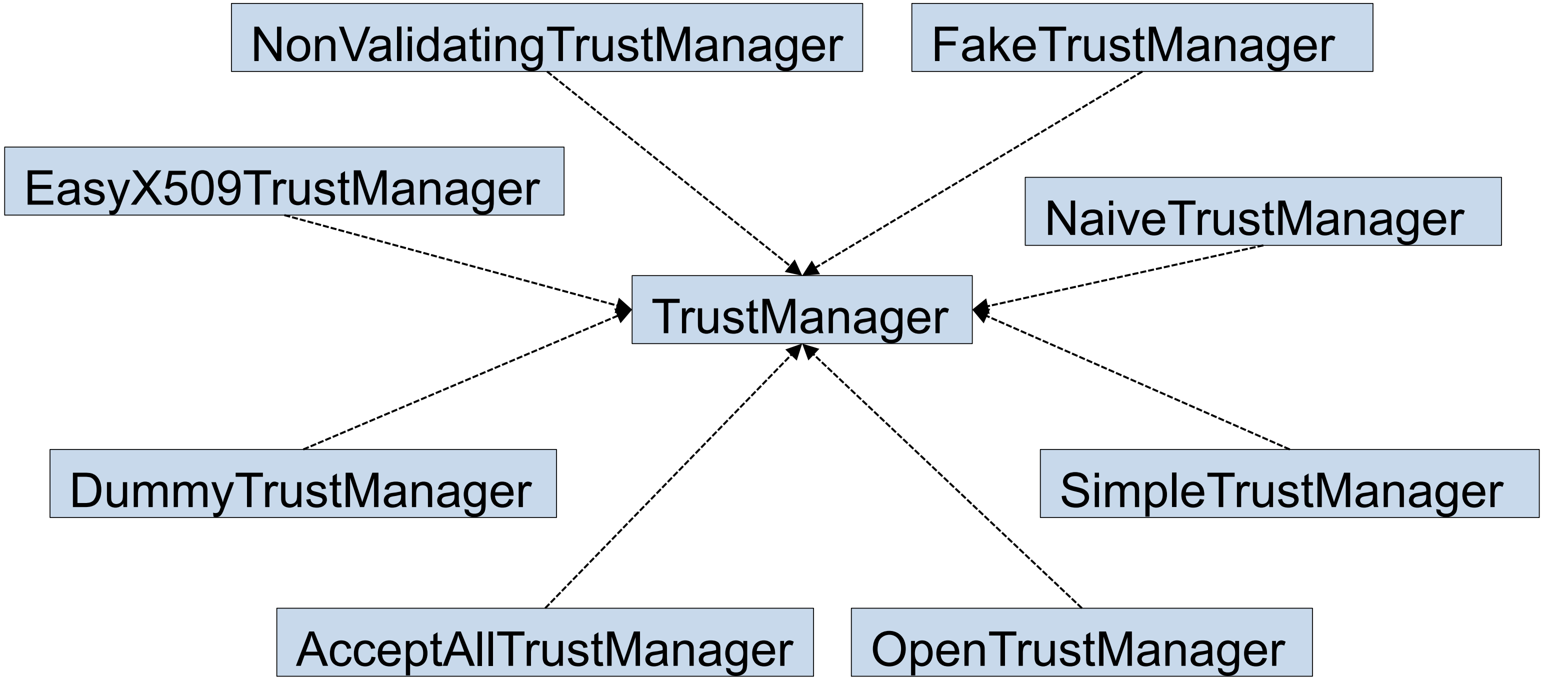


Static Code Analysis Results

- 92,8 % Apps use INTERNET permission
  - 91,7 % of networking API calls HTTP(S) related
  - 0,8 % exclusively HTTPS URLs
  - 46,2 % mix HTTP and HTTPS
- 17,28 % of all Apps that use HTTPS include code that fails during SSL certificate validation
  - 1074 include critical code
  - 790 accept all certificates
  - 284 accept all hostnames

TrustManager Implementations

- 22 different TrustManager implementations

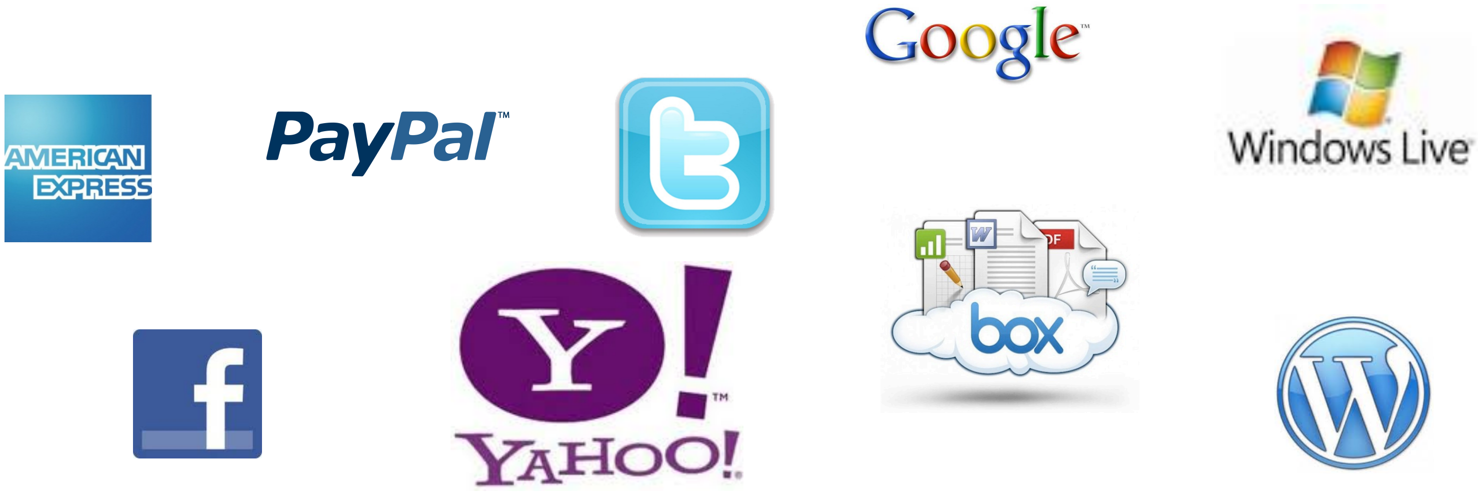


- and all turn effective certificate validation off

Manual App Testing Results

- cherry-picked 100 Apps
- 21 Apps trust all certificates
- 20 Apps accept all hostnames

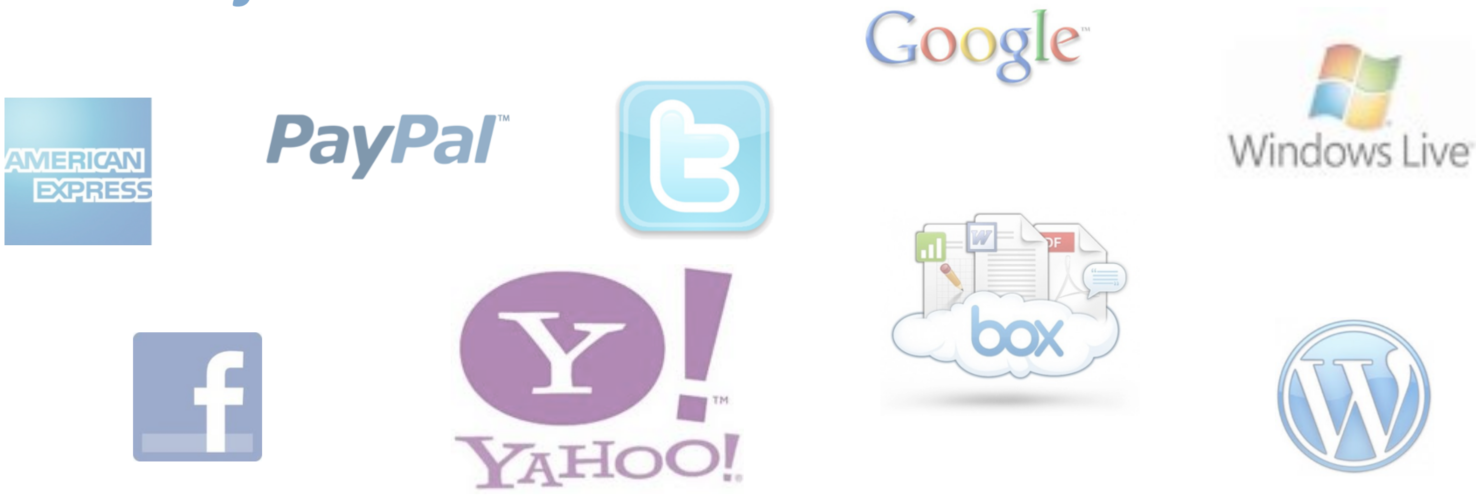
What we found:



Manual App Testing Results

39 – 185 million affected installs!

What we found:



One Example

Zoner AV

- Anti-Virus App for Android
- Awarded best free Anti-Virus App for Android by av-test.org

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Zoner AV

- Virus signature updates via HTTPS GET
- No check for the virus update’s authenticity!
- The good thing: It uses SSL
  - Unfortunately: The wrong way

```
static final HostnameVerifier DO_NOT_VERIFY = new HostnameVerifier()
{
        public boolean verify(String paramString, SSLSession paramSSLSession)
        {
          return true;
        }
};
```

Zoner AV

- We did the following

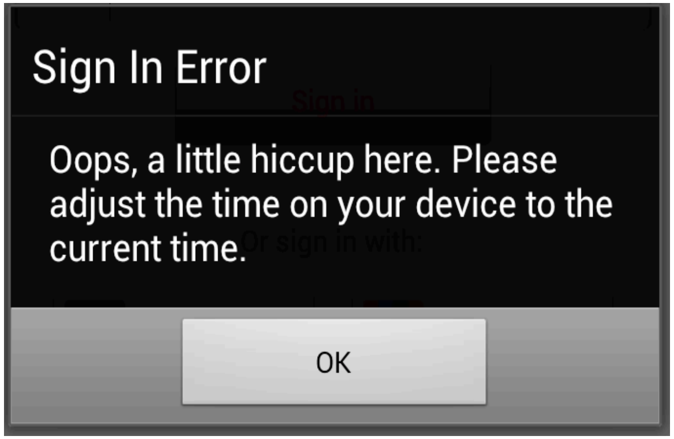
[redacted]

More Examples

- Remote Control App
- Remote Code Injection
- Unlocking Rental Cars

How Do (Good) Apps React to MITMAs?

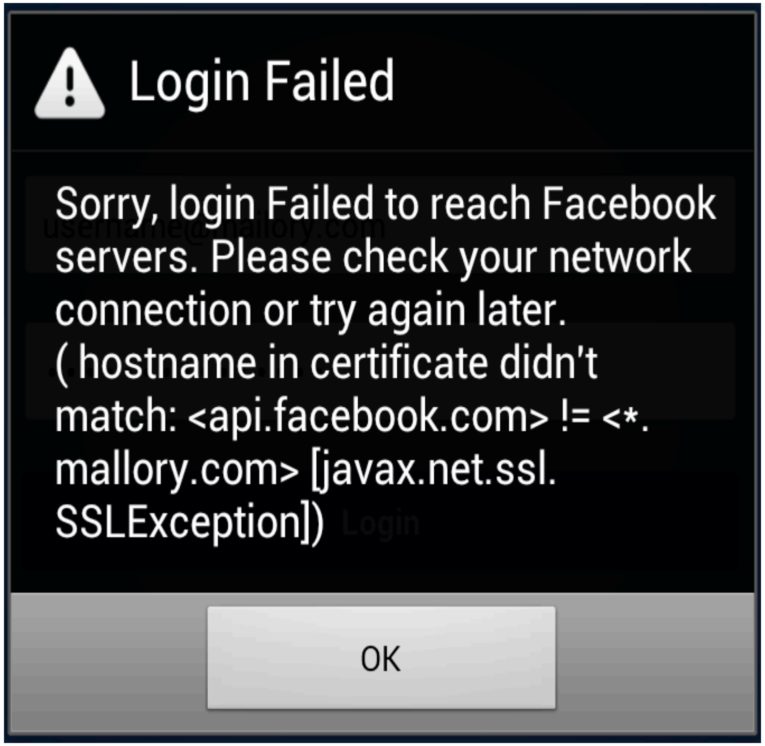
- Technically ✓
- Usability ?



Sign In Error

Oops, a little hiccup here. Please adjust the time on your device to the current time.

Flickr



Login Failed

Sorry, login Failed to reach Facebook servers. Please check your network connection or try again later. (hostname in certificate didn't match: <api.facebook.com> != <*. mallory.com> [javax.net.ssl. SSLException])

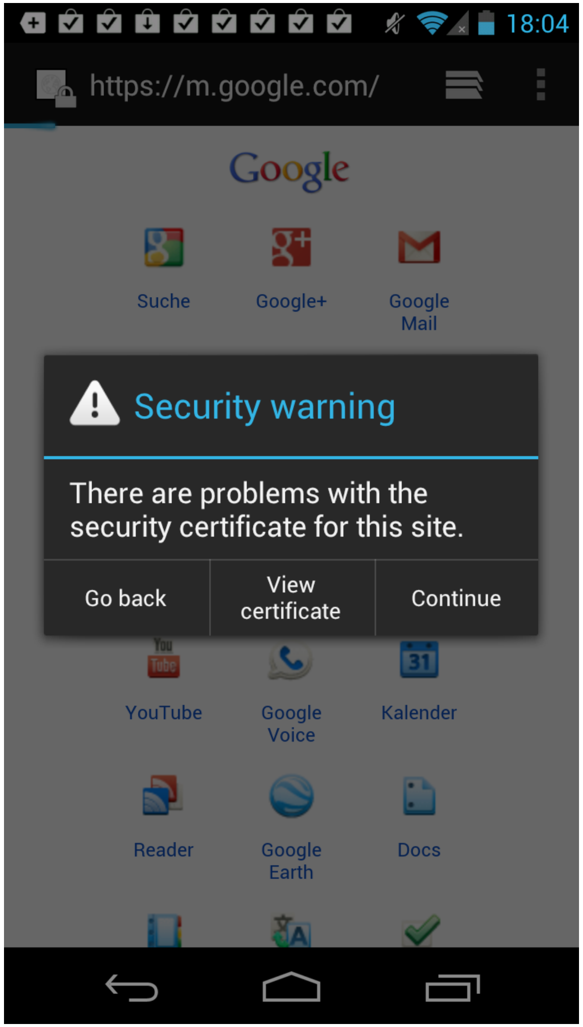
Facebook

Browser Warning Messages

All do SSL certificate validation correctly…

… and warn the user if something goes wrong….

SSL Warning Messages – Android Stock Browser

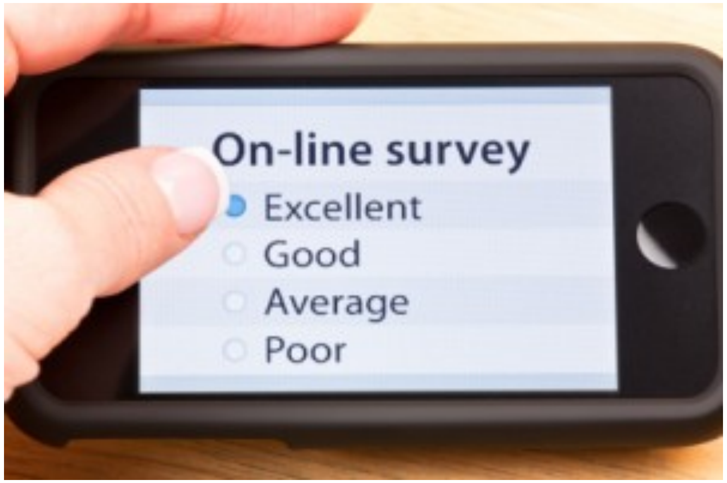


Security warning

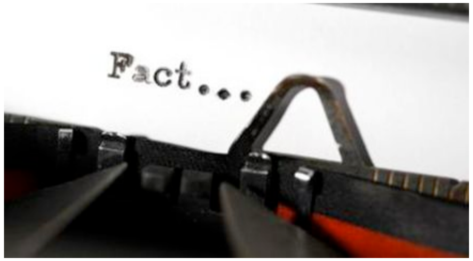
There are problems with the security certificate for this site.

Online Survey

- To find out if the Browser's warning messages help the users
  - presented an SSL warning message
- To see if users know when they are surfing on an SSL protected website
  - half of the participants HTTP
  - half of the participants HTTPS



Online Survey - Results



- 745 participants

- 47.5% of non-IT experts believed they were using a secure Internet connection... although it was plain HTTP.
- ... 34.7 % of IT experts thought so too.

- ~50% had not seen an SSL warning message on their phone before.
- The risk users were warned against was rated with 2.86 (sd=.94) on a scale between 1 (low risk) and 5 (high risk)
- Overall, a considerable amount of participants struggled to judge connection security accurately.

Our Recommendations

- Integrate SSL certificate validation testing into the development process

- Inform the user
  - INTERNET_SSL and INTERNET_PLAIN permission
  - global SSL warning message