CSE316
Computer Systems Security

Lab 2. Lightweight AKE

2020-04-15, 13:00-14:00, Wednesday

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

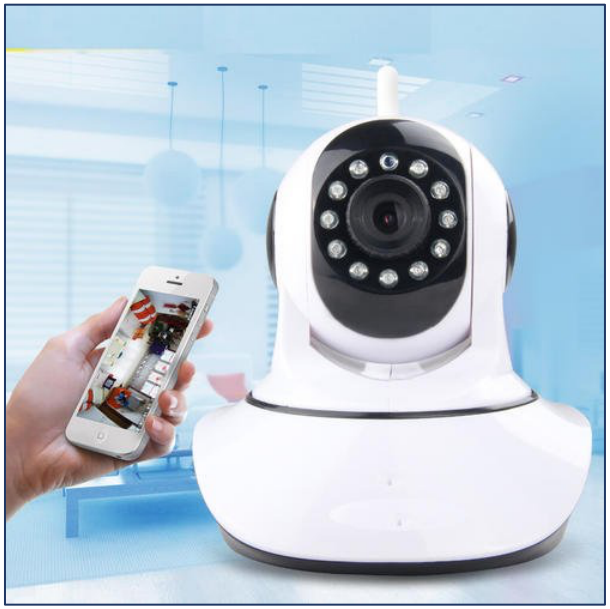
Outline

- Background
- Lightweight method

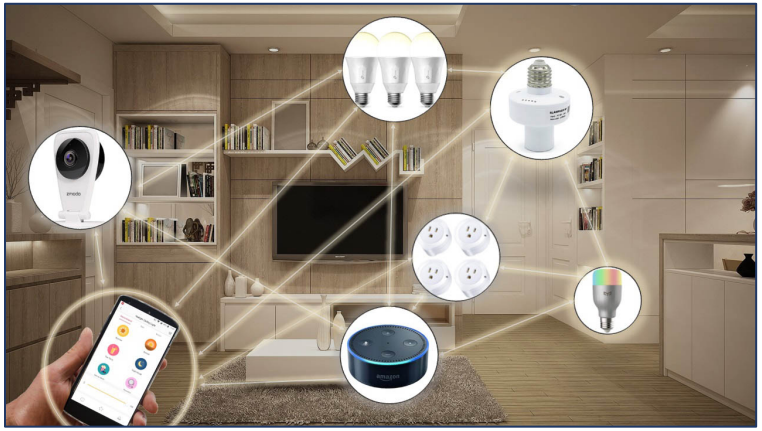
1. Background

Scenario

- Unbalanced capabilities



Common feature?



Scenario

- Communications between
  - a sensor node and a base station
  - a mobile terminal and a cloud center
  - ……
  - devices have different computational capabilities.
- Available AKE protocols
  - Have equivalent computational requirements on the two parties.
- Question
  - How to reduce the burden on the limited party?

2. Method

Offline computation

- Let the limited device to pre-compute some values
- Suffer from ephemeral-secret-leakage (ESL) attacks

- Example

E, G, q

h_1

h_2

Precomputation:

$x \leftarrow Z_q$

$h_1 = xG$

$k_1 = xh_2$

$y \leftarrow Z_q$

$h_2 = yG$

$k_2 = yh_1$

Transferring computations

- Based on a variety of (EC)DH: Yacobi-Shmuely (EC)DH

SK_A, PK_A, PK_B E, G, q SK_B, PK_B, PK_A

U_A

U_B

$K_1 = (U_B \cdot G - PK_B) \cdot R_A$

$R_A \leftarrow Z_q$

$U_A = R_A + SK_A$

$K_2 = (U_A \cdot G - PK_A) \cdot R_B$

$R_B \leftarrow Z_q$

$U_B = R_B + SK_B$

Transferring computations

- Suppose the computational capabilities A<<B
- Transfer the computation $U_B \cdot G$ from Alice to Bob.

SK_A, PK_A, PK_B $\quad$ E, G, q $\quad$ SK_B, PK_B, PK_A

U_A

T_B

$K_1 = (T_B - PK_B) \cdot R_A$

$R_A \leftarrow Z_q$
$U_A = R_A + SK_A$

$K_2 = (U_A \cdot G - PK_A) \cdot R_B$

$R_B \leftarrow Z_q$
$U_B = R_B + SK_B$
$T_B = U_B \cdot G$

Comparison

- Elliptic curve scalar multiplication (i.e., elliptic curve group exponentiation)
  - YS-ECDH
    - First party: $(U_B \cdot G - PK_B) \cdot R_A$
    - Second party: $K_2 = (U_A \cdot G - PK_A) \cdot R_B$
  - Computation-unbalance YS-ECDH
    - First party: $(T_B - PK_B) \cdot R_A$
    - Second party: $T_B = U_B \cdot G, K_2 = (U_A \cdot G - PK_A) \cdot R_B$

	First Party	**Second Party**
YS-ECDH	2	2
Computation-unbalance YS-ECDH	1	3

Tasks

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