MPRI Exam 2-30 (part 1)
Cryptographic protocols: formal and computational proofs

Duration: 3h. All documents are allowed. Electronic devices are forbidden.

December, 3rd, 2014

Exercise 1 : Constraint solving

We consider the BAN-Yahalom protocol as described informally below. The purpose of this protocol is to establish a fresh session key K_{ab} between two participants A and B. This is done through a server S who shares a long-term symmetric key with each participant. The key K_{as} (resp. K_{bs}) is a symmetric key shared between A (resp. B) and S.

$$\begin{array}{ll} 1.\ A \to B: & A,\ N_a \\ 2.\ B \to S: & B,\ N_b,\ \{A, N_a\}_{K_{bs}} \\ 3.\ S \to A: & N_b,\ \{B, K_{ab}, N_a\}_{K_{as}},\ \{A, K_{ab}, N_b\}_{K_{bs}} \\ 4.\ A \to B: & \{A, K_{ab}, N_b\}_{Kbs},\ \{N_b\}_{K_{ab}} \end{array}$$

We consider the constraint system $\mathcal{C}$ given below with $T_0 = \{a,\ b, n_i, k_i\}$ and the classical inference system $\mathcal{I}_{\mathsf{DY}}$ to deal with symmetric encryption and pair.

$$\begin{array}{rcl} T_1 \stackrel{\mathsf{def}}{=} T_0,\ \langle a, n_a\rangle & \stackrel{?}{\vdash} & \langle a, x\rangle \\ T_2 \stackrel{\mathsf{def}}{=} T_1, \langle b, \langle n_b, \mathsf{senc}(\langle a, x\rangle, k_{bs})\rangle\rangle & \stackrel{?}{\vdash} & \langle a, x'\rangle \\ T_3 \stackrel{\mathsf{def}}{=} T_2,\ \langle b, \langle n'_b, \mathsf{senc}(\langle a, x'\rangle, k_{bs})\rangle\rangle & \stackrel{?}{\vdash} & \langle \mathsf{senc}(\langle a, \langle y, n_b\rangle\rangle, k_{bs}),\ \mathsf{senc}(n_b, y)\rangle \\ T_3 & \stackrel{?}{\vdash} & y \end{array}$$

1. Explain the scenario encoded by the constraint system $\mathcal{C}$. Who are the agents involved in this scenario ? What are the roles played by each agent ? How many instances of each role are they playing ? What is the security property under study ?
2. Check that the substitution $\sigma = \{x \mapsto n_i;\ x' \mapsto \langle k_i, n_b\rangle;\ y \mapsto k_i\}$ is a solution of $\mathcal{C}$, *i.e.* give proof trees witnessing that σ is a solution of the constraint system $\mathcal{C}$. Explain the underlying attack on the protocol using the informal Alice & Bob notation.
3. Solve the deducibility constraint system $\mathcal{C}$, using the simplification rules of the lectures, and give all the solutions of the constraint system $\mathcal{C}$. *You may notice that the simplification rules can always be applied to the first unsolved deducibility constraint, according to the completeness proof. Moreover, when using the rules* R_2 *and* R_3*, you may assume that* t, u, t_1, t_2 *are neither variables nor of the form* $\langle v_1, v_2\rangle$*. Completeness is still true under these hypotheses. This avoids unnecessary branching.*
4. We propose to modify the protocol by adding *tags*. We consider public constants $\mathsf{c}_1, \mathsf{c}_2, \ldots$ and we add such a constant in each ciphertext. For instance, messages 2 and 3 will be modified as follows :

$$\begin{array}{ll} 2.\ B \to S: & B,\ N_b,\ \{\mathsf{c}_1, A, N_a\}_{K_{bs}} \\ 3.\ S \to A: & N_b,\ \{\mathsf{c}_2, B, K_{ab}, N_a\}_{K_{as}},\ \{\mathsf{c}_3, A, K_{ab}, N_b\}_{K_{bs}} \end{array}$$

Of course, when an agent receives such a message, he will check (after decrypting the ciphertext) that the plaintext starts with the expected constant. Modify the constraint system $\mathcal{C}$ to reflect the changes done on the protocol. Let $\mathcal{C}_{\mathsf{tag}}$ the resulting constraint system. Is $\mathcal{C}_{\mathsf{tag}}$ satisfiable ? Could you comment on the usefulness of such a tagging mechanism from a security point of view ?

Exercise 2 : Blind signatures

We want to study the intruder deduction problem for the inference system $\mathcal{I}_{\mathsf{sign}}$ given below :

$$\frac{x \quad y}{\mathsf{blind}(x,y)} \qquad \frac{x \quad y}{\mathsf{sign}(x,y)} \qquad \frac{\mathsf{blind}(x,y) \quad y}{x} \qquad \frac{\mathsf{sign}(\mathsf{blind}(x,y),z) \quad y}{\mathsf{sign}(x,z)}$$

We consider two binary function symbols sign and blind. Intuitively, the term $\mathsf{sign}(m,k)$ represents the signature of the message m with the key k, and the term $\mathsf{blind}(m,r)$ represents the message m *hidden* with the random factor r. The blind signature primitive has the following property : given the signature of a blind message, *i.e.* $\mathsf{sign}(\mathsf{blind}(m,r),k)$, and the blinding factor r, it is possible to compute the signature of the message m, *i.e.* $\mathsf{sign}(m,k)$. This additional ability is also given to the intruder. This is the purpose of the last inference rule of the system $\mathcal{I}_{\mathsf{sign}}$.

1. Show that the inference system $\mathcal{I}_{\mathsf{sign}}$ is not *local* w.r.t. the notion of syntactic subterm that we have seen during the lectures.

   We consider a notion of extended subterms defined as follows : $st_{ext}(t)$ is the smallest set such that $st(t) \subseteq st_{ext}(t)$ and

   $$\text{if } \mathsf{sign}(\mathsf{blind}(u_1,u_2),u_3) \in st_{ext}(t) \text{ then } \mathsf{sign}(u_1,u_3) \in st_{ext}(t).$$

   This notion is extended to sets of terms as follows : $st_{ext}(T) = \bigcup_{t\in T} st_{ext}(t)$.
2. Let $T_0 = \{\mathsf{blind}(m,r),\ k,\ r\}$ and $u = \mathsf{sign}(m,k)$. Give two different proof trees Π_1 and Π_2 of $T \vdash u$ in $\mathcal{I}_{\mathsf{sign}}$ having minimal size (size = number of nodes).
3. Show that the inference system $\mathcal{I}_{\mathsf{sign}}$ is local w.r.t. the notion of extended subterms.
4. Show that the intruder deduction problem is decidable
   Input : a finite set T of terms, and a term u ;
   Output : Is u deducible from T in $\mathcal{I}_{\mathsf{sign}}$?

   Justify the termination of your algorithm.
5. We consider the simplification rules seen during the lectures where the underlying deduction relation used in R_1 is $\mathcal{I}_{\mathsf{sign}}$, and the notion of subterm used in R_2 and R_3 is the notion of extended subterm mentioned above. We consider the following theorem :

   Termination : There is no infinite chain $\mathcal{C} \rightsquigarrow_{\sigma_1} \mathcal{C}_1 \ldots \rightsquigarrow_{\sigma_n} \mathcal{C}_n$.

   Correctness : If $\mathcal{C} \rightsquigarrow_{\sigma}^{*} \mathcal{C}'$ for some constraint system $\mathcal{C}'$ and some substitution σ and if θ is a solution of $\mathcal{C}'$ then $\sigma\theta$ is a solution of $\mathcal{C}$.

   Completeness : If θ is a solution of $\mathcal{C}$, then there exist a solved constraint system $\mathcal{C}'$ and substitutions σ, θ' such that $\theta = \sigma\theta'$, $\mathcal{C} \rightsquigarrow_{\sigma}^{*} \mathcal{C}'$ and θ' is a solution of $\mathcal{C}'$.

   Say whether each of these statements is true or not. You will provide a short explanation to justify a positive answer, and a counter-example to illustrate a negative answer.

Exercice 3 : Encrypted Key Exchange protocol

The EKE protocol is designed to solve the problem of authenticated key exchange while being resistant against dictionay attacks. EKE is a password-only protocol : the password pw is the only shared data between the two participants A and B.

1. $A \to B : \quad \{pkey\}_{pw}$
2. $B \to A : \quad \{\{R\}_{pkey}\}_{pw}$
3. $A \to B : \quad \{N_a\}_R$
4. $B \to A : \quad \{N_a, N_b\}_R$
5. $A \to B : \quad \{N_b\}_R$

First, A generated a fresh private/public key pair, and then sends the public key encrypted with the password pw shared with B. Then B extracts the public key, generates a fresh session key R, encrypts it with the public key, and encrypts the result with the password. B sends this message to A. Then, nonces N_a and N_b are exchanged to perform the "hand-shaking" necessary to defend again replay attacks.

1. Give a signature $\mathcal{F}$ and an equational theory E suitable to model this protocol in a reasonnable way. We will assume that the operations symmetric encryption and decryption are commutative, *i.e.* $\mathsf{senc}(\mathsf{sdec}(x, y), y) = x$ is one of the equations in E. In the following, all the function symbols will be assumed to be public. So, your model is supposed to be reasonnable in this setting.
2. Write the processes $P_A(pw)$ and $P_B(pw)$ to model one session of the role A and one session of the role B.

   In the following, we consider the frame $\phi_0 = \mathsf{new}\, pw.\mathsf{new}\, \tilde{n}.\sigma_0$ obtained after a normal execution of one session this protocol. In other words, the attacker does not try to intercept, modify, or inject some messages during this execution.
3. Write the substitution σ_0, and the names $\tilde{n}$ that represent such an execution. We are interested in the following static equivalence (modulo the theory E you defined above) :

   $$\mathsf{new}\, \tilde{n}.\sigma_0 \overset{?}{\sim} \mathsf{new}\, pw.\mathsf{new}\, \tilde{n}.\sigma_0$$

   Does this static equivalence hold or not ? Justify your answer.
   Hint : You could rely on the algorithm seen during the lectures.
4. Using the result obtained at the previous question, deduce whether ϕ_0 is resistant to dictionary attack against pw or not ? Justify your answer.
5. Now, we assume that the asymmetric cryptosystem that is used to implement this protocol is *which-key revealing*, allowing an attacker to deduce if two ciphertexts were encrypted under the same key. Propose a signature $\mathcal{F}^+$ and a set of equations E^+ to reflect this new attacker model. Is ϕ_0 resistant to dictionary attacks against pw (considering the signature $\mathcal{F}^+$ and the equational theory E^+) ?