Protokollsicherheit

Protocol Goals and Protocol Design Principles

Motivation

Motivation

Protocol designers lack a standard definition for the goals of a protocol. In fact, the same name is used for different purposes. For example: “**authentication**”.

Motivation

Protocol designers lack a standard definition for the goals of a protocol. In fact, the same name is used for different purposes. For example: “**authentication**”.

Simple Example

1. $A \rightarrow B : N_A$
2. $B \rightarrow A : \mathrm{MAC}_{K_{AB}}(B, A, N_A), N_B$
3. $A \rightarrow B : \mathrm{MAC}_{K_{AB}}(A, B, N_B)$

The intention is to check “**whether A can communicate with B using the previously exchanged key K_{AB}.**”

Motivation

The intention is to check "**whether A can communicate with B using the previously exchanged key K_{AB}.**"

1. $C(A) \rightarrow B : N_C$
2. $B \rightarrow C(A) : \text{MAC}_{K_{AB}}(B, A, N_C), N_B$
3. $C(B) \rightarrow A : N_B$
4. $A \rightarrow B : \text{MAC}_{K_{AB}}(A, B, N_B), N_A$
5. $C(A) \rightarrow \text{MAC}_{K_{AB}}(A, B, N_B)$

Motivation

The intention is to check **"whether A can communicate with B using the previously exchanged key K_{AB}."**

1. $C(A) \rightarrow B : N_C$
2. $B \rightarrow C(A) : \text{MAC}_{K_{AB}}(B, A, N_C), N_B$
3. $C(B) \rightarrow A : N_B$
4. $A \rightarrow B : \text{MAC}_{K_{AB}}(A, B, N_B), N_A$
5. $C(A) \rightarrow B : \text{MAC}_{K_{AB}}(A, B, N_B)$

This seems to be an attack. **But did the protocol fail?** From the sequence above, one could establish that A is willing to communicate with B using K_{AB}.

Motivation

A Recent Example [Basin et al. POST'12]

“The **ISO/IEC 9798** standard **neither** specifies a threat model **nor** defines the security properties that the protocols should satisfy. Instead, the introduction of **ISO/IEC 9798** simply states that the protocols should satisfy mutual or unilateral authentication.”

Motivation

A Recent Example [Basin et al. POST'12]

"The **ISO/IEC 9798** standard **neither** specifies a threat model **nor** defines the security properties that the protocols should satisfy. Instead, the introduction of **ISO/IEC 9798** simply states that the protocols should satisfy mutual or unilateral authentication."

Unfortunately, there are no general precise definitions for the goals of protocols.

Definitions

Definitions

One can distinguish some types goals. The first two are basic goals:

- **User-oriented goals** – concerning entity authentication;
- **Key-oriented goals** – concerning key establishment;
- **Enhanced goals** – some additional goals associated to key establishment;

Definitions

One can distinguish some types goals. The first two are basic goals:

- **User-oriented goals** – concerning entity authentication;
- **Key-oriented goals** – concerning key establishment;
- **Enhanced goals** – some additional goals associated to key establishment;

User-Oriented Goals

Definition: Entity authentication is the process whereby one party is assured (**through the acquisition of corroborative evidence**) of the identity of a second party involved in a protocol, and that party has actually participated.

Definitions

User-Oriented Goals

1. $A \rightarrow B : N_A$
2. $B \rightarrow A : \text{Sign}_B(N_A)$

Definitions

User-Oriented Goals

1. $A \rightarrow B : N_A$
2. $B \rightarrow A : \text{Sign}_B(N_A)$

However, B has not indicated that she is aware of A.

Definition: A principal A is said to have *knowledge* of A as his peer entity if A is aware of B as his claimed peer entity in the protocol.

1. $A \rightarrow B : N_A$
2. $B \rightarrow A : \text{Sign}_B(A, N_A)$

Definition: *Strong entity authentication* of A to B is provided if B has *fresh* assurance that A has knowledge of B as his peer.

Definitions

Key-Oriented Goals

Definitions

Key-Oriented Goals

As we have seen, protocols have three entities, which we can use for establishing a key exchange:

- **keys** – which may be long-term or session keys.
- **identifiers** for principals;
- **nonces** which may be random values, timestamps or counters.

Definitions

Key-Oriented Goals

As we have seen, protocols have three entities, which we can use for establishing a key exchange:

- **keys** – which may be long-term or session keys.
- **identifiers** for principals;
- **nonces** which may be random values, timestamps or counters.

Session Keys

Definition: The shared session key is a *good* key for A to use with B only if A has assurance that:

- the key is **fresh** also called **key freshness**;
- the key is known only to A and B which are **mutually trusted parties**, also called **key authentication**.

Definitions

Enhanced Goals

Definitions

Enhanced Goals

Combination of user and key goals. Some protocols' goals are not only to exchange a key but also to establish the **readiness** of a partner.

Definitions

Enhanced Goals

Combination of user and key goals. Some protocols' goals are not only to exchange a key but also to establish the **readiness** of a partner.

Definition: Key confirmation of A to B is provided if B has assurance that a key K is a good key to communicate with A and that principal A has possession of key K.

Definitions

Enhanced Goals

Combination of user and key goals. Some protocols' goals are not only to exchange a key but also to establish the **readiness** of a partner.

Definition: Key confirmation of A to B is provided if B has assurance that a key K is a good key to communicate with A and that principal A has possession of key K.

Not really standard definition. In ISO/IEC the following definition appears:

"Key confirmation: the assurance for one entity that another identified entity is in possession of the correct key."

Not clear what correct key means.

Definitions

Enhanced Goals

Combination of user and key goals. Some protocols' goals are not only to exchange a key but also to establish the **readiness** of a partner.

Definition: Key confirmation of A to B is provided if B has assurance that a key K is a good key to communicate with A and that principal A has possession of key K.

Not really standard definition. In ISO/IEC the following definition appears:

"Key confirmation: the assurance for one entity that another identified entity is in possession of the correct key."

Not clear what correct key means.

Definition: Explicit key authentication is the property obtained when both **key authentication** and **key confirmation** hold.

Definitions

Enhanced Goals

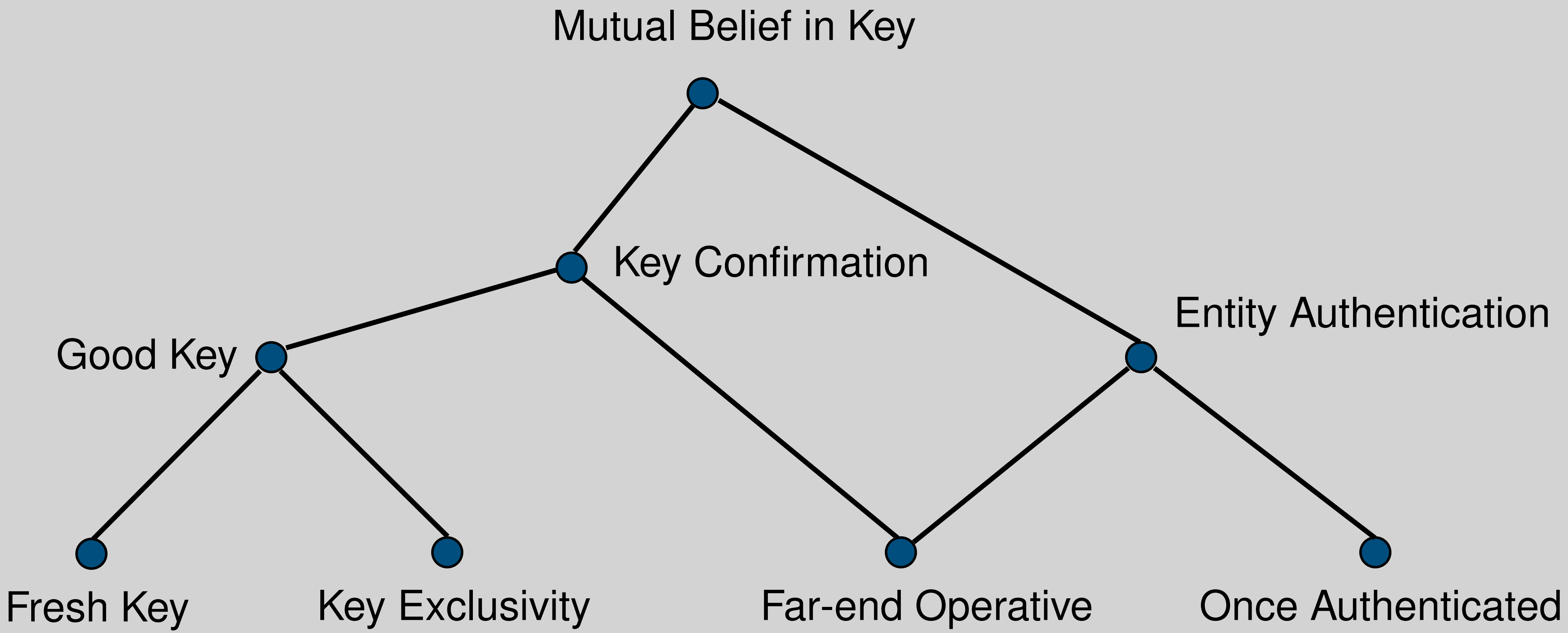
Definition: Mutual belief in the key K is provided for B only if K is a good key for use with A and A wishes to communicate with B using key K, which A **believes is good for that purpose**.

Definitions

Enhanced Goals

Definition: Mutual belief in the key K is provided for B only if K is a good key for use with A and A wishes to communicate with B using key K, which A **believes is good for that purpose**.

Goal Hierarchy



Abadi-Needham's 11 Principles

Abadi-Needham's 11 Principles

Principle 1: Every message should say what it means: the interpretation of a message should **not** depend on the context.

Abadi-Needham's 11 Principles

Principle 1: Every message should say what it means: the interpretation of a message should **not** depend on the context.

Principle 2: The conditions for a message to be acted upon should be clearly set out so that someone reviewing a design may see whether they are acceptable or not.

Handshake

i. $A \rightarrow B : \{N_A\}_K$

i+1. $A \rightarrow B : \{N_A + 1\}_K$

N_A is a challenge nonce and K is the exchanged session key.

Abadi-Needham's 11 Principles

Principle 3: If the identity of a principal is essential to the meaning of a message, it is prudent to mention the principal's name **explicitly** in the message.

Abadi-Needham's 11 Principles

Principle 3: If the identity of a principal is essential to the meaning of a message, it is prudent to mention the principal's name **explicitly** in the message.

Example

1. $A \rightarrow S : A, B$
2. $S \rightarrow A : C_A, C_B$
3. $A \rightarrow B : C_A, C_B, \{\text{sign}((K_{ab}, T_a), K_a)\}_{K_b}$

Abadi-Needham's 11 Principles

Principle 3: If the identity of a principal is essential to the meaning of a message, it is prudent to mention the principal's name **explicitly** in the message.

Example

1. $A \rightarrow S : A, B$
2. $S \rightarrow A : C_A, C_B$
3. $A \rightarrow B : C_A, C_B, \{\text{sign}((K_{ab}, T_a), K_a)\}_{K_b}$

Attack

3'. $B \rightarrow C : C_A, C_C, \{\text{sign}((K_{ab}, T_a), K_a)\}_{K_c}$

Abadi-Needham's 11 Principles

Principle 3: If the identity of a principal is essential to the meaning of a message, it is prudent to mention the principal's name **explicitly** in the message.

Example

1. $A \rightarrow S : A, B$
2. $S \rightarrow A : C_A, C_B$
3. $A \rightarrow B : C_A, C_B, \{\text{sign}((K_{ab}, T_a), K_a)\}_{K_b}$

Attack

3'. $B \rightarrow C : C_A, C_C, \{\text{sign}((K_{ab}, T_a), K_a)\}_{K_c}$

Solution

3. $B \rightarrow C : C_A, C_B, \{\text{sign}((A, B, K_{ab}, T_a), K_a)\}_{K_b}$

Abadi-Needham's 11 Principles

Principle 4: Be clear about why encryption is being done. Encryption is not wholly cheap, and not asking precisely why it is being done can lead to redundancy. **Encryption is not synonymous with security**.

Abadi-Needham's 11 Principles

Principle 4: Be clear about why encryption is being done. Encryption is not wholly cheap, and not asking precisely why it is being done can lead to redundancy. **Encryption is not synonymous with security**.

Possible Uses of Encryption

- **Preservation of confidentiality:** $\{X\}_K$ only those that have K may recover X.
- **Guarantee authenticity:** The partner is indeed some particular principal.
- **Guarantee confidentiality and authenticity:** binds two parts of a message – $\{X, Y\}_K$ is not the same as $\{X\}_K$ and $\{Y\}_K$.
- **Produce random numbers:** This is not really explicit in our symbolic model. In practice, however, encryption techniques can also be used to produce random numbers.

Abadi-Needham's 11 Principles

Kerberos

1. $A \rightarrow S : A, B$
2. $S \rightarrow A : \{T_s, L, K_{ab}, B, \{T_s, L, K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$
3. $A \rightarrow B : \{T_s, L, K_{ab}, A\}_{K_{bs}}, \{A, T_a\}_{K_{ab}}$
4. $B \rightarrow A : \{T_a + 1\}_{K_{ab}}$

Abadi-Needham's 11 Principles

Kerberos

1. $A \rightarrow S : A, B$
2. $S \rightarrow A : \{T_s, L, K_{ab}, B, \{T_s, L, K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$
3. $A \rightarrow B : \{T_s, L, K_{ab}, A\}_{K_{bs}}, \{A, T_a\}_{K_{ab}}$
4. $B \rightarrow A : \{T_a + 1\}_{K_{ab}}$

Message 1: Although encryption of the message is not necessary, it may allow an intruder to flood the server with request keys.

Abadi-Needham's 11 Principles

Kerberos

1. $A \rightarrow S : A, B$
2. $S \rightarrow A : \{T_s, L, K_{ab}, B, \{T_s, L, K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$
3. $A \rightarrow B : \{T_s, L, K_{ab}, A\}_{K_{bs}}, \{A, T_a\}_{K_{ab}}$
4. $B \rightarrow A : \{T_a + 1\}_{K_{ab}}$

Message 1: Although encryption of the message is not necessary, it may allow an intruder to flood the server with request keys.

Message 2: Double encryption is not really needed. (In later Kerberos versions, the double encryption is not there.)

Abadi-Needham's 11 Principles

Kerberos

1. $A \rightarrow S : A, B$
2. $S \rightarrow A : \{T_s, L, K_{ab}, B, \{T_s, L, K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$
3. $A \rightarrow B : \{T_s, L, K_{ab}, A\}_{K_{bs}}, \{A, T_a\}_{K_{ab}}$
4. $B \rightarrow A : \{T_a + 1\}_{K_{ab}}$

Message 1: Although encryption of the message is not necessary, it may allow an intruder to flood the server with request keys.

Message 2: Double encryption is not really needed. (In later Kerberos versions, the double encryption is not there.)

Message 3: The purpose of the encryption with K_{ab} is to prove knowledge of K_{ab} near T_a. The same use happens in message 4. However, if T_a is **not** that different from T_s it could be eliminated. In this case, B uses T_s in message 4.

Abadi-Needham's 11 Principles

Principle 5: When a principal signs material that has already been encrypted, it should **not be inferred** that the principal knows the content of the message. On the other hand, it is **proper to infer** that the principal that signs a message and then encrypts it for privacy **knows the content** of the message.

Abadi-Needham's 11 Principles

Principle 5: When a principal signs material that has already been encrypted, it should **not be inferred** that the principal knows the content of the message. On the other hand, it is **proper to infer** that the principal that signs a message and then encrypts it for privacy **knows the content** of the message.

1. $A \rightarrow B : A, \text{sign}((T_a, N_a, B, X_a, \underbrace{\{Y_a\}}_{}{}_{K_b}), K_a)$

A might not know this message!

Abadi-Needham's 11 Principles

Principle 6: Be clear what properties you are assuming about **nonces**. What may do for ensuring temporal succession may not do for ensuring association—and perhaps association is best established by other means.

Abadi-Needham's 11 Principles

Principle 6: Be clear what properties you are assuming about **nonces**. What may do for ensuring temporal succession may not do for ensuring association—and perhaps association is best established by other means.

Otway-Rees

1. $A \rightarrow B : M, A, B, \{N_A, M, A, B\}_{K_{AS}}$
2. $B \rightarrow S : M, A, B, \{N_A, M, A, B\}_{K_{AS}}, \{N_B, M, A, B\}_{K_{BS}}$
3. $S \rightarrow B : M, \{N_A, K_{AB}\}_{K_{AS}}, \{N_B, K_{AB}\}_{K_{BS}}$
4. $B \rightarrow A : M, \{N_A, K_{AB}\}_{K_{AS}}$

Abadi-Needham's 11 Principles

Principle 6: Be clear what properties you are assuming about **nonces**. What may do for ensuring temporal succession may not do for ensuring association—and perhaps association is best established by other means.

Otway-Rees

1. $A \rightarrow B : M, A, B, \{N_A, M, A, B\}_{K_{AS}}$
2. $B \rightarrow S : M, A, B, \{N_A, M, A, B\}_{K_{AS}}, \{N_B, M, A, B\}_{K_{BS}}$
3. $S \rightarrow B : M, \{N_A, K_{AB}\}_{K_{AS}}, \{N_B, K_{AB}\}_{K_{BS}}$
4. $B \rightarrow A : M, \{N_A, K_{AB}\}_{K_{AS}}$

Encryption is for binding the messages.

Abadi-Needham's 11 Principles

Principle 7: The use of a predictable quantity such as the value of a counter **can serve in guaranteeing newness**, through a challenge-response exchange. But if a predictable quantity is to be effective, it should be protected so that an intruder **cannot** simulate a challenge and later replay a response.

Abadi-Needham's 11 Principles

Principle 7: The use of a predictable quantity such as the value of a counter **can serve in guaranteeing newness**, through a challenge-response exchange. But if a predictable quantity is to be effective, it should be protected so that an intruder **cannot** simulate a challenge and later replay a response.

1. $A \rightarrow S : A, N_a$
2. $S \rightarrow A : \{T_s, N_a\}_{K_{as}}$

When completed, A sets his time to T_s.

Abadi-Needham's 11 Principles

Principle 7: The use of a predictable quantity such as the value of a counter **can serve in guaranteeing newness**, through a challenge-response exchange. But if a predictable quantity is to be effective, it should be protected so that an intruder **cannot** simulate a challenge and later replay a response.

1. $A \rightarrow S : A, N_a$
2. $S \rightarrow A : \{T_s, N_a\}_{K_{as}}$

When completed, A sets his time to T_s.

If N_a is predictible, then the intruder could request the current time using a **future nonce**. Then the intruder could use the returned message in the future to set A's time to the past.

Abadi-Needham's 11 Principles

Principle 8: If timestamps are used as freshness guarantees by reference to absolute time, then the **difference between local clocks** at various machines must be much less than the allowable age of a message deemed to be valid. Furthermore, the time maintenance mechanism everywhere becomes part of the trusted computing base.

Abadi-Needham's 11 Principles

Principle 8: If timestamps are used as freshness guarantees by reference to absolute time, then the **difference between local clocks** at various machines must be much less than the allowable age of a message deemed to be valid. Furthermore, the time maintenance mechanism everywhere becomes part of the trusted computing base.

Principle 9: A key may have been used recently, for example to encrypt a nonce, **yet be quite old, and possibly compromised**. Recent use does not make the key look any better than it would otherwise.

Example: Denning-Sacco attack on **Needham-Schroeder**

Abadi-Needham’s 11 Principles

Principle 10: If an encoding is used to present the meaning of a message, then it should be possible to tell which encoding is being used.

Abadi-Needham's 11 Principles

Principle 10: If an encoding is used to present the meaning of a message, then it should be possible to tell which encoding is being used.

Handshake

i. $A \rightarrow B : \{N_A\}_K$

i+1. $A \rightarrow B : \{N_A + 1\}_K$

The purpose of incrementing the nonce is simply for **distinguishing the two messages.**

Abadi-Needham's 11 Principles

Principle 10: If an encoding is used to present the meaning of a message, then it should be possible to tell which encoding is being used.

Handshake

i. $A \rightarrow B : \{N_A\}_K$

i+1. $A \rightarrow B : \{N_A + 1\}_K$

The purpose of incrementing the nonce is simply for **distinguishing the two messages.**

i. $A \rightarrow B : \{\text{Message i} : N_A\}_K$

i+1. $A \rightarrow B : \{\text{Message i + 1} : N_A\}_K$

Abadi-Needham's 11 Principles

Principle 11: The protocol designer should **know which trust relations his protocol depends on, and why the dependence is necessary**. The reasons for particular trust relations being acceptable should be explicit though they will be founded on judgment and policy rather than on logic.

Abadi-Needham’s 11 Principles

Principle 11: The protocol designer should **know which trust relations his protocol depends on, and why the dependence is necessary**. The reasons for particular trust relations being acceptable should be explicit though they will be founded on judgment and policy rather than on logic.

Example Kerberos: Server providing false timestamps leads to an attack.

Example Certification Authorities (CAs): CAs are trusted to certify a key only after proper steps have been taken to identify the principal that owns it.