{ CSCI 6331 · 4331 | Lecture 5 }

Cryptography

Hoeteck Wee · hoeteck@gwu.edu

http://tinyurl.com/cryptogw/

Announcements

- Evaluation:

  10% In-Class/Piazza, 20% Final Presentation / Project

  30% Homework, 40% Final (Apr 25)

- Homework 3 will be out by Sun (Feb 19)

  due Feb 29 (Wed) in class

Message Integrity

Example. Bank gets message "Transfer one thousand dollars from account A to B"

- Is message authentic? i.e. really from owner of account A?
- If so, were the details tampered with? Intended amount? Intended recipient?

Note. message not a secret, privacy not an issue

Message Integrity

Goal. Protect Integrity of communication

Trust Model. Three entities, sender, receiver. Allow tampering on channel

Who is the adversary? Active adversary

Powers? Can change messages exchanged between sender and receiver

What constitutes a break? Change message without being detected

- orthogonal to secrecy, relevant regardless whether encryption is applied

One-Time Pad. example of perfect cipher

- $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^\ell$; Gen outputs a random ℓ-bit string k
- $\mathrm{Enc}_\mathrm{k}(\mathrm{m}) = \mathrm{k} \oplus \mathrm{m}$ (bit-wise XOR)
- attack: adversary flips the first bit; Q. what happens to message?
- error-detection codes are insufficent

Message Authentication Codes

setting.

- both users generate and share a *secret* key k in advance
  — runs key generation algorithm $\mathrm{k} \leftarrow \mathrm{Gen}(1^{\mathrm{n}})$
- to send message m, sender computes a MAC tag t and sends (m, t)
  — runs tag generation algorithm $\mathrm{t} \leftarrow \mathrm{Mac}_{\mathrm{k}}(\mathrm{m})$
- upon receiving (m, t), receiver verifies whether t is a valid tag on m
  — runs verification algorithm $\mathrm{Vrfy}(\mathrm{m}, \mathrm{t}) \in \{0, 1\}$ (1 being valid)

syntax. *message authentication code* (MAC) is a triple of randomized algorithms

$(\mathrm{Gen}, \mathrm{Mac}, \mathrm{Vrfy})$

- correctness. for every key k output by $\mathrm{Gen}(1^{\mathrm{n}})$, and every $\mathrm{m} \in \{0, 1\}^*$, we have $\mathrm{Vrfy}_{\mathrm{k}}(\mathrm{m}, \mathrm{Mac}_{\mathrm{k}}(\mathrm{m})) = 1$.

Message Authentication Codes

Security Definition. hard to generate a valid tag on any "new" message that was not previously sent – existentially unforgeable under adaptive chosen-message attack

Q. adversary's power?

— observe communication $\Rightarrow$ can see all messages sent by parties + MAC tags

— influence content of messages?

adversary gets access to MAC oracle $\mathrm{Mac}_{\mathrm{k}}(\cdot)$

Q. what constitutes a break?

— adversary outputs message + valid tag (m, t)

i.e. it can fool honest party into thinking (m, t) originates from legitimate party

— "new" message, different from queries to MAC oracle

i.e. replay attack not a "break" (still a security concern)

Message Authentication Codes

Security Definition. hard to generate a valid tag on any "new" message that was not previously sent – existentially unforgeable under adaptive chosen-message attack

1. Generate random key k using $\mathrm{Gen}(1^{\mathrm{n}})$
2. Adversary given 1^{n} and oracle access to $\mathrm{Mac}_{\mathrm{k}}(\cdot)$, eventually outputs (m, t). Let Q = set of queries
3. Wins if $\mathrm{Vrfy}_{\mathrm{k}}(\mathrm{m}, \mathrm{t}) = 1$ and $\mathrm{m} \notin \mathrm{Q}$.

definition. (t, ϵ)-secure if for all advesaries running in time t, winning probability bounded by ϵ.

— too strong? restrict to "legitimate messages"?

— replay attacks, e.g. "transfer $1,000 to my account" times 10?

use time stamps (require clock synchronization)

next. How to build MACs from PRF

Pseudorandom Functions (PRF)

Pseudorandom Functions (PRF) defined over (K, X, Y):

$$F : K \times X \to Y \quad (\text{ key} \times \text{input} \to \text{output })$$

- "efficient" algorithm to evaluate $F(k, x)$

example. AES : $\{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$

intuition. gives us many one-time pads, $F(k,0), F(k,1), F(k,2), F(k,3), \ldots$

1. (challenge bit) random bit $b \leftarrow \{0,1\}$.
2. (challenge function) if $b = 1$, f is truly random function from X to Y;

   if $b = 0$, f is $F(k, \cdot)$ for a random k
3. $\mathcal{A}$ gets $f(0), f(1), f(2), \ldots$
4. $\mathcal{A}$ outputs b' and wins if $b' = b$

definition. $F : K \times X \to Y$ is (t, ϵ)-secure PRF if for all adversaries $\mathcal{A}$ running in time t, winning probability bounded by $1/2 + \epsilon$

Message Authentication Codes from PRFs

Security Definition. hard to generate a valid tag on any "new" message that was not previously sent – existentially unforgeable under adaptive chosen-message attack

1. Gen : choose random $\mathrm{k} \leftarrow \mathrm{K}$
2. $\mathrm{Mac}_{\mathrm{k}}(\mathrm{m})$: output tag $\mathrm{F}(\mathrm{k}, \mathrm{m})$
3. $\mathrm{Vrfy}_{\mathrm{k}}(\mathrm{m}, \mathrm{t})$: output 1 iff $\mathrm{t} = \mathrm{F}(\mathrm{k}, \mathrm{m})$

Q. if F is truly random function, what is the probability of winning?