FSEM 1111 Computer Security – from a Free Software Perspective

Christian Grothoff
christian@grothoff.org

http://grothoff.org/christian/

Protocols

- "A **protocol** is a series of steps, involving two or more parties, designed to accomplish a task."
- Everyone involved must know the steps in advance and agree to follow it.
- The protocol must be complete and unambiguous.
- For cryptographic protocols, it should not be possible to do more or learn more than what is specified in the protocol.

Dramatis Personae[1]

- Alice, Bob, Carol and Dave
- Eve – Eavesdropper
- Mallory – Malicious active attacker
- Trent – Trusted arbitrator
- Walter – Warden
- Peggy – Prover
- Victor – Verifier

[1] More at `http://en.wikipedia.org/wiki/Alice_and_Bob`

Efficiency

- Number of steps in protocol
- Size of messages
- Conflict resolution cost:
  1. Involvement of trusted party (arbitrated protocols)
  2. Resolution by trusted party on dispute (adjudicated protocols)
  3. Self-enforcing protocols

Attack Personae

- Eavesdroppers
- Passive cheaters
- Active cheaters
- Real-world adversaries – Mallory

Example: Secret Splitting

1. Trend generates a random key K of the same size as the secret M and computes $M xor K = E$
2. Trend gives Alice K.
3. Trend gives Bob E.

Example: Symmetric Cryptography

1. Alice and Bob agree on a cryptosystem
2. Alice and Bob agree on a key
3. Alice encrypts plaintext with key
4. Alice sends ciphertext to Bob
5. Bob decrypts ciphertext and reads it

One-Way (hash) Functions

- Easy to compute $f(x)$, hard to compute $f^{-1}(y)$
- Trapdoor one-way hash functions: hard to compute f^{-1} without the secret
- Good hash functions are collision-free: it is hard to generate two pre-images with the same hash value

Alternative names

- Contraction function
- Message digest
- Fingerprint
- Cryptographic checksum
- Message integrity check (MIC)
- Manipulation detection code (MDC)
- Message authentication code (MAC) $\equiv$ hash + key

Hash-based Authentication

1. Alice sends host her password P
2. Host compares $H(P)$ with database of hashed passwords

Salt

- Need to prevent Mallory from building database of all (common) passwords (**dictionary attack**)
- **Salt** is a random string that is concatenated with the password before hashing.
- Database contains salt S and hash $H(P + S)$

$\Rightarrow$ Mallory needs larger database

Public-key Cryptography

The mathematical primitive is often similar to trapdoor one-way hash functions.

Canonical use:

1. Alice and Bob agree on a public-key cryptosystem.
2. Bob sends Alice his public key.
3. Alice encrypts her message using Bob's public key.
4. Alice sends the ciphertext to Bob.
5. Bob decrypts Alice's message using his private key.

Signatures

Autenticic: The signer deliberately signed the document.

Unforgeable:
Nobody but the signer signed the document.

not reusable:
The signature cannot be moved to another document.

Unalterable:
The document cannot be changed after signing.

not repudiatable:
The signer cannot later claim not to have signed it.

Questions

?

Problem

Alice has an item x, and Bob has a set of five distinct items $y_1, \ldots, y_5$. Design a protocol through which Alice (but not Bob) finds out whether her x equals any of Bob's five items; Alice should not find out anything other than the answer ("Yes" or "No") to the above question, and Bob should not know that answer. Your solution must always be correct, not just with high probability.

Defining Risk

Numerous different definitions of risk exist. We will quantify risk as:

$$\text{Risk} = \text{Probability} * \text{Impact}. \tag{1}$$

Risk and Business

Insurance is a risk-reducing investment in which the buyer pays a small fixed amount to be protected from a potential large loss.

Gambling is a risk-increasing investment, wherein money on hand is risked for a possible large return, but with the possibility of losing it all.

An operation with greater risk should have greater (potential) returns.

Risk Management

- Risk Identification
- Risk Assessment
- Risk Mitigation

Risk Identification

- Objectives-based (which events can endanger us reaching our target(s)?)
- Scenario-based (simulate various possible event chains)
- Taxonomy-based (use answers to pre-defined set of questions to reveal risks)
- Common-risk Checking (check set of known risks)

Risk Assessment

Risk assessment should be rational, but humans are not:

- Humans discount the risk of extreme events – the probability is too low or the risk too high for intuitive evaluation.
- Humans tend to underestimate the probability of events they personally control (car accidents) and overestimate the probability of events they cannot control (plane accidents)

Problems in Risk Assessment

Wishful Thinking Disturbing events that the assessment team wishes not to happen may be ignored in analysis.

Trauma Extremely disturbing events that did happen may continue to be ignored despite the fact that they have occurred and thus have a nonzero probability.

Inevitable Events Events that are inevitable may be ruled out of analysis due to unwillingness to admit that they are inevitable.

Mitigating Framing Problems

Require that the scenarios **must** include unpopular (high-impact), unbelievable (low-probability) threats or events.

$\Rightarrow$ participants can justify raising their fears as part of satisfying formal process requirements.

Risk Mitigation

- Purchase Insurance
- Change Process
- Abort Operation