Security Homework

Guillaume Scerri, guillaume.scerri@lmf.cnrs.fr

December 20, 2024
Due date : January 7, 2025 midnight

1 A naïve protocol

We define the following key exchange protocol where g is the generator of some group, n_a, n_b, r are random numbers and $\{.\}_k^r$ is the symetric encryption of a message with key k and randomness r:

- $A \to B$: g^{n_a}
- $B \to A$: g^{n_b}
- $A \to B$: $\{ok\}^r_{(g^{n_b})^{n_a}}$

The goal of the protocol is to establish a shared key $g^{n_a \cdot n_b}$, we say that B accepts after receiving the last message from A and checking it.

Question 1. Provide a pi-calculus process modeling A, and one modelling B. You may use pattern matching for binding variables. Recall that A does not know n_b, and B does not know n_a.

In the remainder of this exercise, we model messages as terms built over variables $\mathcal{X}$, and names $\mathcal{N}$ with

- constructors $\cdot^{\cdot}/2$, $g/0$, $\{.\}/3$ and $ok/0$;
- destructor dec;
- equational theory: $(x^y)^z = (x^z)^y$;
- rewrite rule: $\mathrm{dec}(\{x\}^z_y, y) \to x$

Question 2. Provide a trace that leads to B accepting.

Question 3. Show that if we remove the equational theory there is no trace that leads to B accepting.
hint: you may want to reason on the set of messages that can be derived by the adversary.

Question 4. Does there exist a trace where B accepts and the key is not secret?

Question 5. Define the attacker deduction rule $\phi \vdash t$ (for t a ground term and ϕ ground substitution) if there exists a term $R \in \mathcal{T}(\mathcal{X})$ such that $R\phi \Downarrow t$. Show that $\vdash$ is decidable.

2 Signing

We add signature to our terms model, precisely we add:

- constructors sign, vk modeling the signing algorithm and verification key derivation (from the secret key);
- destructor verify;
- rewrite rule verify(sign(x, z), vk(z)) $\to x$

We modify the protocol by signing the first two messages as follows:

- Setup: vk(s_a), vk(s_b) is common knowledge (i.e. adversary, A and B)
- $A \to B$: sign(g^{n_a}, s_a)
- $B \to A$: sign(g^{n_b}, s_b)
- $A \to B$: $\{ok\}^r_{(g^{n_b})^{n_a}}$

Question 6. Describe a process $P_A(s_a, s_b)$ modeling A and a process $P_B(s_b, s_b)$ modeling B.

Question 7. Show that for a single instance of each A and B, if B accepts the key is secret at the end (i.e. $\phi \not\vdash k$ where k is the key derived by B, and ϕ the knowledge of the attacker at the end of the trace).

Question 8. Show that in the process $!P_A(s_a, s_b) \| !P_B(s_b, s_b)$, if a session of B accepts with key k then k is secret.

Question 9. Does the result still hold if we add a unary function symbol f and the rewrite rule $f(g^x) = x$ to our term model?

3 Computational model

We now consider the computational interpretation of the protocol.

A function $f : x \longmapsto f(x)$ (from $\mathbb{R}^+$ to $\mathbb{R}^+$) is called *negligible* (in x) when, for any polynomial p, there exists $\eta_0 \in \mathbb{N}$, such that for all $\eta \in \mathbb{N}, \eta > \eta_0$, we have $f(\eta) \leq \frac{1}{p(\eta)}$

We assume that no Probabilistic Polynomial time Turing Machine (PPTM) can distinguish the two following scenarios with non negligible probability (where the security parameter η is the size of the group):

1. g^a, g^b, g^{ab} with a, b randomly chosen,
2. g^a, g^b, g^r with a, b, r randomly chosen.

Precisely for all $\mathcal{A}$ PPTM (in η)

$$|\mathbb{P}(\mathcal{A}(1^\eta, g^a, g^b, g^{ab}) = 1) - \mathbb{P}(\mathcal{A}(1^\eta, g^a, g^b, g^r) = 1)| \text{ is negligible in } \eta$$

Question 10. Give an example of a group where this property does not hold.

We additionally assume that no PPTM can guess the key of the encryption scheme. Precisely for all $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ PPTM (in η)

$$|\mathbb{P}(\mathsf{n}, \mathsf{r} \text{ sampled at random; } m \leftarrow \mathcal{A}_1(1^\eta) : \mathcal{A}_2(1^\eta, \{m\}_{g^{\mathsf{n}}}^{\mathsf{r}}) = g^{\mathsf{n}}))| \text{ is negligible in } \eta$$

Question 11. Show that the sum of two negligible functions is still negligible.

Question 12. We consider a passive adversary that only observes and honestly forwards messages (i.e. the only trace of the protocol is the honest trace). Show that, under the hypothesis outlined above we have, for all $\mathcal{A}$ PPTM (in η), we have

$$\mathbb{P}(\mathcal{A}(1^\eta, \phi) = k(\phi)) \text{ is negligible in } \eta$$

where ϕ is the honest trace of the protocol, and k the key as derived by B for one instance of A and B.