Security in Personal Area Network

Jong-Phil Yang
Pukyong National University
Republic of KOREA
Contents

● Personal Area Network (PAN)
● Personal PKI
  ○ Imprinting
  ○ Manual Authentication Protocol
  ○ Security issues
    ○ Certificate and key pair update
    ○ Key status management
    ○ Trust management
● Questions and Conclusion
Personal Area Network (PAN)

- PAN
  - SHAMAN project
    - Security for Heterogeneous Access in Mobile Applications and Networks
    - European Union’s IST (Information Society Technologies)
    - [http://www.ist-shamman.org](http://www.ist-shamman.org)
  - PAN interconnected using wireless communication in license-free spectrum
  - Small ad hoc or semi-permanent networks
  - Range around 10 meters
- Use cases
  - Car scenario, household scenario, office and meeting scenario, campus and public scenario, business meeting scenario
Business meeting scenario

Two persons, an employee and a guest, meet in a room equipped with a video projector. The two persons in the room are both carrying one laptop each. The laptops contain presentation information that the users would like to present to each other using the video projector. Furthermore, after the presentation, the guest would like to send over his presentation to the employee. There are three components in this PAN scenario: a video projector, a guest laptop, an employee laptop. Since the presentation material might be sensitive information, the employee and the guest would like to have the local wireless communication protected from eavesdropping. This can be provided by a proper security protocol and a shared secret that is a part of a security association between the two components.
Initialization of security association

- One association, symmetric keys
  - Manual Authentication Protocol (MANA)
- One association, asymmetric keys
- Group association, symmetric keys
- Group association, asymmetric keys
  - Personal PKI
  - ID-based cryptography
Personal PKI

- Assumption in PAN
  - At least one device acting as a ‘Personal Certification Authority(CA)’, which is responsible for generating public key certificates for all devices within the PAN

- Persona CA
  - It is different from large scale or global CA functions, a function used by an ordinary user for home or small office deployment
  - Similar to any other PKI, we would like all units in a communication network to share CA’s root public key and use certificates issued by a trusted CA
Imprinting PAN component

- Imprinting
  - A PAN component generates key-pair and obtains a corresponding certificate from personal CA

- Steps
  - Personal CA sends its public key $P_{CA}$ together with other relevant information to the PAN component
  - PAN component sends its public key $P_{M}$ together with other relevant information, such as the identity, to the CA
  - The exchanged information $D = \{ P_{CA}, P_{M}, id_{M}, \ldots \}$ is authenticated using a Manual Authentication Protocol
  - CA generates a certificate for the PAN component
  - PAN component verifies the certificate
Manual Authentication Protocol

- In personal PKI
  - A imprinting PAN component does not know a public key of personal CA
  - The personal CA also does not know a public key of imprinting PAN component
- To conform the other’s public key and additional information, MANA can be used
- Three types of MANA
  - **MANA I**
  - **MANA II**
  - **MANA III**

The first device has an output interface suitable for short strings of alphabetic and/or numeric symbols and a simple input interface.

The second device has an input interface suitable for short strings of alphabetic and/or numeric symbols and a simple output interface.
To authenticate a shared data $D$

1. Generates $K$
2. Computes MAC over data $D$
3. Outputs $K$ and MAC (via display)

User reads $K$ and MAC

User enters $K$ and MAC

1. Computes own MAC over $D$
2. Compares it with the entered one
3. Outputs Accept or Reject (via display)

User enters result

User reads result
Certificate Management

- Once a mobile device has been imprinted and provided with a public key certificate, there is a need for ongoing key management

- Three issues
  - Certificate and key pair update
    - If device need new key pair or new certificate for existing key pair
  - Key status management
    - Disseminating revocation information
    - CRL, OCSP, Ad hoc status dissemination
  - Trust management
    - Managing relationship between CA and PAN component, including root public key update and changing CA, in the event of lost and stolen personal CA
Currently interesting two questions and their informal solutions
Question. 1

Differently from global CA, we always consider that personal CA is relatively easy to be unavailable due to network- or power-down, lost, stolen, etc.

- Are there some preventative s against the compromise of the personal CA?

Intuitive Solution

To distribute the role of CA

Threshold cryptosystem
Question. 1

- Considerations
  - The short lifetime of PAN
    - Whether to make Personal CA fault-tolerant via threshold cryptosystem is meaningful or not, considering the short lifetime of PAN
  - The necessity of trust dealer
    - A human can act as a trust dealer. Fully distributed threshold cryptosystems are not necessary
Question. 1

\((t, n)\) – threshold cryptosystem

- **Approaches**
  - **All PAN component participates in the role of CA**
    - Each PAN component must obtain a share for the private key of CA in imprinting
    - A dynamic threshold is required according to the leave/join of PAN components
    - To protect the private key of CA, proactive secret sharing must be considered
  - **A pre-defined group is specified for the role of CA**
    - A dynamic threshold is not required
    - Proactive secret sharing is not necessary considering the short lifetime of PAN
Question. 2

- How can a PAN component, which has a limited computation and communication power, be effectively integrated into the Personal PKI environment?

- Hash chain
- Delegation of signing capability
- Server supported signature
- Light checking of certificate status
- Certificate revocation system
- Certificate revocation tree
- J. Zhou et al.'s framework
Question. 2

- Delegation of signing capability
  - During imprinting, the root value of hash chain must be inserted in the certificate
  - Discovery method
    - A PAN component can discover a PAN component which owns the high computing power
  - Delegation policy
    - To protect malicious delegation (e.g., Denial of service attack) of signing
- Non-repudiation
  - To perform server-supported signature, both client and server must cache relevant information to prevent the other from repudiating
  - Caching occurs insufficiency of memory in the mobile device
Question. 2

- Light checking of certificate status
  - Which one will be a main body for distributing a hash value?
    - A PAN component
      - J. Zhou et al’s framework
      - In addition, it is necessary to restrict the window of vulnerability
    - Personal CA
      - Certificate Revocation System
      - Certificate Revocation Tree
      - Personal CA must be online (without temporary absence caused by network down or power down, etc.)
  
- Advantages
  - If personal CA is online, the status checking of a certificate is the same as OCSP
  - Since the type of response is not a digital signature but a hash value, it reduces computational resources both personal CA and PAN component
Question. 2

- Considerations
  - To Apply hash chain to Personal PKI, the modification of the certificate is necessary
  - That causes interoperability issues in the Inter-PAN communication

Thank you!!