Security Through Obscurity

... powered by HTTPS!

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

redacted version
Live-Demo on Wowtalk
1. (HTTPS): Request

2a. (SMS): PIN

2b. (HTTPS): 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", (int)err);
    goto fail;
}

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
Quizduell
extremely popular in Germany
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> & [...]
Photoswap
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
75%

25%

certificate pinning
no certificate pinning
E-Banking apps?

Erste Bank
Sparkasse

UBS Mobile Banking

E-Banking apps?

BNI Internet Banking

Commerzbank

Deutsche Bank

Raiffeisenbanken

BPN Paribas

Bank Republic

ING Diba

Targobank

Raiffeisen Bank

Union Bank

Alpha Bank

Postbank

Volksbank

Bank Austria

Volksbanken Raiffeisenbanken
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