Lecture 2

Friday, 10 February 2023 08:38

Security deals with (digital) systems

Safety is related to the real world (especially people)

---

attacker models provide assumptions regarding attacker capabilities & behaviors

an attack is a specific set of actions carried out by an attacker through a specific set of capabilities & tools, to reach a specific malicious goal

passive attacker model
- eavesdropper
- honest-but-curious

active attacker model
- Dolev-Yao
- Canetti & Krawczyk
- Cyber-Physical Dolev-Yao

passive attackers do not modify communication, but they can perform offline activities

active attackers modify / inject traffic

attacker tools are a set of devices and systems that the attacker can use to generate an attack

passive
- receiving antenna
- data mining capabilities

active
- receive + transmit
- message generation
- optionally: data mining capabilities, (critical) knowledge of secrets

attack model: specific usage of a set of capabilities and tools to cause damage to another system

passive: eavesdropping, traffic analysis
active: man-in-the-middle / impersonation, replay attack
threat model: practical damage caused by an attack

one-way hashing functions

input message m b bits

output digest h n bits such that $h = H(m)$

one-way computationally unfeasible to obtain m from h

weak collision resistance computationally hard to find $y \neq x$, such that $H(x) = H(y)$ given x

strong collision resistance computationally hard to find $y \neq x$, such that $H(x) = H(y)$ not given x

services provided by hashing

message integrity verification — digest matches reconstruction

signatures, i.e. authenticity — encrypt hash, then verify integrity

hashes do not provide confidentiality, since the message cannot be recovered (exc. by a authorized party)

→ they can only verify the information

in this year's iteration of the course, the security algorithms are public

cryptography provides secure, reversible transformations

elements of a cryptosystem

- plaintext m
- ciphertext c
- encryption key k
- encryption algorithm $E(m, k) = c$
- decryption key k'
- decryption algorithm $D(c, k') = m$

symmetric cryptography: $k = k'$

asymmetric cryptography: $k \neq k'$

- confidentiality — key distribution
- message authentication
- data confidentiality and authentication

we do not consider privacy to be a security service

here Diffie-Hellman does not achieve authentication

ElGamal will not be asked for; the slide is just for reference.

Elliptic curves — any scalar can be mapped to a point on curve using the generator: $A = a \cdot G$
- addition gives another point on curve $C = A + B$
- multiplication gives another point on curve $C = A \cdot B$

→ efficient, hence often used in IoT

ElGamal / ECDH details will not be asked in exam