Introduction to Trusted Computing: Crypto and Security Basics

Ariel Segall
ariels@alum.mit.edu

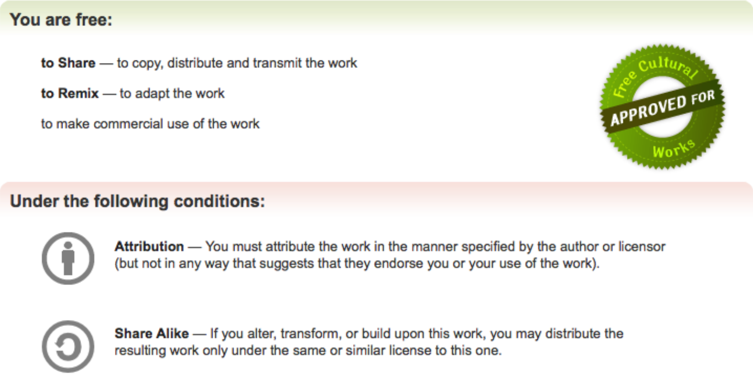
Day 1

Approved for Public Release: 12-2749.
Distribution unlimited

License

All materials are licensed under a Creative Commons “Share Alike” license.

- http://creativecommons.org/licenses/by-sa/3.0



You are free:

to Share — to copy, distribute and transmit the work

to Remix — to adapt the work

to make commercial use of the work

Under the following conditions:

Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

The Lightning Review

Goal: quickly familiarize you with the following concepts, or refresh your memory

- Core security principles
- Nonce
- Cryptographic keys (symmetric and asymmetric)
- Hashes
- Common attack terms

Confused? Ask questions early and often!

What do we mean by secure?

Three basic concepts:

- Confidentiality (Secrecy)
- Integrity
- Availability

Trusted computing focuses on the first two.

Freshness and Nonces

- We often want to be sure that data is *fresh*, or recent.
  - Am I actually talking to you now, or is this a recording?
- Our primary tool: *nonces*
- Nonce: *freshly generated* random number
  - Must be unpredictable!
- Nonce generator knows any message containing their nonce was created after the nonce
- Allows locally verifiable confirmation that remote activity current
  - Timestamps aren't verifiable! Too predictable.

Cryptographic Keys

Two main types:

- Symmetric keys
- Asymmetric keys
  - aka “public keys”, “public-private key pairs”

Symmetric Key Cryptography

- Same key used for all operations: encryption vs. decryption, signing vs. verifying
- Usually very fast, good for bulk operations
- Big disadvantage: key distribution
- Not a primary topic for today

Public Key Cryptographic (Asymmetric)

- Keys come in pairs: one public, one private
  - Public key is just that: no security risk from world knowing
  - Private key must be kept secret.
- Private key used for decryption, signing
- Public key used for encryption, verification
- Great for proofs of identity
- Slow to use; not very good for bulk operations
- RSA: most common public key algorithm in use now

Hashes

- Cryptographic hash: one-way function from arbitrary data to fixed length
- Critical hash properties:
  - Easy to calculate
  - Infeasible to reconstruct data from hash
  - Infeasible to find collisions (different data, same hash)
  - Infeasible to modify data without changing hash
- SHA1: hash algorithm primarily referred to in this class
  - More recent algorithms exist; not widely supported in hardware yet

Common Attack Terms

Denial of Service (DoS) Attack where adversary causes service to be unavailable, temporarily or permanently. DoSes can also happen by accident.

Man in the Middle (MitM) Attack where adversary fowards messages between parties, potentially modifying them, to deceive one or both parties or to reveal supposedly secret information.

Questions?