6.111 Project Checklist

Andres Erbsen   Adam Yedidia

November 14, 2014

Basic goal: phone system and crypto

- A working phone system: what is spoken to one labkit's microphone is heard from the other's headset. Communication between the two labkits is done in a digital fashion in discrete packets.
- In simulation (and synthesizable): public key cryptography to generate a public key from a secret key and establish a shared key in less than one second along with automated software tests that verify that the implementation conforms to the Curve25519 specification.
- In simulation (and synthesizable): secret key cryptography for encrypting a stream at the required rate (estimated 1Mbit/s) along with automated tests that verify that the implementation conforms to the ChaCha specification.

Main goal: encrypted phone system

1. Each labkit collects high-quality randomness to create a secret key. The quality of the randomness will be estimated using the amount of entropy per output bit before compression.
2. Each labkit computes a public key from their own secret key and they both compute *the same* shared secret from their own secret key and the other's public key (verified by step 3 and in simulation).
3. The audio information sent over the wire is encrypted using the shared key. The phone still works. The quality encryption is notoriously hard to test, but we will demonstrate obfuscation by inspecting the waveform and the encryption module is separately verified in simulation.

Stretch goal: encrypted and authenticated phone system

1. Each labkit displays the hash of the two public keys it has seen: its own, and the one of the labkit it is communicating with. The verification code on two labkits' displays is the same if and only if they are communicating with each other – users can detect man-in-the-middle attacks.
2. Before revealing its own public key, each labkit requires the other to commit to a particular public key by sending a hash of it (which is later verified). Therefore, an attacker cannot try possible values for its own public key until they find one that when combined with the victim's produces the desired verification code. Verify code (simulated against BLAKE spec).
3. Extra stretch: All audio packets are authenticated so the attacker cannot blindly modify them.

References

Curve25519 definitive paper: http://cr.yp.to/chacha/chacha-20080128.pdf.
Curve25519 known-answer tests: https://code.google.com/p/go/source/browse/curve25519/curve25519_test.go?repo=crypto

ChaCha20 definitive paper: http://cr.yp.to/chacha/chacha-20080128.pdf.
ChaCha20 known-answer tests: https://tools.ietf.org/html/draft-agl-tls-chacha20poly1305-04

BlAKE definitive paper, with known-answer tests: https://131002.net/blake/blake.pdf.