CSE316
Computer Systems Security

Lab 3. Leakage-resilient AKE

2020-04-22, 13:00-14:00, Wednesday

Jie Zhang
Department of Computer Science and Software Engineering
Email: jie.zhang01@xjtlu.edu.cn
Office: SD561

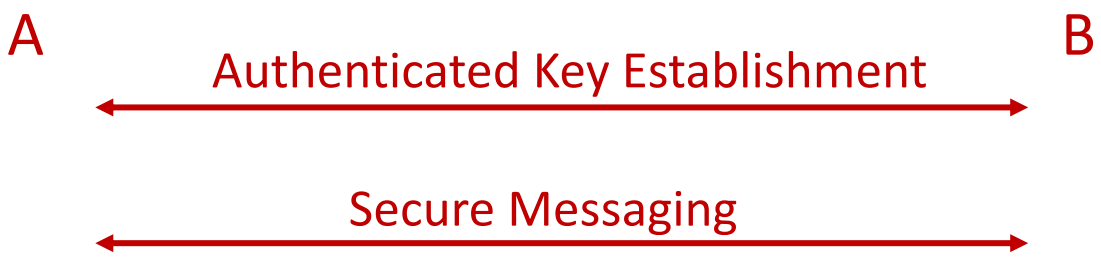
Outline

- Background
- Method

1. Background

Authenticated key exchange

- Security protocols protect communications.



- Phase 1, Authenticated key establishment
  - Establish authenticated shared keys
- Phase 2, Secure messaging
  - Use AES, HMAC, etc., to protect messages under shared keys.

Authenticated key establishment **underlies** the security of communications.

Authenticated key exchange

- Authenticated key establishment
  - A cryptographic mechanism that provides two or more parties communicating over an open network with a shared secret key.
- Category
  - Key transport protocols
    - The shared secret key is created by one party and securely transmitted to the second party.
  - Key agreement (or exchange) protocols
    - Both parties contribute information which is used to derive the shared secret key.
    - Have wide application.

AKE in international standards

- Transport Layer Security (TLS): Handshake Protocol
  - PSK key exchange mode
  - Certificate-based key exchange mode
- IEEE 802.15.6 (WBAN): Authenticated Association
  - Password Authenticated Association
  - Display Authenticated Association
- Bluetooth 5.0: Secure Simple Pairing
  - Numeric Comparison
  - Just Works
  - Out Of Band
  - Passkey Entry

Are those AKA protocols secure enough to underlie the security of communications?

Side channel attacks

- Kerckhoffs' principle
  - A cryptographic system should be secure even if everything about the system, except the key, is public knowledge.
- In AKE
  - Long-term keys (pre shared keys, private keys, or password) are kept secretly.
  - Provable security based on certain computational complexity assumptions.

Auguste Kerckhoffs

Side channel attacks can learn information about **long-term keys**.

Side channel attacks

- Why and how SCAs leak long-term keys?
  - Every cryptographic algorithm is ultimately implemented on a physical device that affects the environment around it in measurable ways
  - SCAs exploit
    - the time taken by a particular implementation of a cryptographic algorithm,
    - the amount of power consumed,
    - the electromagnetic radiation,
    - …

2. Method

Leakage resilient methods

- Hardware level
  - Build hardware that leaks as few information as possible
  - E.g., shielding electromagnetic radiation
- Software/Algorithmic
  - Masking/blinding
    - Concealing se…on with random data
    - Circuit compilers, inner product extractor, secret sharing
  - Other countermeasures
    - Introducing noise in the side channels
    - Random delays, random order execution, dummy operations

We only introduce the simplest ones here

Additive mask

- is usually used in ECC
- Parameters: n is the group order, P is a base point
- To mask the exponent d of $Q = d \cdot P$
- Generate a small random number k
- Blind d with kn: $d' = d + kn$
- Compute $Q = d' \cdot P$

Corollary of Fermat's little theorem:
Let G be a finite group of order m. Then for $g \in G$ and integer x, it holds that $g^x = g^{[x \bmod m]}$

Exponent splitting

- is a variant of the additive mask
- Represent d with a random k and $d' = d - k$
- To mask the exponent d of $Q = d \cdot P$
- Compute $R_1 = k \cdot P$
- Compute $R_2 = d' \cdot P$
- Compute $Q = R_1 + R_2$

Multiplicative mask

- is a multiplicative analogue of exponent splitting
- Parameters: n is the group order, P is a any group element.
- Represent d with a random k and $d' = k^{-1}d$
- To mask the exponent d of $Q = d \cdot P$
- Compute $R = k \cdot P$
- Compute $Q = d' \cdot R$

Tasks

- Design and realize a leakage-resilient AKE protocol
  - use the method introduced in this lecture; or
  - use your self-proposed method