COMP2121 Lab 9

Security

The goal of this tutorial is to better understand the main technique to achieve integrity, authentication and confidentiality and their applications to exchange information among peers.

Exercise 1: Integrity vs. confidentiality

What is the difference between integrity and confidentiality? Provide a scenario where confidentiality is satisfied while integrity is not.

What is the main difference between a symmetric crypto-system (i.e., using secret key) and an asymmetric crypto-system (i.e., using public-private key)?

In what way does a hash of a message provide a better message integrity check than a checksum (such at the Internet checksum)?

Can you decrypt the hash of a message to get the original message if you know the hash function? Explain your answer.

Can you decrypt a message encrypted with a private key if you only have the private key? Explain your answer.

Duration: 15 min

Exercise 2: Torrent integrity

In the BitTorrent P2P file distribution protocol, the seed breaks the file into blocks, and the peers redistribute the blocks to each other. Without any protection, an attacker can easily weak havoc in a torrent by masquerading as a benevolent peer and sending bogus blocks to a small subset of peers in the torrent. These unsuspecting peers then redistribute the bogus blocks to other peers, which in turn redistribute the bogus blocks to even more peers. Thus, it is critical for BitTorrent to have a mechanism that allows a peer to verify the integrity of a block, so that it does not redistribute bogus blocks. Assume that when a peer joins a torrent, it initially gets a `.torrent` file from a *fully* trusted source. Describe a simple scheme that allows peers to verify the integrity of blocks.

Duration: 10 min

Exercise 3: Authentication and confidentiality

Suppose Alice wants to send an e-mail to Bob. Bob has a public-private key pair (K_B^+, K_B^-) and Alice has Bob's certificate. But Alice does not have a public, private key pair. Alice and Bob (and the entire world) share the same hash function $H(.)$

1. In this situation, is it possible to design a scheme so that Bob can verify that Alice created the message? If so, show how with a block diagram for Alice and Bob.
2. Is it possible to design a scheme that provides confidentiality for sending the message from Alice to Bob? If so, show how with a block diagram for Alice and Bob.

Duration: 10 min

Exercise 4: RSA

Consider RSA with $p = 5$ and $q = 11$

1. What are n and z?
2. Let e be 3. Why is this an acceptable choice for e?
3. Find d such that $de = 1 \bmod z$.
4. Encrypt the message $m = 8$ using the key (n, e). Let c denote the corresponding cyphertext.

Duration: 15 min