Information Security / Fall 2015

Key Establishment and Key Managament

Prof.dr. Ferucio Laurenţiu Ţiplea

"Al. I. Cuza" University of Iaşi

Department of Computer Science

Iasi 740083, Romania

E-mail: fltiplea@mail.dntis.ro

URL: http://www.infoiasi.ro/~fltiplea

Contents

1. Introduction

In order to use cryptographic primitives (symmetric and asymmetric cryptosystems, keyed hash functions, digital signatures) and implement security services (such as e-payment, e-auction etc.), we need techniques for

- controlling the distribution, use, and update of cryptographic keys;
- providing shared secrets between two or more parties (typically for the use of symmetric keys).

The techniques for solving these problems can be classified into:

- key establishment techniques;
- key management techniques.

2. Key establishment techniques

A key establishment technique is a protocol whereby a shared secret becomes available to two or more parties (for subsequent cryptographic use).

Key establishment techniques can be classified into:

- key transport techniques – one party creates or obtains a secret value (from a key distribution center, for example) and securely transfers it to the other(s);
- key agreement techniques – each party derives a shared secret from some common data (keying material).

Each technique can be based on symmetric or asymmetric cryptography.

2a. Key transport techniques

Key transport techniques based on symmetric cryptography may make use of a key distribution center (KDC) and/or timestamps.

Some of the most important key transport techniques based on symmetric cryptography:

Protocol	KDC	timestamps
point-to-point key update	no	optional
Shamir's no-key protocol	no	no
Kerberos	yes	yes
Needham-Schroeder shared-key	yes	no
Otway-Rees	yes	no

2a. Key transport techniques

Shamir's no-key protocol: it is based on a commutative cryptosystem, K_A is A's secret key, and K_B is B's secret key:

$$\begin{array}{lll} 1. & A \to B: & \{K\}_{K_A} \\ 2. & B \to A: & \{\{K\}_{K_A}\}_{K_B} \\ 3. & A \to B: & \{K\}_{K_B} \end{array}$$

Goal: A chooses a key K and transports it to B.

Correctness of step 3: $\{\{K\}_{K_A}\}_{K_B} = \{\{K\}_{K_B}\}_{K_A}$ by commutativity.

The protocol is called no-key because it does not require shared or public keys.

2a. Key transport techniques

Choosing a commutative cryptosystem:

- let p be a large prime;
- $\mathcal{P} = \mathbf{Z}_p = \mathcal{C}$;
- $\mathcal{K} = \mathbf{Z}^*_{p-1}$. For any $K_X \in \mathcal{K}$, there exists $K_X^{-1}\ mod\ (p-1)$;
- $e_{K_X}(z) = z^{K_X}\ mod\ p$ and $d_{K_X}(z) = z^{K_X^{-1}}\ mod\ p$, for any $z \in \mathbf{Z}_p$;
- p is public.

With such a cryptosystem, A has to choose K from $\mathbf{Z}_p$ and transport it to B.

Caution is needed if commutative cryptosystems based on XOR are considered.

2a. Key transport techniques

Attack (man-in-the-middle):

- C intercepts the first message from A;
- C encrypts it by its key K_C

$$\{\{K\}_{K_A}\}_{K_C}$$

  and sends it back to A;
- C intercepts $\{K\}_{K_C}$ from A and recovers K.

How can be prevented this attack?

2a. Key transport techniques

Needham-Schroeder shared-key protocol: it is based on a trusted server T (which is also a KDC) and a symmetric cryptosystem. K_{AT} is the key shared by A and T, K_{BT} is the key shared by B and T, and N_X is a nonce generated by X:

$$
\begin{array}{lll}
1. & A \to T: & A, B, N_A \\
2. & T \to A: & \{N_A, B, K, \{K, A\}_{K_{BT}}\}_{K_{AT}} \\
3. & A \to B: & \{K, A\}_{K_{BT}} \\
4. & B \to A: & \{N_B\}_K \\
5. & A \to B: & \{N_B - 1\}_K
\end{array}
$$

Goal: A requests from T a communication key with B, and then transports the key to B.

2a. Key transport techniques

Key transport techniques based on public-key cryptography may make use of digital signatures and/or authentication.

Some of the most important key transport techniques based on public-key cryptography:

Protocol	signature	authentication
X.509 (2-pass)	yes	mutual
X.509 (3-pass)	yes	mutual
Beller-Yacobi (4-pass)	yes	mutual
Beller-Yacobi (2-pass)	yes	unilateral
Needham-Schroeder public-key	no	mutual

2a. Key transport techniques

Needham-Schroeder public-key: In this protocol, K_X is the public key of X:

$$\begin{array}{lll} 1. & A \rightarrow B: & A, B, \{N_A, A\}_{K_B} \\ 2. & B \rightarrow A: & B, A, \{N_A, N_B\}_{K_A} \\ 3. & A \rightarrow B: & A, B, \{N_B\}_{K_B} \end{array}$$

Goal: A and B agree on the values of N_A and N_B, and no one else knows these values (A and B can then compute their session key by $f(N_A, N_B)$, where f is a publicly known "one-way" function).

2a. Key transport techniques

Attack (interleave, Lowe, 1996):

$$\begin{array}{lll}
1. & A \rightarrow C: & A, C, \{N_A, A\}_{K_C} \\
2. & C(A) \rightarrow B: & A, B, \{N_A, A\}_{K_B} \\
3. & B \rightarrow C(A): & B, A, \{N_A, N_B\}_{K_A} \\
4. & C \rightarrow A: & C, A, \{N_A, N_B\}_{K_A} \\
5. & A \rightarrow C: & A, C, \{N_B\}_{K_C} \\
6. & C(A) \rightarrow B: & A, B, \{N_B\}_{K_B}
\end{array}$$

where C is a recognized user. At the end of this:

- A thinks that he and C exclusively share N_A and N_B;
- B thinks that he and A exclusively share N_A and N_B.

The fix: Add identity of sender in step 2: $A, B, \{N_A, N_B, B\}_{K_A}$.

2b. Key agreement techniques

One of the most attractive key agreement techniques based on symmetric cryptography is Bloom's protocol:

- assume that a TA has to distribute communication keys for members of an n user group. This will be done by giving to any two users U and V some information so that these users can compute by themselves a communication key $K_{UV} = K_{VU}$;
- TA chooses a large prime p so that $p > n$;
- TA chooses three numbers $a, b, c \in \mathbf{Z}_p$ (not necessarily pairwise distinct) and computes the symmetric polynomial

$$f(x, y) = a + b(x + y) + cxy;$$

- for each user U, a random $r_U \in \mathbf{Z}_p$ is made public. It is assumed that $r_U \neq r_V$, for any two distinct users U and V;

2b. Key agreement techniques

- for each user U, TA computes the polynomial

$$g_U(x) = f(x, r_U)\ mod\ p = a_U + b_U x\ mod\ p$$

  and gives g_U to U using a secure channel (g_U is U's secret);

- U and V can communicate using the key

$$K_{UV} = g_U(r_V) = f(r_U, r_V) = f(r_V, r_U) = g_V(r_U) = K_{VU}.$$

2b. Key agreement techniques

Theorem 1 Let U, V, and W be three distinct users in Bloom's scheme. Then, for any $l \in \mathbf{Z}_p$, the system

$$\begin{cases} a + b(r_U + r_V) + c r_U r_V = l \\ a + b r_W = a_W \\ b + c r_W = b_W \end{cases}$$

has unique solution.

Proof The determinant of the system is non-zero. □

Theorem 1 shows that no single user W can compute uniquely K_{UV} by knowing only his parameters r_W, a_W, and b_W. Moreover, K_{UV} can be equally chosen as being any value in $\mathbf{Z}_p$.

2b. Key agreement techniques

It is easy to see that, if any two distinct users W and W' put together their information (r_W, $r_{W'}$, a_W, $a_{W'}$, b_W, and $b_{W'}$), then they are able to compute K_{UV}, for any U and V.

Can you extend Bloom's scheme to make it resistant to size k coalition attacks?

2b. Key agreement techniques

Key agreement techniques based on public-key cryptography may make use of key authentication and/or entity authentication.

Some of the most important key agreement techniques based on public-key cryptography:

Protocol	key authentication	entity authentication
Diffie-Hellman	no	no
ElGamal key agreement	unilateral	no
STS	mutual-explicit	mutual

2b. Key agreement techniques

Diffie-Hellman protocol: In this protocol, p is a (public) large prime, α is a (public) primitive root modulo p, $1 \leq x \leq p-2$ is a random secret chosen by A, and $1 \leq y \leq p-2$ is a random secret chosen by B:

$$\begin{array}{lll} 1. & A \rightarrow B: & \alpha^x \ mod\ p \\ 2. & B \rightarrow A: & \alpha^y \ mod\ p \end{array}$$

Goal: A computes the shared key $K = (\alpha^y)^x \ mod\ p$ and B computes the shared key $K = (\alpha^x)^y \ mod\ p$.

2b. Key agreement techniques

Attack (man-in-the-middle):

$$\begin{array}{lll} 1. & A \rightarrow C: & \alpha^{x}\ mod\ p \\ 2. & C(A) \rightarrow B: & \alpha^{x'}\ mod\ p \\ 3. & B \rightarrow C(A): & \alpha^{y}\ mod\ p \\ 4. & C \rightarrow A: & \alpha^{y'}\ mod\ p \end{array}$$

where C is a recognized user. At the end of this:

- A computes the session key $K_{AB} = \alpha^{xy'}\ mod\ p$;
- B computes the session key $K_{BA} = \alpha^{x'y}\ mod\ p$.

A and B believe they communicate securely, while C can read all traffic.

What is the fix?

3. Secret sharing schemes

A secret sharing scheme starts with a secret and derives from it several partial secrets, also called shadows, which are distributed amongst a group of users. Moreover, specific subgroups of users are able to recover the main secret if the members of such a subgroup put together their partial secrets.

A secret sharing scheme is called a (k, n) threshold scheme ($k \leq n$) if any k users who pool their shares may easily recover the secret.

Examples of threshold schemes:

- Mignotte's scheme;
- Shamir's scheme;

3. Secret sharing schemes

Shamir's secret sharing scheme

1. **input:** n users and a threshold k, $k \leq n$;
2. **setup:**
   - TA chooses a secret $S \neq 0$, a prime number $p > max\{S, n\}$, and $k-1$ distinct parameters $a_1, \ldots, a_k \in \mathbf{Z}_p^*$;
   - TA computes the polynomial $f(x) = \sum_{i=0}^{k-1} a_i x^i$ of degree $k-1$ in $\mathbf{Z}_p$, where $a_0 = S$;
   - TA transfers the share $S_i = f(i)$ to the user i, $1 \leq i \leq n$;
3. **secret recovery:** any group of k distinct users who pool their shares can recompute the polynomial f by Lagrange interpolation and then can recompute the secret S by $S = f(0)$.

Lagrange interpolation formula is (f is a polynomial of degree $k-1$ and A is a set of k interpolation nodes)

$$f(x) = \sum_{(a,b)\in A} b \prod_{(a',b')\neq(a,b)} \frac{x-a'}{a-a'}$$

3. Secret sharing schemes

A natural generalization of the concept of a threshold is that of an **access structure**:

- given a set U of users, an **access structure** for U is any non-empty set $\mathcal{A}$ of non-empty subsets of U;
- if $A \in \mathcal{A}$, then A is called an **authorized subset**;
- an access structure $\mathcal{A}$ is called **monotone** if $B \in \mathcal{A}$ whenever $A \in \mathcal{A}$ and $A \subseteq B$.

The access structure of a (k, n) threshold scheme consists of all subsets of $k' \geq k$ users.

3. Secret sharing schemes

A secret sharing scheme with an access structure $\mathcal{A}$ is called perfect if $H(S|A) = 0$ for any $A \in \mathcal{A}$ and $H(S|B) = H(S)$, for any $B \not\in \mathcal{A}$, where H denotes the entropy (that is, each unauthorized subset gets absolutely no information about the master secret).

The information rate for a particular user of a secret sharing scheme is

$$\frac{\text{size of the master secret}}{\text{size of the user's share}}$$

The information rate of a secret sharing scheme is the minimum of its user information rates.

Theorem 2 *The information rate of any perfect secret sharing scheme is less than or equal to 1.*

Secret sharing scheme of information rate 1 are called ideal.

3. Secret sharing schemes

Theorem 3 *Shamir's secret sharing scheme is perfect and ideal.*

Proof in class. □

Shamir's secret sharing scheme embraces many other nice features such as:

- easily extendable for new users;
- no unproven assumptions – its security is not based on unproven assumptions.

Does Mignotte's secret sharing scheme satisfy similar properties?

4. Key management techniques

By keying material we understand common data to a group of entities, used to derive cryptographic keys.

Key management techniques are used for:

- initialization of system users within a domain;
- generation, distribution, and installation of keying material;
- controlling the use of keying material;
- update, revocation, and destruction of keying material;
- storage, backup/recovery, and archival of keying material.