Security

CS 241

Dec 4, 2013

8f6e31c6a268c8bdf0f9fe4522f0dceed7adfd866c0622934425bc5ecb43ad10

“Security” is a **very** broad topic…

- “Security” describes
  - Hardware
  - Software
  - Data
  - People
  - Policies
  - Procedures
  - Governance

…even the best software algorithm has several points of failure!

Case Study: AACS encryption

- AACS: “Advanced Access Content System”
  - Copyright protection on HD DVD media

- What happened?

Case Study: AACS encryption

- AACS: “Advanced Access Content System”
  - Copyright protection on HD DVD media

- What happened?
  - PowerDVD and AnyDVD software stored the “master” decryption key in RAM
    - Analysis: “nothing was hacked, cracked, or reverse engineered”, “no debugger was used”, “no binaries changed”
  - **`09F911029D74E35BD84156C5635688C0`**

Encryption Algorithms

- **Two-way encryption**
  - Used to share information privately/securely between multiple parties.
  - Ex: HTTPS (SSL), SSH, PKI, RSA, etc
  - Learn more: **CS 461: Computer Security I**

- **One-way validation**
  - Used to validate previously known data
  - Ex: cryptographic hash functions
    - MD5, SHA-0, SHA-1, SHA-256, SHA-3, …

Cryptographic Hash Function

- Any general **hash function**:
  - Takes in data and produces a numeric result
  - Java: Object.hashCode()
    - Used for hash tables, fast string comparisons, etc.

Cryptographic Hash Function

- A **cryptographic hash function** should be:
  - Easy:
    -
  - Hard / Impossible:
    -
    -
    -

SHA-2/256 Examples

- (empty string)
  - **e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855**
- The quick brown fox jumps over the lazy dog
  - **d7a8fbb307d7809469ca9abcb0082e4f8d5651e46d3cdb762d02d0bf37c9e592**
- The quick brown fox jumps over the lazy dog.
  - **ef537f25c895bfa782526529a9b63d97aa631564d5d789c2b765448c8635fb6c**
- The quick brown fox jumps ovar the lazy dog.
  - **02e4625126139fbd3f91e44749fa51a9f7aeabeb63301cb251be1904b7c668c0**

Storing Passwords

- How does Facebook store a password?

What's wrong?

- "password"

  ➔ (SHA-256) ➔

5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

Storing Passwords

- How does Facebook store a password?

Password Salt

- A salt is a string added to the input before a hash function is applied.
  - A different salt must be used for every input.

- Why use a salt?