AHA – Android HTTPS Analysis

Ralph Ankele, Robin Ankele

Simon Pöllitsch, Sebastian Sommer

Outline

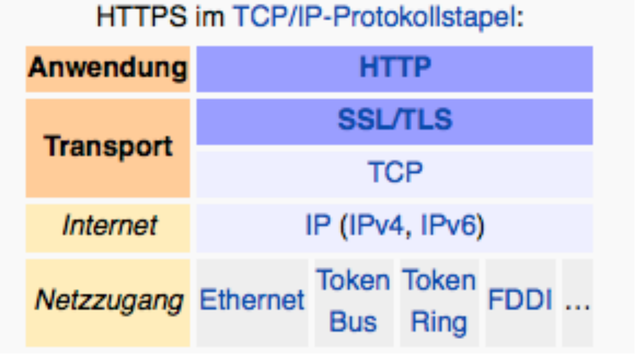
- Introduction
- Recapitulation
  - HTTPS / SSL
  - Certificates
- Man In The Middle Attack
- Implementation Details
- Apps / Statistics
- Live Demo

Introduction

- AHA – Android HTTPS Analysis
  - App which checks if HTTPS connection (i.e. certificate check) is correct implemented
  - MITM (Man in the middle attack)
  - Analyse of several apps – on different environments

Recapitulation – HTTPS / SSL

- Secure implementation of the Hypertext Transfer Protocol



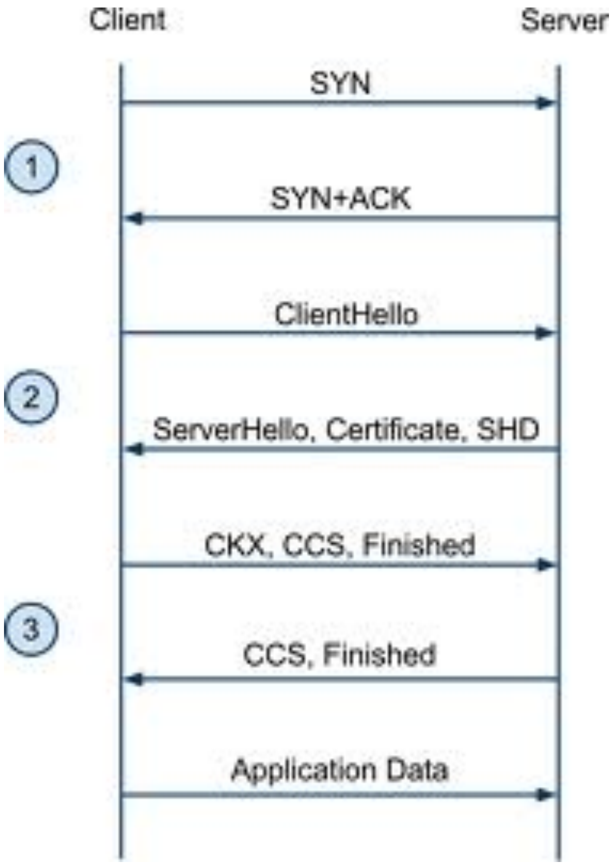
HTTPS im TCP/IP-Protokollstapel:

Anwendung	HTTP				
Transport	SSL/TLS				
	TCP				
Internet	IP (IPv4, IPv6)				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	...

- Security through TLS (Transport Layer Security)
  - Handshake
  - Security (DES, Tripple DES, AES)
  - Integrity (HMAC)

Recapitulation – HTTPS / SSL

- TLS Handshake



http://www.imperialviolet.org/binary/overclocking-ssl-1.png

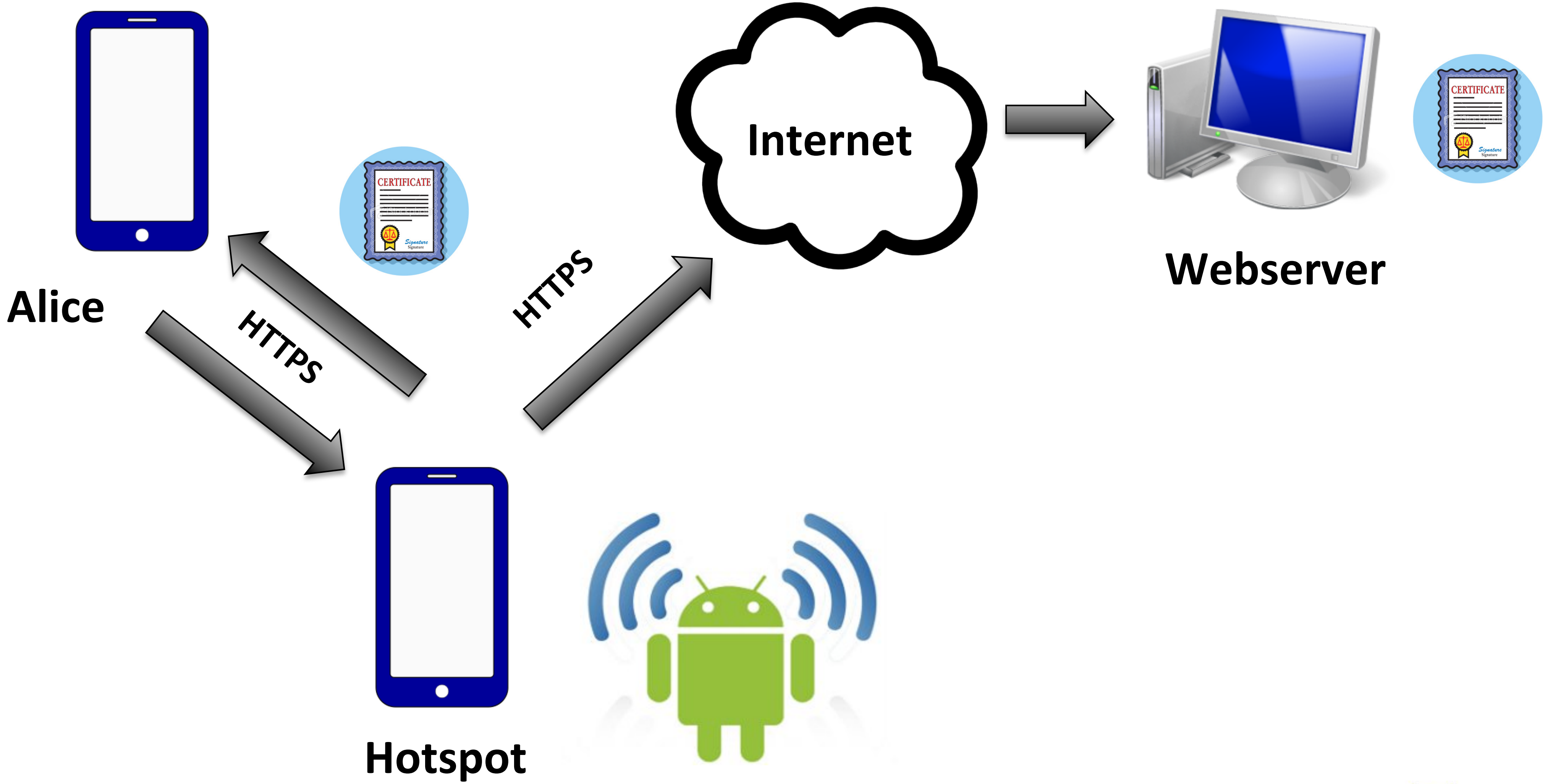
SHD … Server Hello Done
CKX … Client Key Exchange
CCS … Change Cipher Spec

Recapitulation – Certificates

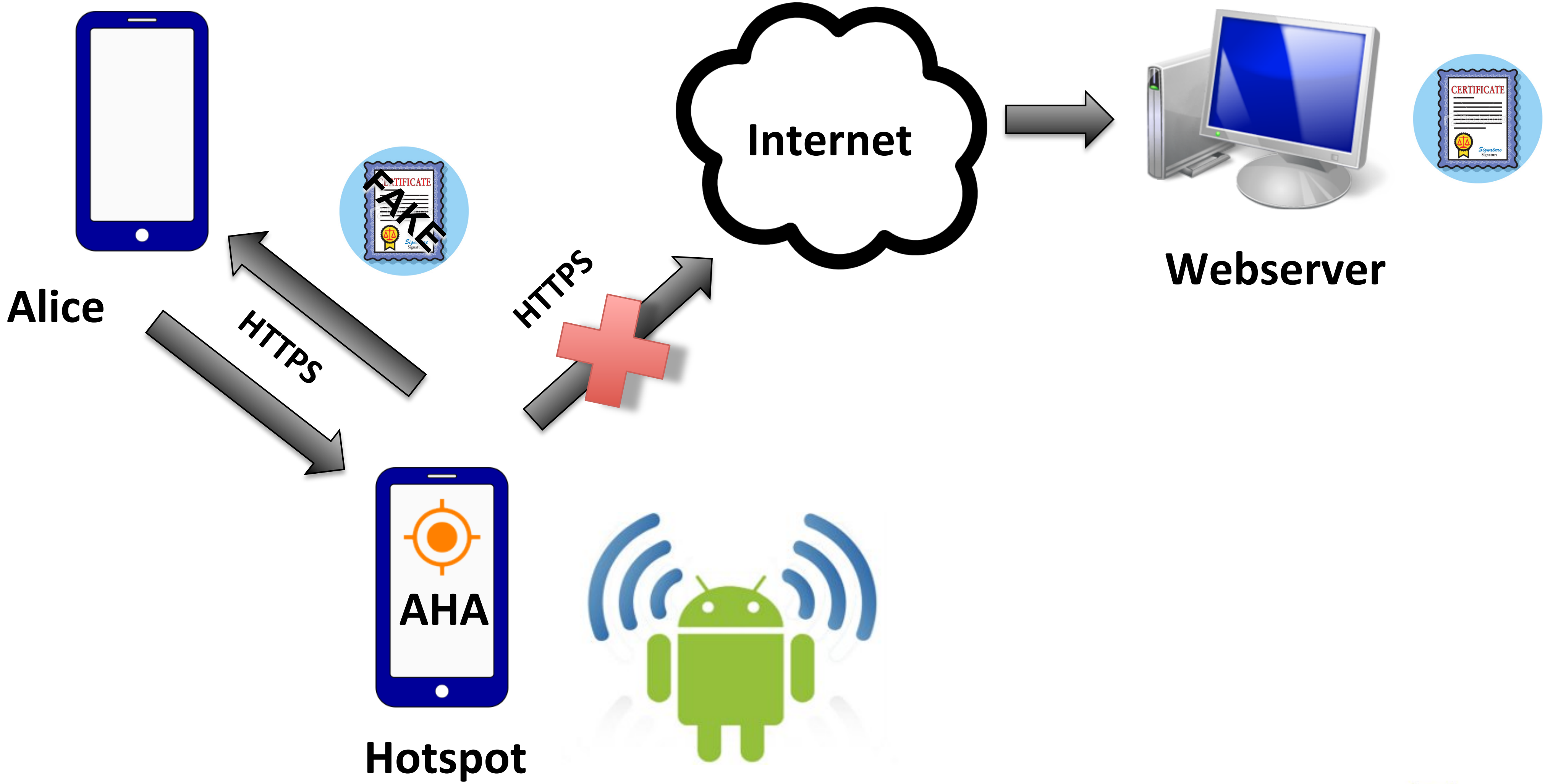
- Electronic document that uses a digital signature to bind a public key with an identity
  - uses PKI (Public Key Infrastructure)
  - signed by CA (Certification Authority)
- Typical X.509 Certificates

Issuer, Subject, Signature, Validity, Public Key

Normal HTTPS Connection



MITM – Man In The Middle Attack



MITM – Man In The Middle Attack

- Evesdrop and manipulate the traffic between two communication partners (e.g. client / server)
  - How?
    By physical/logical interception of the connection
  - AHA - App
    Change the certificate from the server with our own fake certificate

MITM – Different Attack Modi

- Trusting all certificates
  - No check who signed the certificate
- Allowing all hostnames
  - No check if the certificate was issued for a given address
- Trusting many CAs
  - Android 4.0 trusts 134 root CAs
- SSL strip
  - Rewrite HTTPS link to HTTP

MITM – What we’ve done

- Replacing the certificate from the webserver with our own fake certificate
- Check if *application under test* continues with traffic or rejects the fake certificate

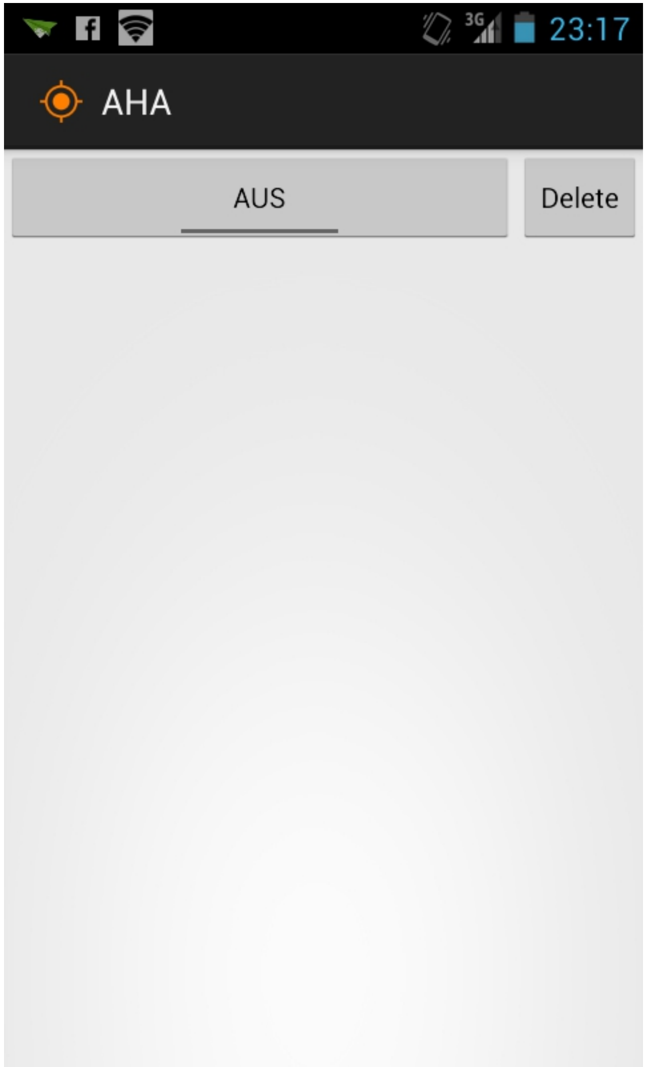
AHA - Certificate

Common Name: AHA
Issued To/By: TUGraz, IAIK

created with Bouncycastle

Implementation Details

- Android application
- Self-signed certificate (BouncyCastle)
- SSLServer
- Requires root



Implementation Details

SSL Server:

- Forward HTTPS-traffic to our app (443 → 1236)

```
iptables -t nat -A PREROUTING -p tcp --destination-port 443 -j REDIRECT --to-port 1236
```

- Set up SSLServerSocket and listen on port
  with self signed certificate

- Wait for incoming connection

```
new Thread(new mySession(sslServerSocket.accept()));
```

Implementation Details

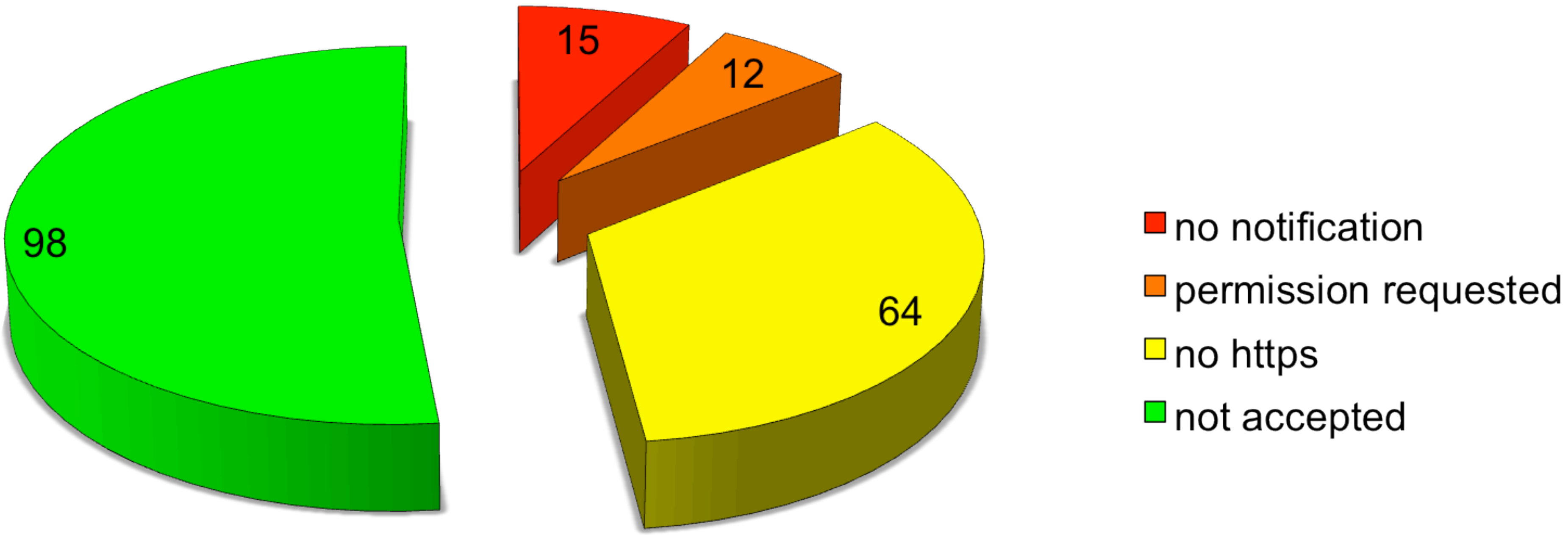
Incoming connection:

- One thread and socket per connection
- Client starts handshake with us
  If we read anything on the socket, the client accepted our cert
- Perform handshake to the target server
  We get the hostname from the HTTP-header
- Perform phishing
  Forward all the (manipulated) traffic from the target server to the client

App Analysis

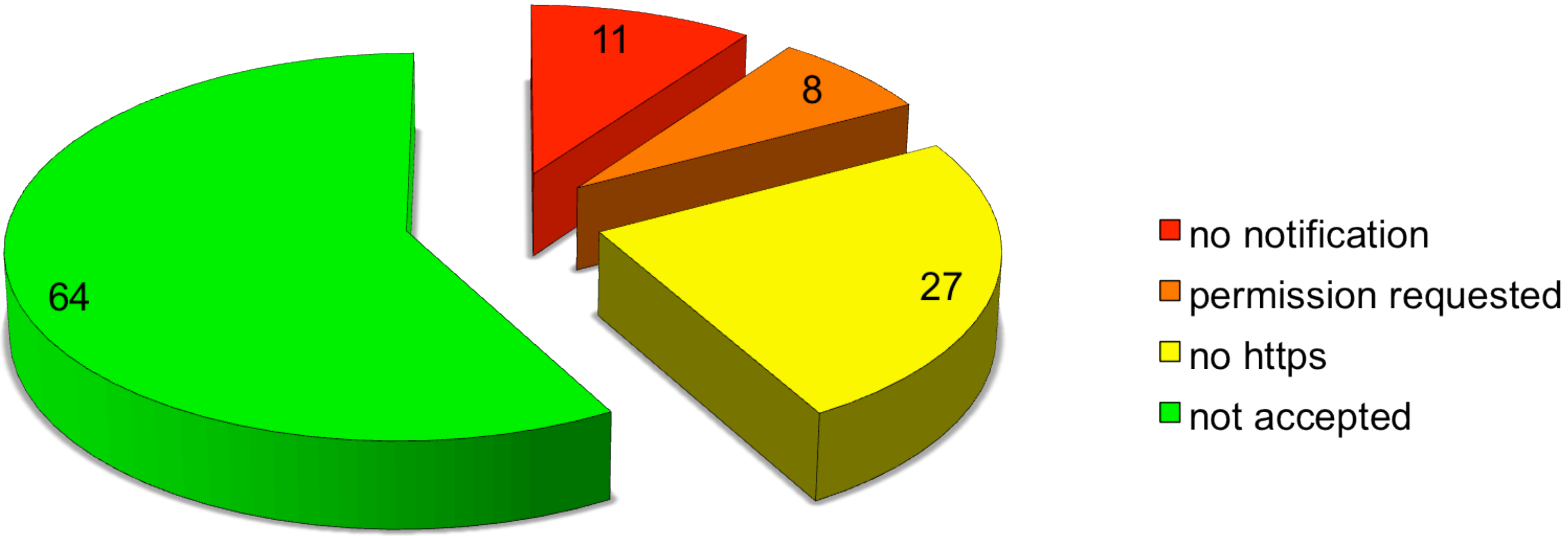
- Android (110)
- iOS (75)
- BlackBerry RIM (4)

Apps



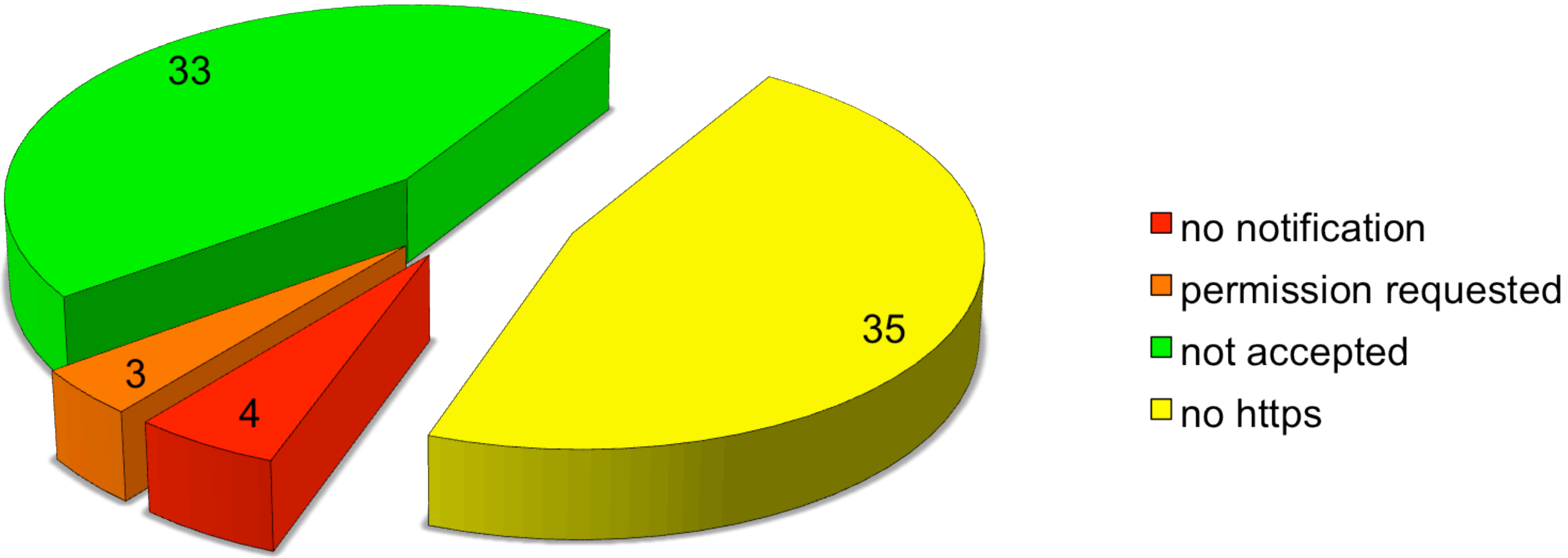
- Total tested Apps: 189

Android



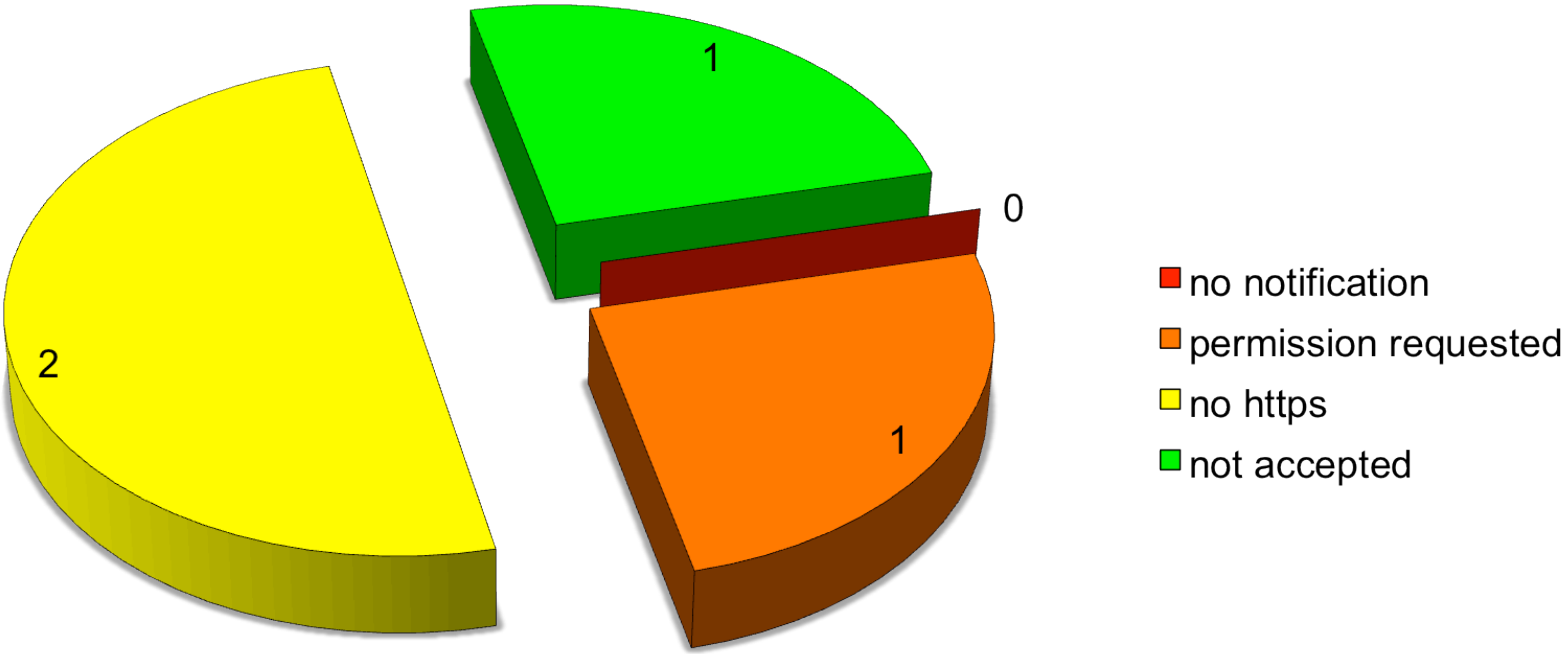
○ Total tested Apps: 110

iOS



- Total tested Apps: 75

BlackBerry RIM



- Total tested Apps: 4

Cut the Rope

- Installs: 10,000,000 – 50,000,000
- Current Version: 2.1
- Requires Android: 1.6 and up
- Category: Brain & Puzzles
- Prize: Free
- Content Rating: Low Maturity

- Android / iOS
- No notification

Mein A1

- Installs: 100,000 – 500,000
- Current Version: 3.3.0.6.734
- Requires Android: 2.1 and up
- Category: Finance
- Prize: Free
- Content Rating: Everyone

- Android

- No notification

ÖBB Tickets

- Installs: 50,000 – 100,000
- Current Version: 1.4.5
- Requires Android: 2.2 and up
- Category: Transportation
- Prize: Free
- Content Rating: Low Maturity

- Android

- No notification

Bank Austria mobile

- Installs: 50,000 – 100,000
- Current Version: 2.0
- Requires Android: 2.2 and up
- Category: Finance
- Prize: Free
- Content Rating: Everyone

- Android

- Permission requested

AppMe

- Current Version: 1.2
- Requires iOS: iOS 4.0 and later
- Category: Social Networking
- Prize: Free

- iOS
- No notification

Dropbox

- Current Version: 2.0.2
- Requires iOS: iOS 5.0 and later
- Category: Productivity
- Prize: Free

- iOS

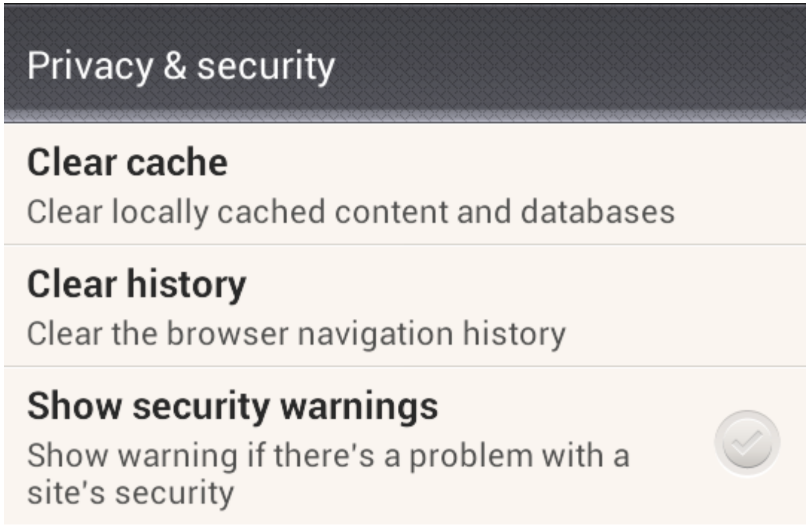
- No HTTPS

BlackBerry Browser

- Installs: Standard browser on every BlackBerry
- Current Version: 7.0
- Prize: Free

- BlackBerry RIM
- Permission requested

Standard Browsers - Android / iOS / RIM

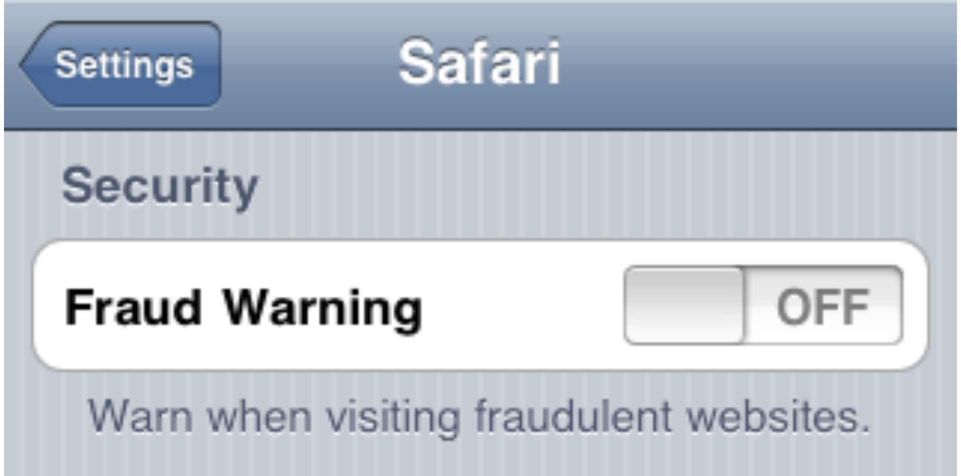


Privacy & security

Clear cache
Clear locally cached content and databases

Clear history
Clear the browser navigation history

Show security warnings ○
Show warning if there's a problem with a site's security



Security

Fraud Warning OFF

Warn when visiting fraudulent websites.

Live Presentation

- Live Presentation

Thank you for your attention!