Crypto Projects that Might not Suck

CloudFlare Crypto Meetup
July 2014

Steve Weis
PrivateCore

#CryptoMightNotSuck

Today’s Talk

- Goal was to learn about new projects and who is working on them.
- Projects marked with ☢ are experimental or are relatively new.
- Tried to cite project owners or main contributors; sorry for omissions.

Methodology

- Unscientific survey of projects from Twitter and mailing lists
- Excluded closed source projects & crypto currencies
- Stats:
  - **1300** pageviews on submission form
  - **110** total nominations
  - **89** unique nominations
  - **32** mentioned today

The People’s Choice

- **Open Whisper Systems**: https://whispersystems.org/
  - Moxie Marlinspike (@moxie) & open source community
  - Acquired by Twitter 2011

- **TextSecure**: Encrypt your texts and chat messages for Android
  - OTP-like forward security & Axolotl key racheting by @trevp
  - https://github.com/whispersystems/textsecure/

- **RedPhone**: Secure calling app for Android
  - ZRTP for key agreement, SRTP for call encryption
  - https://github.com/whispersystems/redphone/

Honorable Mention

- ☢ **Networking and Crypto Library (NaCl):** http://nacl.cr.yp.to/
  - Easy to use, high speed XSalsa20, Poly1305, Curve25519, etc
  - No dynamic memory allocation or data-dependent branches
  - DJ Bernstein (@hashbreaker), Tanja Lange (@hyperelliptic), Peter Schwabe (@cryptojedi)

- ☢ **libsodium:** https://github.com/jedisct1/libsodium
  - Portable, cross-compatible NaCL
  - OpenDNS & Frank Denis (@jedisct1)

The Old Standbys

- **Gnu Privacy Guard (GPG)**: https://www.gnupg.org/
- **OpenSSH**: http://www.openssh.com/
- **Tor**: https://www.torproject.org/
- **Off-the-Record (OTR)**: https://otr.cypherpunks.ca
  - Ian Goldberg & Jake Applebaum (@ioerror)
  - Used by several clients, including derivative by TextSecure
  - ☢ Invisible.im: New project XMPP/OTR using Tor Hidden services

The SSL Libraries

- **OpenSSL**: Seriously. https://www.openssl.org/
- ☢ **LibreSSL**: http://www.libressl.org/
  - Hilarious code reviews
  - OpenBSD team and Bob Beck (@bob_beck)
- ☢ **BoringSSL**: https://boringssl.googlesource.com/boringssl/
  - Google's OpenSSL fork by Adam Langley (@agl__)

JavaScript Crypto Libraries

- **Stanford JS Crypto Lib (SJCL)**: https://crypto.stanford.edu/sjcl/
  - Audited for Crypton.io from SpiderOak & David Dahl (@deezthugs)
  - Emily Stark, Mike Hamburg, & Dan Boneh

- ☢ **Microsoft JS Crypto Library**
  - 800 MB of test vectors for 9000 lines of code
  - Non-commercial and research license only

Browser Crypto

- ☢ **End-to-End**: https://code.google.com/p/end-to-end/
  - OpenPGP in a Chrome Extension
  - Google, Drew Hintz (@DrewHintz) & Eduardo Vela (@sirdarckcat)

- ☢ **WebCrypto**: http://www.w3.org/TR/WebCryptoAPI/
  - Native crypto support in the browser
  - Used for PKI by **PKIjs.org**.
  - Ryan Sleevi (@sleevi_) / Google & Mark Watson / Netflix

Online Storage

- **Tahoe-LAFS**: https://tahoe-lafs.org/
  - Distributed, provider-independent cloud storage
  - Least Authority Systems, Zooko (@zooko), et al.

- **Tarsnap**: http://tarsnap.com
  - Client-side encryption; must build from source
  - Commercial service archives on S3
  - Colin Percival (@cperciva)

Libraries and Frameworks

- **Crypto++**: http://www.cryptopp.com/
  - Long-lived C++ crypto library by Wei Dai
- **go.crypto**: http://golang.org/pkg/crypto/
- **Keyczar**: http://keyczar.org
  - Simple crypto library wrapper for Java, Python, and C++
  - Google, Ben Laurie (@benl), Steve Weis (@sweis), many others

Libraries and Frameworks

- ☢ **Cryptography.io**: https://cryptography.io/
  - Attempt to build a good Python crypto library
  - Paul Kehrer (@reaperhulk) & Alex Gaynor (@alex_gaynor)

- ☢ **ECClib:** http://research.microsoft.com/en-us/projects/nums/
  - Microsoft Research & Patrick Longa (@PatrickLonga)

Messaging and Publishing

- ☢ **Pond**: https://pond.imperialviolet.org/
  - Forward secure, asynchronous messaging
  - Adam Langley (@agl__)

- ☢ **Cryptosphere**: http://cryptosphere.org/
  - Peer-to-peer content publishing
  - Tony Arcieri (@bascule)

Community Efforts

- **Open Crypto Audit Project (OCAP)**: https://opencryptoaudit.org/
  - Audited TrueCrypt. Great technical advisory board.

- **Better Crypto**: https://bettercrypto.org/
  - Community-generated guidelines for applied crypto hardening

-  **Password Hashing Competition**: https://password-hashing.net/
  - Community-driven contest for password hashing replacement

-  **Safe Curves**: http://safecurves.cr.yp.to/
  - Criteria to ensure elliptic-curve crypto security
  - DJ Bernstein (@hashbreaker) & Tanja Lange (@hyperelliptic)

Experimental Toolkits

- ☢ **Relic Toolkit:** https://code.google.com/p/relic-toolkit/
  - Bilinear maps, pairing-based crypto, ID-based crypto
  - Implemented in C
  - Diego Aranha (@dfaranha) and C.P. L. Gouvêa

- ☢ **CHARM:** http://www.charm-crypto.com/
  - Tool for rapid cryptographic prototyping
  - Bilinear maps, multiparty protocol engine, non-interactive ZK
  - Python with native C modules
  - JHU ISI: J. Ayo Akinyele (@ja_akinyele), et al.

Miscellaneous Project

- ☢ **Cryptol:** http://cryptol.net/
  - Domain-specific language for specifying crypto algorithms
  - Galois Inc. & Adam C. Foltzer (@acfoltzer)

- ☢ **libsnark:** https://github.com/scipr-lab/libsnark
  - C++ library for zero-knowledge proof system with succinct proofs
  - Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza

- ☢ **libmacaroons:** https://github.com/rescrv/libmacaroons
  - Decentralized authentication for distributed systems
  - Paper: Chalmers/Brown/Google; Code: Robert Escriva (@rescrv)


Thanks!