Protocol Verification minicourse 2023 — Exam

Alessandro Bruni

May 23, 2023

1 Exam format

For this course's exam, you can choose one of two formats. The first is a mini project exam, where you prepare a group presentation on an interesting case-study or theory extension followed by individual questions. The second is based on solving the set of exercises in Section 3.

2 Mini-project exam

For the mini-project exam, you must form a 3-person group and select a paper from this list: `https://bblanche.gitlabpages.inria.fr/proverif/proverif-users.html`

Broadly speaking, the papers in this list refer to either case-studies of interesting cryptographic protocol that have been verified with ProVerif, or theoretical papers that build on proverif to extend its verification capabilities. You are welcome to look at the list to find a paper that matches your interest. Once you selected a paper, you can write to me at brun@itu.dk with your proposal and we can book a short 15 minute slot to discuss it.

You must then study the paper and prepare a 10-15 minutes presentation of the work. For theory papers, present a short summary of the theory that is introduced along with an example that showcases its use. For case studies, present the protocol and interesting design choices in its modeling with ProVerif, along with some interesting queries.

The exam will be in the form of an oral presentation, followed by individual questions, and should take about 30 minutes per group. The date of the oral exam is set on **July 4th**.

3 Exercise-based exam

For the exercise-based exam, you must solve the following exercise and **submit them to brun@itu.dk by June 19th**.

Exercise 1 (Message deduction)**.** Consider the inference system $\mathcal{I}_{DY}$ for the Dolev-Yao attacker (See [2] on page 14).

1. Construct a proof tree that solves the following message deduction problem:

$$sk_A, sk_B, \mathsf{aenc}(n_A, \mathsf{pk}(sk_B)), \mathsf{senc}(\mathsf{aenc}(n_B, \mathsf{pk}(sk_A)), n_A), \mathsf{senc}(s, \langle n_A, n_B \rangle) \vdash_{\mathcal{I}_{DY}} s$$

2. Explain why $\mathcal{I}_{DY}$ is called a *local theory*.

Exercise 2 (Deduction under equational theories)**.** Consider following equational theory E_{enc}, which correspond to the inference system $\mathcal{I}_{DY}$:

$$\mathsf{sdec}(\mathsf{senc}(x,y),y) = x \qquad \mathsf{adec}(\mathsf{aenc}(x,\mathsf{pk}(y)),y) = x$$
$$\mathsf{fst}(\langle x,y\rangle) = x \qquad \mathsf{snd}(\langle x,y\rangle) = y$$

1. Convert the proof tree of Exercise 1 into a proof tree that uses the equational theory (See $S \vdash_{E_{enc}} t$, [2] page 23).

Exercise 3 (Static equivalence of frames)**.** Which of the following pairs of frames are statically equivalent? For those that are not statically equivalent, present two distinguishing terms. That is, find a pair of terms M, N such that:

$$(M =_{E_{enc}} N)_{\varphi_1} \text{ and } (M \neq_{E_{enc}} N)_{\varphi_2} \text{ or viceversa}$$

1.
$$\varphi_1 = \nu a,b,k.\,\{\mathsf{h}(\mathsf{senc}(a,k))/x, \mathsf{senc}(b,k)/y\}$$
$$\varphi_2 = \nu a,b,k.\,\{\mathsf{h}(\mathsf{senc}(b,k))/x, \mathsf{senc}(b,k)/y\}$$

2.
$$\varphi_1 = \nu a,b,k.\,\{\mathsf{aenc}(\langle\mathsf{senc}(a,k),c\rangle, pk(k))/x, pk(k)/y, \mathsf{senc}(a,k)/z\}$$
$$\varphi_2 = \nu a,b,k.\,\{\mathsf{aenc}(\langle\mathsf{senc}(b,k),c\rangle, pk(k))/x, pk(k)/y, \mathsf{senc}(a,k)/z\}$$

Exercise 4 (Observational equivalence)**.** 1. Show that $A \not\approx B$:

$$A = \mathsf{in}(c,x);\mathsf{in}(c,y);\nu s;\nu k;\mathsf{out}(c,\mathsf{pk}(k));\mathsf{if}\ x \neq y\ \mathsf{then}\ \mathsf{out}(c,\mathsf{aenc}(\langle x,y,s\rangle,\mathsf{pk}(k)))$$
$$B = \mathsf{in}(c,x);\mathsf{in}(c,y);\nu s;\nu k;\mathsf{out}(c,\mathsf{pk}(k));\mathsf{if}\ x \neq y\ \mathsf{then}\ \mathsf{out}(c,\mathsf{aenc}(\langle x,y\rangle,\mathsf{pk}(k)))$$

Exercise 5 (Secrecy and authentication)**.** Model the following protocol in ProVerif. Does it satisfy the desired *Security Properties* (listed at the end)? Present adequate queries that prove or disprove each claim of *authentication, integrity, confidentiality.*

$$A \to S : \{\{A\}_{pk_B}, B\}_{k_{AS}} \tag{1}$$
$$S \to B : \{\{A\}_{pk_B}\}_{k_{BS}} \tag{2}$$
$$B \to A : \{N_b\}_{pk_A} \tag{3}$$
$$A \to B : \{m\}_{N_b} \tag{4}$$
$$B \to A : h(m) \tag{5}$$

Initial knowledge: A knows a symmetric key k_{AS} to communicate with S, as well as B's public key, denoted pk_B. B knows A's public key pk_A and a symmetric key shared with S called k_{BS}.

Values the protocol generates: m is the secret generated by A. B generates the nonce N_b.

Protocol description: A indicates to S that she wants to talk to B and encrypts the request with k_{AB}. The request contains A's identity encrypted with B's public key. S will transmit the request to B, re-encrypting it with the shared key k_{BS}. B sends the nonce N_b to A encrypted with A's public key pk_A. A sends the secret m to B encrypted with the nonce N_b. B sends the hash $h(m)$ to ensure the integrity of the message m.

Security properties:

1. *Authentication*: when B accepts m, it's certain that it comes from A.
2. *Integrity*: A is certain that B has accepted m by receiving $h(m)$ in (5)
3. *Confidentiality*: A and B are the only ones who know m.

References

[1] Bruno Blanchet, Ben Smyth, Vincent Cheval, and Marc Sylvestre. Proverif 2.00: Automatic cryptographic protocol verifier, user manual and tutorial. 2018.

[2] Véronique Cortier and Steve Kremer. *Formal Models and Techniques for Analyzing Security Protocols-Volume 5*. IOS Press, 2011.