iPhone Crypto

Ralf-Philipp Weinmann
<ralf@coderpunks.org>

Problem

- Phone is locked to SIM card
- unlocking possible, but costs $$$
- price differential between European unlocked phones and locked AT&T phones:
  - approx. 444 EUR

Bigger problem

- I don't actually wanna use it as a phone
- Why: Security on the device ***sucks***!
- However: Speaker finds broken crypto implementations amusing and intriguing
- Also: makes for a great GSM sniffer (baseband runs on an ARM CPU)

Bootloader

- Bootloader 4.6 (most recent version) verifies signature of baseband firmware using a RSA certificate with e=3
- Duhhh.. Flashback, Bleichenbacher, CRYPTO 2006 rump session?
- No. Unfortunately not.
- Previous versions however exploitable

However

- People are actively trying to apply the results of the CRYPTO 2001 paper by Brier, Clavier, Coron and Naccache
- multiplicative attack for RSA signatures with fixed-pattern padding

Network Code Keys

- Used for unlocking phones using an AT command:
  `AT+CLCK="PN",0,”NCK”`
- NCK: 15 digit decimal numbers

Verification of NCKs

- K = SHA1(f(NCK,NORID,CHIPID))
- M = TEA_decrypt_CBC(SecZone, K)
- D = RSA_decrypt(M, RSAKey)
- is D a valid PKCS#1 message?
- check whether msg contains NORID, CHIPID
- function f actually uses 3 passes of TEA for mixing in NORID and CHIPID!

Bruteforcer

- George Hotz wrote a brute-forcer for the NCKs
- Does about 60k NCKs/sec on my lapop
- 400k NCKs/sec on a 4-core Opteron box (AMD 2218, 2.6GHz)
- Willing to wait for a week: 4134 of these boxes needed. Hmmm.