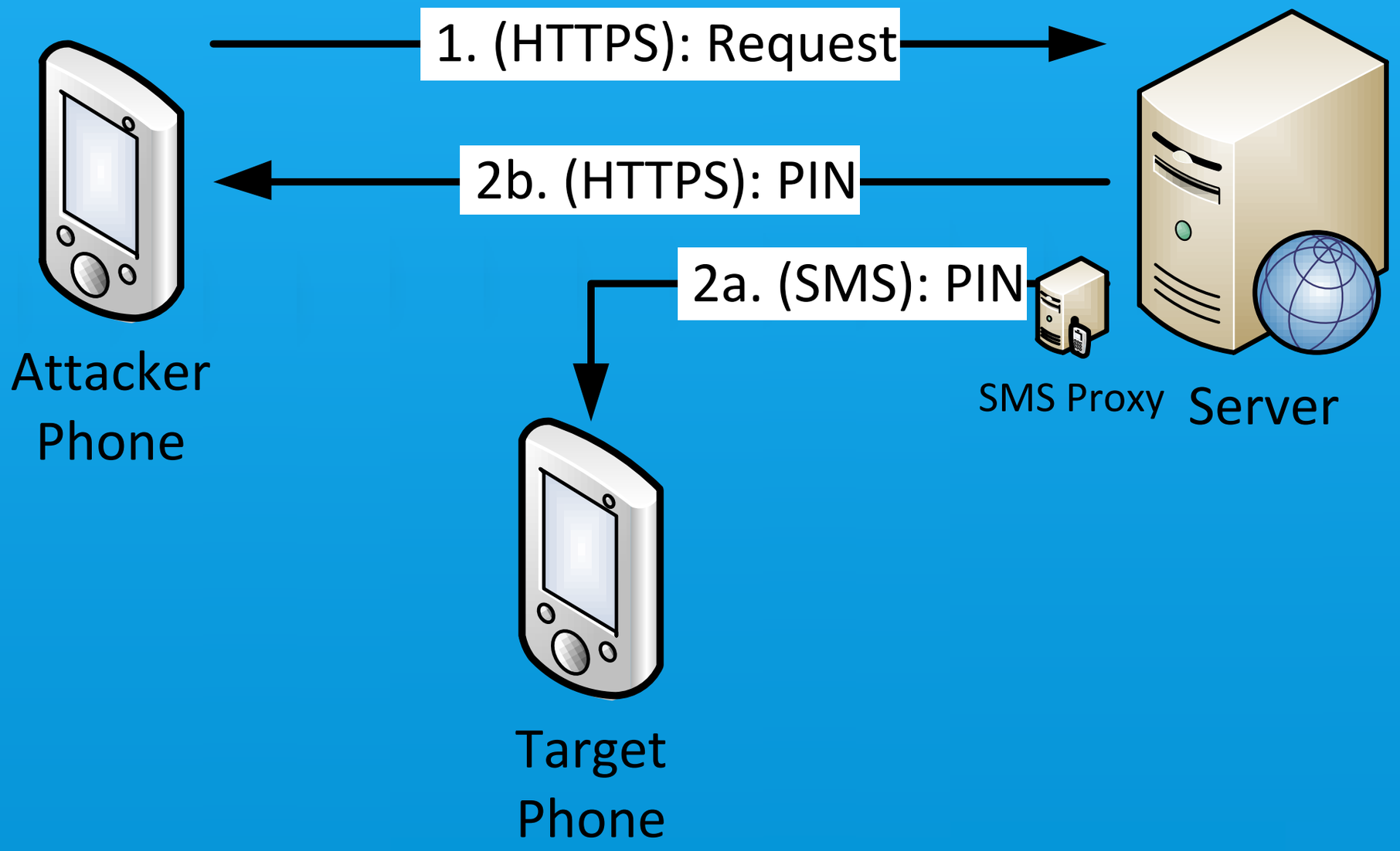
Security Through Obscurity

... powered by HTTPS!

Peter Frühwirt, SBA Research
Sebastian Schrittwieser, FH St. Pölten

redacted version

Live-Demo on Wowtalk


1. (HTTPS): Request
2b. (HTTPS): PIN
2a. (SMS): PIN
Attacker Phone
Target Phone
SMS Proxy
Server

SSL != protection against protocol analysis

SSL interception enables man-in-the-middle attacks for protocol analysis purposes

transport layer encryption cannot replace good protocol design!

Certificates?

```
if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
    goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;

    err = sslRawVerify(ctx,
                       ctx->peerPubKey,
                       dataToSign,                /* plaintext */
                       dataToSignLen,             /* plaintext length */
                       signature,
                       signatureLen);
        if(err) {
            sslErrorLog("SSLDecodeSignedServerKeyExchange: sslRawVerify "
                "returned %d\n", (int)err);
            goto fail;
        }

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;

}
```

http://opensource.apple.com/source/Security/Security-55471/libsecurity_ssl/lib/sslKeyExchange.c

Quizduell

extremely popular in Germany

Für eine größere Ansicht klicken Sie auf das Bild

Für Kunden: Stellen Sie Ihre eigenen Bilder ein.

Hier reinlesen und suchen

Quizduell [Taschenbuch]

Quizduell (Autor)

★★★★☆ (6 Kundenrezensionen)

Preis: EUR 9,99 kostenlose Lieferung. Siehe Details.

Alle Preisangaben inkl. MwSt.

Auf Lager.

Verkauf und Versand durch **Amazon**. Geschenkverpackung verfügbar.

Lieferung bis Dienstag, 11. März: Bestellen Sie innerhalb **2 Stunden und 13 Minuten** und wählen Sie **Internationale Express-Zustellung** an der Kasse. Siehe Details.

69 neu ab EUR 9,99 **2 gebraucht** ab EUR 9,99

Weitere Ausgaben	Amazon-Preis	Neu ab	Gebraucht ab
Kindle Edition	EUR 4,99	--	--
Taschenbuch	EUR 9,99	EUR 9,99	EUR 9,99

Menge: 1

In den Einkaufswagen

oder

Loggen Sie sich ein, um 1-Click® einzuschalten.

Auf meinen Wunschzettel

Jetzt eintauschen

und **EUR 3,60** Gutschein erhalten

Eintauschen

Weitere Informationen

Alle Angebote

71 Angebote ab EUR 9,99

Möchten Sie verkaufen?

Diesen Artikel verkaufen

Empfehlen

extremely popular in Germany

Let’s play a round of Quizduell ;)

Curiosity

November 2012 - May 2013

326 layers

69 billion small cubes

4 million players

3,000,000,000 coins for a diamond chisel

Bonus points for clearing the entire screen!

Parameter for multiplier is set by the server!

[...]
&backgroundColor=**blue**
&backgroundText=**Curiosity**
&bonusMultiplier=~~**10**~~ 10000000
&hardwareID=**<UDID>**&
[...]


8108
22:21:27.4
login
1 294 989 562

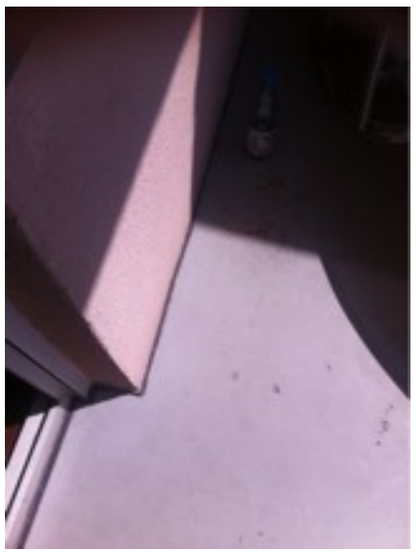
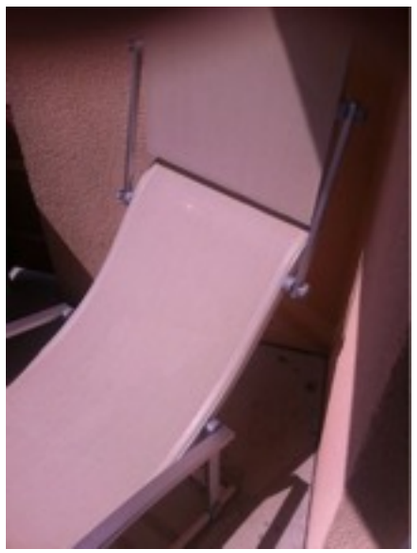
iPhone Apps

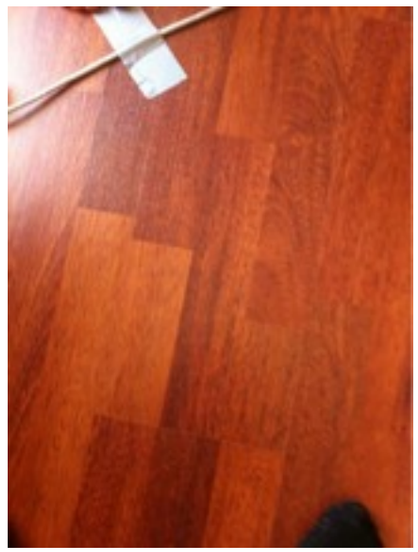
PhotoSwap
Social Networking

Photo-swap
Entertainment

SuperSwap
Social Networking

Photoswap

http://www.server.com/images/12345.jpg

http://www.server.com/images/12347.jpg

http://www.server.com/images/12349.jpg

http://www.server.com/images/12351.jpg

http://www.server.com/images/12353.jpg

```
for i in {1..12345}; do
wget -k http://www.server.com/images/$i.jpg;
done
```

Demo

Countermeasures?

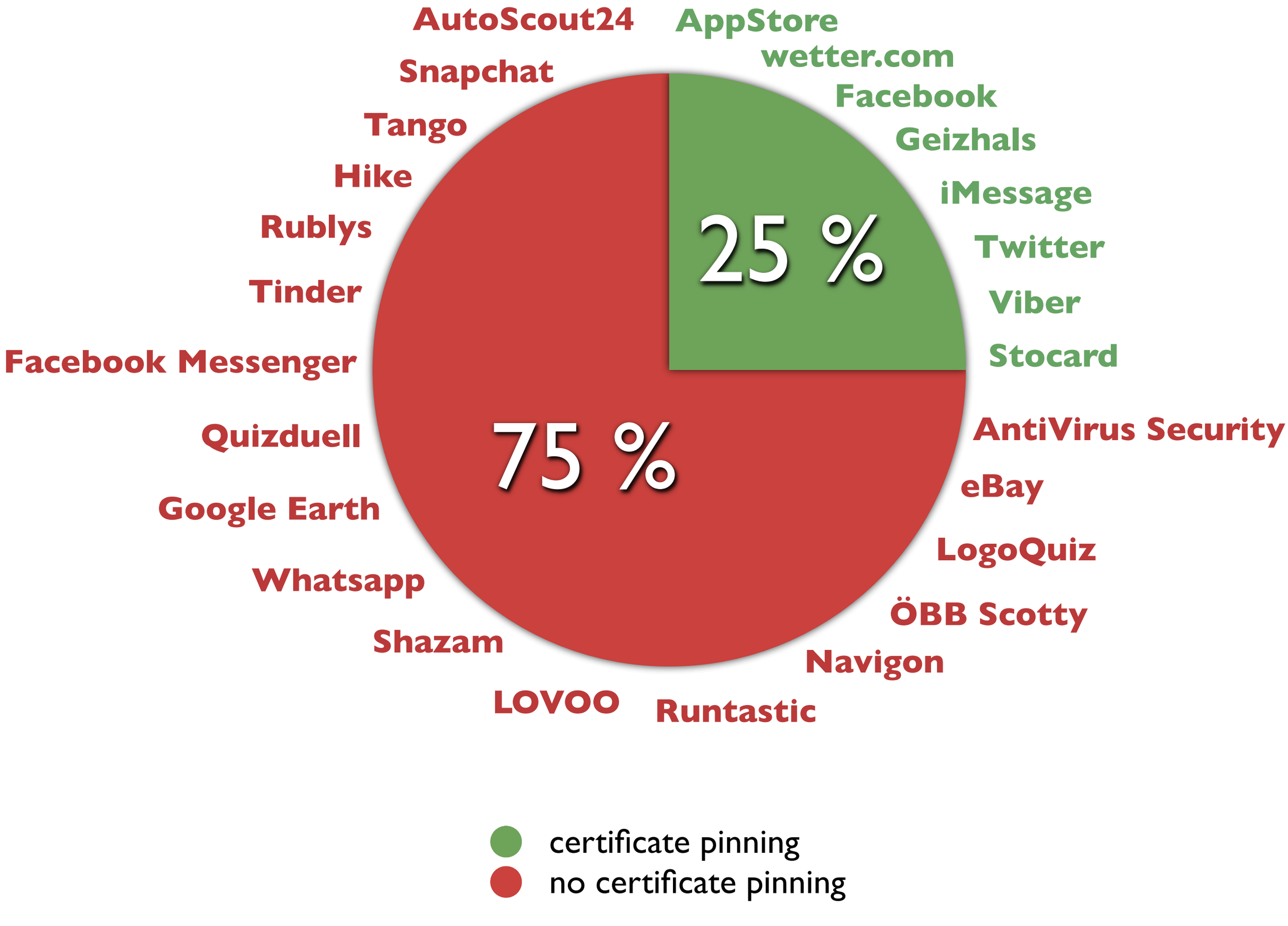
Certificate Pinning

Verification if particular certificate is used

Increased security

Reduced costs

Less flexibility


AutoScout24
Snapchat
Tango
Hike
Rublys
Tinder
Facebook Messenger
Quizduell
Google Earth
Whatsapp
Shazam
LOVOO
Runtastic
Navigon
ÖBB Scotty
LogoQuiz
eBay
AntiVirus Security
Stocard
Viber
Twitter
iMessage
Geizhals
Facebook
wetter.com
AppStore
25 %
75 %
certificate pinning
no certificate pinning

Deutsche Bank

Westpack Banking

Erste Bank

Sparkasse

BNI Internet Banking

Union Bank

Alpha Bank

UBS Mobile Banking

Commerzbank

Postbank

E-Banking apps?

Raiffeisen Bank

BPN Paribas

Eniteo DZ Bank

Bank Republic

Volksbank

Bank Austria

Volksbanken Raiffeisenbanken

Targobank

ING Diba

never ever trust the client
(even if it's your own client)!

(the 80's called and want their advice back)

server-side validation of every client request

secure side channel

establish a trusted second channel

Conclusions

- Many smartphone applications implement insecure protocols

- These protocols are hidden behind transport encryption, which does not prevent protocol analysis

- Don’t rely on *Security through Obscurity*

Peter Frühwirt

IT-Sicherheitsforscher, SBA Research
Doktoratsstudent TU Wien

pfruewirt@sba-research.org

Mobile Security | Digital forensics in Databases

Sebastian Schrittwieser

Dozent Fachhochschule St. Pölten
Doktoratsstudent TU Wien

sebastian.schrittwieser@fhstp.ac.at

Code obfuscation | Fingerprinting of anonymized microdata
Mobile security | Digital forensics | Research ethics