Secure Protocols for Secrecy

Hanane Houmani and Mohamed Mejri

LSFM Research Group

Computer Science Department

LAVAL University

Quebec, Canada

Outline

- Motivations
- Related works
- Overview
- Protocol Modelling
- Secrecy property
- Correctness conditions
- Correctness theorem
- Example
- Conclusion and future works

Motivations

- Problems:
  - Internet, www, electronic trade, etc. ⇨ Urgent need of security to develop confidence between the electronic market actors
  - Analysis of security protocols ⇨ subtle and complex
  - Need of guarantee that the protocols, used to make our transactions secure, don't have any flaw ⇨ Need of methods to verify the correctness of cryptographic protocols

Motivations

- Problems:
  - Internet, www, electronic trade, etc. ➪ Urgent need of security to develop confidence between the electronic market actors
  - Analysis of security protocols ➪ subtle and complex
  - Need of guarantee that the protocols, used to make our transactions secure, don't have any flaw ➪ Need of methods to verify the correctness of cryptographic protocols
- Objectives:
  - Establish some sufficient conditions under which the correctness of a given protocol is guaranteed
  - Conditions must be verified easily on a protocol

Related works

- Logical methods: based on multi-modal logics (temporal, epistemic and doxatic logics).
  - BAN, CKT5, GNY, etc.
- General purpose formal methods: based on the use of traditional formal specification and verification methods.
  - Z, VDM, B, RSL, Coq, Isabelle, HOL, etc.
- Process algebra methods: based on the use of process algebra for the protocol description and for verification.
  - CSP, CCS, LOTOS, SPI, etc.
- Search oriented methods: based on the intruder abilities modeling and the search of insecure states.
  - Interrogator, NRL, etc.
- Correctness oriented methods : based on proving correctness of protocols
  - Methods based on model-checking, Typing system of Abadi, Inductive method of Paulson, method proving of Guttman, etc.

Overview

- Result:
  - Any protocol that satisfies correctness conditions, is correct with respect to the secrecy property

Overview

- Result:
  - Any protocol that satisfies correctness conditions, is correct with respect to the secrecy property
- Correctness verification:
  - The verification of the correctness condition on a given protocol consists of a verification on the whole of messages sent in roles-based specification of this protocol.
  - The verification of the correctness condition on protocols can be automatized.
  - This result involves the protocols that use symmetric and atomic keys

Outline

- Motivations
- Related works
- Overview
- Protocol Modelling
  - Basics
  - Protocol & Generalized roles
  - Reduction
  - Example
- Secrecy property
- Correctness conditions
- Correctness theorem
- Example
- Conclusion and future works

Basics

- Message :
  - $A, B,\ C,\ S\ and\ I.$: principal identities
  - N_a : nonce chosen by A
  - k_{ab} : shared key between A and B
  - k_a (resp k_a^{-1}): A's public key (resp A's private key.)
  - $\{m\}_k$: message encrypted by public key of A
  - $m.m$: composed message
- Communication step:

$$i\ \ A \ \rightarrow\ B : m$$

Protocol Modelling

- A Protocol is defined by a pair $\langle P,\ K\rangle$, where:
  - P has to respect the following BNF grammar:

$$P \quad ::= \langle i,\ A \rightarrow B : m\rangle \mid P.P$$

  - K is a set of triples like (X, K_X, F_X)

- Role-based specification : is a set of generalized roles extracted from the analyzed protocol. Generalized roles are extracted from the protocol according to the following steps
  - Extracting the roles: A role is a protocol abstraction where the emphasis is put on a particular principal.
  - Extracting the generalized roles: A generalized role is an abstraction of a role where some messages are replaced by variables

Protocol Modelling

- **Reduction ($\downarrow$):** Let M be a set of messages. The reduction of M, denoted by $M_\downarrow$, is defined as the normal form of M obtained from the following rewriting rules:

$$\begin{array}{lcl} (M \cup \{m_1.m_2\})_\downarrow & \rightarrow_c & (M \cup \{m_1, m_2\})_\downarrow \\ (M \cup \{\{m\}_k,\ k\})_\downarrow & \rightarrow_e & (M \cup \{m,\ k\})_\downarrow \end{array}$$

- **Extended Reduction ($\downarrow_x$):** Let M be a set of messages. The extended reduction of M, denoted by $M_{\downarrow_x}$, is defined as the normal form of M obtained using the following rewriting rules:

$$\begin{array}{lcl} M \cup \{m_1.m_2\} & \rightarrow_{c_x} & M \cup \{m_1, m_2\} \\ M \cup \{\{m\}_\alpha, \beta\} & \rightarrow_{e_x} & M \cup \{\{m\}_\alpha, \beta\} \cup \{m\sigma, \beta\sigma \mid \sigma = mgu(\alpha, \beta)\} \end{array}$$

Protocol Modelling

- Example: Let $p = \langle P, K \rangle$ be the following protocol :

$$\left\{\begin{array}{ll} P = & \langle 1, A \rightarrow S : \{A.B.N_a\}_{k_{as}} \rangle. \\ & \langle 2, S \rightarrow A : \{\{A\}_{N_a}.B.k_{ab}\}_{k_{as}} \rangle. \\ & \langle 3, S \rightarrow B : \{A.B.k_{ab}\}_{k_{bs}} \rangle \\ & \\ K = & \{(A, K_A, F_A), (B, K_B, F_B), (S, K_S, F_S)\} \\ & K_A = \{A, B, S, k_{as}\} \\ & K_B = \{A, B, S, k_{bs}\} \\ & K_S = \{A, B, S, k_{ab}, k_{bs}, k_{as}\} \\ & F_A = \{N_a\} \\ & F_B = \emptyset \\ & F_S = \{k_{ab}\} \end{array}\right. \Rightarrow$$

$$\begin{array}{ll} \mathcal{A} = & \langle \alpha.1, A \rightarrow I(S) : \{A.B.N_a^\alpha\}_{k_{as}} \rangle. \\ & \langle \alpha.2, I(S) \rightarrow A : \{\{A\}_{N_a^\alpha}.B.k_{ab}^\alpha\}_{k_{as}} \rangle \\ & \\ \mathcal{B} = & \langle \alpha.3, I(S) \rightarrow B : \{A.B.k_{ab}^\alpha\}_{k_{bs}} \rangle \\ & \\ \mathcal{S} = & \langle \alpha.1, I(A) \rightarrow S : \{A.B.N_a^\alpha\}_{k_{as}} \rangle. \\ & \langle \alpha.2, S \rightarrow I(A) : \{\{A\}_{N_a^\alpha}.B.k_{ab}^\alpha\}_{k_{as}} \rangle. \\ & \langle \alpha.3, S \rightarrow I(B) : \{A.B.k_{ab}^\alpha\}_{k_{bs}} \rangle \end{array}$$

Protocol Modelling

- Example:

$$\mathcal{A} = \langle \alpha.1, A \rightarrow I(S) : \{A.B.N_a^\alpha\}_{k_{as}}\rangle. \langle \alpha.2, I(S) \rightarrow A : \{\{A\}_{N_a^\alpha}.B.k_{ab}^\alpha\}_{k_{as}}\rangle$$

$$\mathcal{A}_G = \langle \alpha.1, A \rightarrow I(S) : \{A.B.N_a^\alpha\}_{k_{as}}\rangle. \langle \alpha.2, I(S) \rightarrow A : \{\{A\}_{N_a^\alpha}.B.X\}_{k_{as}}\rangle$$

$$\mathcal{B} = \langle \alpha.3, I(S) \rightarrow B : \{A.B.k_{ab}^\alpha\}_{k_{bs}}\rangle \quad \Rightarrow \quad \mathcal{B}_G = \langle \alpha.3, I(S) \rightarrow B : \{A.B.Y\}_{k_{bs}}\rangle$$

$$\mathcal{S} = \langle \alpha.1, I(A) \rightarrow S : \{A.B.N_a^\alpha\}_{k_{as}}\rangle. \langle \alpha.2, S \rightarrow I(A) : \{\{A\}_{N_a^\alpha}.B.k_{ab}^\alpha\}_{k_{as}}\rangle. \langle \alpha.3, S \rightarrow I(B) : \{A.B.k_{ab}^\alpha\}_{k_{bs}}\rangle$$

$$\mathcal{S}_G = \langle \alpha.1, I(A) \rightarrow S : \{A.B.Z\}_{k_{as}}\rangle. \langle \alpha.2, S \rightarrow I(A) : \{\{A\}_Z.B.k_{ab}^\alpha\}_{k_{as}}\rangle. \langle \alpha.3, S \rightarrow I(B) : \{A.B.k_{ab}^\alpha\}_{k_{bs}}\rangle$$

- $\mathcal{D}(p)$ the set of all messages sent by the honest agents in all generalized roles of p and the initial knowledge of the intruder

$$\mathcal{D}(p) = K_I \cup \{\{A.B.N_a^\alpha\}_{k_{as}}, \{\{A\}_Z.B.k_{ab}^\alpha\}_{k_{as}}, \{A.B.k_{ab}^\alpha\}_{k_{bs}}\}$$

Outline

- Motivations
- Overview
- Protocol Modelling
- Secrecy property
  - Trace
  - Def/ Use
  - Secrecy property
  - Relationship between valid trace and generalized roles
- Correctness conditions
- Correctness theorem
- Example
- Conclusion and future works

Secrecy property

- Valid trace : Intuitively, a trace is an interleaving of many runs of the protocol in the presence of an active intruder. A trace is considered as valid when all the honest principals act according to the protocol specification and all the messages sent by the intruder are previously known by him

Secrecy property

- Valid trace : Intuitively, a trace is an interleaving of many runs of the protocol in the presence of an active intruder. A trace is considered as valid when all the honest principals act according to the protocol specification and all the messages sent by the intruder are previously known by him
- Def/Use :
  - Def(τ) : The set of messages sent by the honest agent in τ
  - Use(τ) : The set of messages received by the honest agent in τ

Secrecy property

- Valid trace : Intuitively, a trace is an interleaving of many runs of the protocol in the presence of an active intruder. A trace is considered as valid when all the honest principals act according to the protocol specification and all the messages sent by the intruder are previously known by him
- Def/Use :
  - Def(τ) : The set of messages sent by the honest agent in τ
  - Use(τ) : The set of messages received by the honest agent in τ
- Secret property: a protocol keeps a message m secret, if there is no valid trace that leaks this message to an intruder. Formally:

$$\forall \tau, \quad S \cap \mathsf{Def}(\tau)_{\downarrow} = \emptyset$$

Relationship between valid traces and generalized roles

- **Valid trace :** Intuitively, a trace is an interleaving of many runs of the protocol in the presence of an active intruder. A trace is considered as valid when all the honest principals act according to the protocol specification and all the messages sent by the intruder are previously known by him
- **Honest agent** acts according to the protocol specification if any given **run** in which he participates is an **instance** (variables are replaced by constant messages) of a **prefix** of his **generalized role**

→ Let p be a protocol and τ a p-valid trace. There exist n communication steps, $\{e_1, \ldots, e_n\} \subseteq_\eta \overline{\mathcal{R}_G(p)}$ and a substitution σ such that:

$$\overline{\tau} = \{e_1, \ldots, e_n\}\sigma$$

Outline

- Motivations
- Overview
- Protocol Modelling
- Secrecy property
- Correctness conditions
- Correctness theorem
- Example
- Conclusion and future works

Correctness conditions

- Zero-Unprotected Secret Message:
  - Intuitively: This condition states that any secret message exchanged during the protocol has to be encrypted using a secret key. It is obvious and necessary but not sufficient.
  - Formally: $S \cap \mathcal{D}(p)_{\downarrow_x} = \emptyset$

Correctness conditions

- Zero-Unprotected Secret Message:
  - Intuitively: This condition states that any secret message exchanged during the protocol has to be encrypted using a secret key. It is obvious and necessary but not sufficient.
  - Formally: $S \cap \mathcal{D}(p)_{\downarrow_x} = \emptyset$
- Zero-Unknown Sent Message:
  - Intuitively: This condition forbids an honest agent to send an unknown message either in clear or encrypted, but an unknown message can be used by an agent as a key to encrypt other messages
  - Formally: $\mathcal{X} \cap \mathcal{V}^{-}(\mathcal{D}(p)) = \emptyset$

Correctness conditions

- Zero-Unprotected Secret Message:
  - Intuitively: This condition states that any secret message exchanged during the protocol has to be encrypted using a secret key. It is obvious and necessary but not sufficient.
  - Formally: $S \cap \mathcal{D}(p)_{\downarrow_x} = \emptyset$
- Zero-Unknown Sent Message:
  - Intuitively: This condition forbids an honest agent to send an unknown message either in clear or encrypted, but an unknown message can be used by an agent as a key to encrypt other messages
  - Formally: $\mathcal{X} \cap \mathcal{V}^{-}(\mathcal{D}(p)) = \emptyset$
- Key Restriction:
  - Intuitively: This condition states that a key used to encrypt a message m cannot be a component of m
  - Formally: $F(\mathcal{D}(p)) = true$

Correctness conditions

- Zero-Unknown Sent Message :
  - Let σ a substitution such that $\mathcal{R}_{G2}(p) = \mathcal{R}_{G1}(p)\sigma$
  - $\mathcal{R}_{G1}(p)$ the set of generalized roles of p
  - Since valid trace is an interleaving of many runs and each run is an instance of a prefix of his generalized, we have:
    - $\mathcal{T}_2(p) \subseteq \mathcal{T}_1(p)$, where $\mathcal{T}_1(p)$ (respectively $\mathcal{T}_2(p)$) is the set of valid traces obtained from $\mathcal{R}_{G1}(p)$ (respectively from $\mathcal{R}_{G2}(p)$)
    - $\mathcal{F}_2(p) \subseteq \mathcal{F}_1(p)$, where $\mathcal{F}_1(p)$ (respectively $\mathcal{F}_2(p)$) is the set of valid traces of $\mathcal{T}_1(p)$ (respectively of $\mathcal{T}_2(p)$) that contains flaws
  - Conclusion:
    - Reduce the number of variables in the generalized roles of a protocol to considerably reduce the set of flawed traces
    - Not reduce this number to zero to still allow agents exchanging secrets

Outline

- Motivations
- Overview
- Protocol Modelling
- Secrecy property
- Correctness conditions
- Correctness theorem
- Example
- Conclusion and future works

Correctness theorem

- Theorem : Any protocol that respects the Key Restriction condition, Zero-Unknown Sent Message condition and Zero-Unprotected Secret Message condition, is correct with respect to the secrecy property

Correctness theorem

- **Theorem :** Any protocol that respects the Key Restriction condition, Zero-Unknown Sent Message condition and Zero-Unprotected Secret Message condition, is correct with respect to the secrecy property
- **Proof :**
  - Since $\forall \tau \in \mathcal{T}(p),\ \exists \sigma :\ \ Def(\tau)_{\downarrow} \subseteq \mathcal{D}(p)_{\downarrow x}\sigma$
  - if $s \in Def(\tau)_{\downarrow}$ so there exists a substitution σ such that $s \in \mathcal{D}(p)_{\downarrow x}\sigma$
  - $s \in \mathcal{D}(p)_{\downarrow x}\sigma \Rightarrow s \in \mathcal{D}(p)_{\downarrow x} \quad \vee \quad \exists x : x \in \mathcal{D}(p)_{\downarrow x}$
  - The assumptions, on the other hand, contribute as follows:
    - The assumption $\mathcal{H}_1(\{s\})$ ensures that $s \notin \mathcal{D}(p)_{\downarrow x}$.
    - The restriction $\mathcal{H}_2$ guarantees that the set $\mathcal{D}(p)_{\downarrow x}$ does not contain any variable ($x \in \mathcal{D}(p)_{\downarrow x}$).
    - Finally, the hypothesis $\mathcal{H}_3$ helps to easily prove the existence of the set $\mathcal{D}(p)_{\downarrow x}$.

Outline

- Motivations
- Overview
- Protocol Modelling
- Secrecy property
- Correctness conditions
- Correctness theorem
- Example
- Conclusion and future works

Example

- Let $p = \langle P, K\rangle$ be the following protocol :

$$\left\{\begin{array}{ll} P = & \langle 1, A \rightarrow S : \{A.B.N_a\}_{k_{as}}\rangle. \\ & \langle 2, S \rightarrow A : \{\{A\}_{N_a}.B.k_{ab}\}_{k_{as}}\rangle. \\ & \langle 3, S \rightarrow B : \{A.B.k_{ab}\}_{k_{bs}}\rangle \\ & \\ K = & \{(A, K_A, F_A), (B, K_B, F_B), (S, K_S, F_S)\} \\ & K_A = \{A, B, S, k_{as}\} \\ & K_B = \{A, B, S, k_{bs}\} \\ & K_S = \{A, B, S, k_{ab}, k_{bs}, k_{as}\} \\ & F_A = \{N_a\} \\ & F_B = \emptyset \\ & F_S = \{k_{ab}\} \end{array}\right. \Rightarrow$$

$$\begin{array}{ll} \mathcal{A}_G = & \langle \alpha.1, A \rightarrow I(S) : \{A.B.N_a^\alpha\}_{k_{as}}\rangle. \\ & \langle \alpha.2, I(S) \rightarrow A : \{\{A\}_{N_a^\alpha}.B.X\}_{k_{as}}\rangle \\ & \\ \mathcal{B}_G = & \langle \alpha.3, I(S) \rightarrow B : \{A.B.Y\}_{k_{bs}}\rangle \\ & \\ \mathcal{S}_G = & \langle \alpha.1, I(A) \rightarrow S : \{A.B.Z\}_{k_{as}}\rangle. \\ & \langle \alpha.2, S \rightarrow I(A) : \{\{A\}_Z.B.k_{ab}^\alpha\}_{k_{as}}\rangle. \\ & \langle \alpha.3, S \rightarrow I(B) : \{A.B.k_{ab}^\alpha\}_{k_{bs}}\rangle \end{array}$$

  - From the generalized roles we deduce that:

$$\mathcal{D}(p) = K_I \cup \{\{A.B.N_a^\alpha\}_{k_{as}}, \{\{A\}_Z.B.k_{ab}^\alpha\}_{k_{as}}, \{A.B.k_{ab}^\alpha\}_{k_{bs}}\}$$

Example

- Let, for instance, $S = \{k_{ab}^{\alpha}\}$ be the set of secret messages, and let $K_I = \{A, B, S, k_{is}, k_{ib}^{\alpha}, k_{ai}^{\alpha}, N_i^{\alpha}\}$ be the initial knowledge of the intruder
- **Verification of the first condition:** This protocol satisfies the condition of zero-unprotected secret message. Indeed, we have :

$$\mathcal{D}(p)_{\downarrow x} \cap S = \emptyset$$

- **Verification of the second condition:** This protocol satisfies the condition of zero-unknown sent message. Indeed, we have :

$$\mathcal{V}^{-}(\mathcal{D}(p)) = K_I \cup \{k_{ab}^{\alpha}\}$$

- **Verification of the third condition:** This protocol satisfies the condition of Key Restriction . Indeed, we have :

$$F(\mathcal{D}(p)) = True$$

➔ Then we conclude that p is correct with respect to the secrecy property.

Outline

- Motivations
- Overview
- Protocol Modelling
- Secrecy property
- Correctness conditions
- Correctness theorem
- Example
- Conclusion and future works

Conclusion and future works

- Conclusion
  - Sufficient conditions that ensure the correctness of security protocols with respect to the secrecy property
  - The verification of the conditions on a protocol doesn't require any verification on traces of the protocols analyzed
  - The verification of the conditions on a protocol can be completely automatized
  - Even if the conditions are strong, protocols that don't satisfy the correctness conditions can be easily adapted

Conclusion and future works

- Conclusion
  - Sufficient conditions that ensure the correctness of security protocols with respect to the secrecy property
  - The verification of the conditions on a protocol doesn't require any verification on traces of the protocols analyzed
  - The verification of the conditions on a protocol can be completely automatized
  - Even if the conditions are strong, protocols that don't satisfy the correctness conditions can be easily adapted
- Future works
  - To study the conditions in order to make them less strong
  - To investigate other security properties (integrity, authentication, etc.)
  - To investigate other class of protocols

Questions?