Blackphone

Jon Callas
CTO and co-founder, Silent Circle

The Device — Blackphone 2

- Android Lollipop (5.1.1)
- Qualcomm hardware
- Medium-to-high end hardware specs
  - 64-bit, 8-core, 3GB RAM
- Spaces virtualization, based on SE Android, not hypervisor
- Target customer is non-technical professionals

Blackphone Features (1)

- Fine-grained app permissions
- Spaces
  - Four virtual phones, one with Google Services
- Silent Circle Services - Secure Voice and Texting

Blackphone Features (2)

- Rapid update of software, bugs fixed quickly
- Often before main Android release
- Silent Store recommendations layer over Google Play Store

Near Future Enhancements

- Android Marshmallow OS
- Privacy meter, monitoring
- Baseband security guidance
    - Includes Silent Circle comms

Much of what makes Blackphone is not crypto

Blackphone Crypto

- Storage encryption via Android
  - Enhanced easy setup, improvements over stock
- ROM / OS signing
- Curated Certificate Store
- Certificate pinning on all SSL
- Silent Circle Service communications

Silent Circle Comms

- Voice/Video via ZRTP + SDES
  - End-to-End with app-to-app
  - SDES alone to PSTN connection
- Texting security through SCIMP/Axolotl±
- Verification mixes ZRTP/Texting modes

Crypto, pre-Snowden

- Philosophical Guidance
  - Choices are good, but choices are bad
  - Too many parameters is hard to do, maintain
  - Create parameter suites
    - P-384 ECC, AES, CCM/CTR, SHA-2
    - 128-bit, 256-bit suites
    - Implementations in C and JS (via SJCL, 128-bit suite)

Two Suites are Important!

- General crypto agility is vital, but easy to overdo
- Two suites means suite-selection gets tested
- This is all software engineering, planning for updates

We succeeded in convincing amateurs not to design crypto, but the crypto people think they can do UX

Crypto people also
think API design is easy

Crypto people think software and release engineering is impossible

Software lifecycle includes end-of-life

Many crypto breaks are really just bad lifecycle management!

Two lifecycle problems

- Bringing in new things you couldn't have thought of
- Retiring things that are at their end of life
  - These can be small or large
  - As small as a protocol parameter, even

Crypto, post-Snowden

- Many users feared security of AES, P-384, SHA2
- Crypto needs confidence in addition to security
- Bernstein/Lange offer to create new EC
  - This is 41417
  - We need greater than 128-bit security because users want it

User Confidence Issues

- Crypto users are passionate
- They have strong opinions, likes, dislikes
  - These may not be rational to us
  - They are real and best worked with

Familiar Options

- ZRTP, like OpenPGP already had options for Twofish. Also support for Skein one-pass-MAC
- Create a new “Non-NIST” cipher suite (256 bits only)
    - P-384 ⇨ 41417
    - AES ⇨ Twofish
    - SHA-2 ⇨ Skein
- Preference in UI for NIST/Non-NIST

Observations

- This is arguably only “marketing" but is there for real user demand

- The new block cipher and hash are NIST competition finalists

- 41417 has nice characteristics: very fast compared to NIST curves, implementations are simpler

- The spread didn’t go to SSL, BP storage, etc.

Deployment

- Previous testing of suite negotiation made it easy
- Old software rejected new suite
- New software preferred it by default
  - At present conflicts resolve to non-NIST

A Tale of Good Intentions

- SC Services are supposed to work like normal dialer, texter.
- Must authenticate user to services
  - Via full-entropy password the user never sees
- Unlocking phone unlocks the app; no *mandatory* secondly passcode
- Has to run when the phone is locked

No "keychain" in Android

- If you want to protect the credentials you need encrypted DB
- If you want encrypted DB, you need a key
- Key needs to come from a user passcode, separate from unlock, and disk encrypt passcode
- End result “Silent Key Manager” that just annoys people. We removed it after a while

Summary

- The real world of Blackphone is that it is privacy-enhanced Android with fast patching

- Crypto management is part of the complete system

- Software Engineering concerns, especially release engineering, drive most of the real security, and crypto is one of these.

Questions?