Security Protocol Verification with Proverif

Laboratory for the class "Security Verification and Testing" (01TYASM/01TYAOV)
Politecnico di Torino – AY 2021/22
Prof. Riccardo Sisto

prepared by:
Riccardo Sisto (riccardo.sisto@polito.it)

v. 0.1 (25/10/2021)

Contents

Purpose of this laboratory

The purpose of this lab is to make experience with security protocol verification using Proverif.

For the proposed exercises you are invited to use the typed version of extended pi calculus (for which Proverif provides type checking). The full language reference can be found in the Proverif manual and Tutorial (`https://bblanche.gitlabpages.inria.fr/proverif/manual.pdf`).

This is a summary of the commands to use Proverif:

- Run Proverif on a script file:

```
proverif filename
```

- Run Proverif on a script file and request Proverif to generate an attack trace in a given directory:

```
proverif -graph directory filename
```

- Run Proverif on a script file in interactive mode to perform a simulation:

```
proverif_interact filename
```

1 Verifying and fixing the sample handshake protocol

In this part of the lab we make some experiments with the sample handshake protocol that was discussed in the lectures.

1.1 Reproducing the results already shown in the classroom

First of all, in order to reproduce the same results shown in the lectures, let's run Proverif on the file handshake1cie.pv, which includes the description of the protocol and the following security queries:

1. secrecy of s
2. reachability of the end of each process (these are not security queries but sanity checks to verify that each process can really reach the end).
3. server to client authentication:

   ```
   query x:pkey,y:pkey,z:bitstring; inj-event(eC(x,y,z)) ==>
   inj-event(bS(x,y,z)).
   ```

   which means: if a client with public key y correctly receives key z, apparently coming from a server with public key x, then a server with public key x really sent key z to the same client and each receive operation corresponds to a distinct send operation (injectivity).

From the Proverif verification report, you can see that properties 1 and 2 are satisfied (note that reachability is satisfied if the queries return false), while 3 is not. Indeed, the report specifies that the non-injective correspondence holds, i.e. only injectivity does not hold.

Run again Proverif with the switch -graph (see command at the beginning), which produces a graphical view of the attack trace found by Proverif and look at the trace. What is the behavior of the attacker in the attack trace?

Solution

As it can be seen in the attack trace reconstructed by Proverif (trace11.pdf), the attacker replays the first message sent by pS to another instance of pC

1.2 Fixing the protocol

If we do want injectivity we need to fix the protocol. One way to do it is to add a preliminary step in the protocol, by which pC first sends a randomly generated value (a nonce, which acts as session id) to pS in order to request the key, and pS responds to this request by sending the same nonce together with the key. In this way, the attacker should not be able to replay the message with the key into a different session. Write a Proverif script that describes the fixed version of the protocol (you can start from the version in handshake1ci.pv and modify it). Note that the events of the correspondence have to be changed accordingly, by including the nonce as well, otherwise events belonging to different sessions cannot be distinguished.

After having described the fixed version, check that it passes the injective version of the server to client authentication property (and that all processes reach the end). In case of problems, you can use the simulator to understand why.

Report the Proverif script with the fixed version of the protocol:

Solution

see handshake1cie_fixed.pv

1.3 Verifying the authenticity of the secret

Now that the protocol has been fixed, we can try to verify that the secret sent by pC to pS is authentic, i.e., whenever pS receives the secret, indeed the secret was sent by pC, and the correspondence is injective, i.e. each receive of the secret is preceded by a distinct send of the secret. Note that, in order to express this property, we need to introduce other events in the protocol description.

Report the Proverif script, modified to include the verification of this additional authentication property.

Solution

see handshake2cie.pv

What is the result? Is the property already true or does the protocol need to be fixed to satisfy it?

Solution

The property is already true.

1.4 Verifying the integrity of the secret

Let's try to verify that the secret cannot be changed while in transit. In order to verify this property, we can modify the description of the processes, so that there is no longer a single secret, but two different secrets, s1 and s2. We can have then some pC sessions that send s1 and some that send s2. Finally, we verify that what is received corresponds (injectively) o what was sent.

Report the Proverif script, modified to include the verification of this additional integrity property.

Solution

see handshake3cie.pv

What is the result? Is the property already true or does the protocol need to be fixed to satisfy it?

Solution

The property is already true.

2 Verifying and fixing the sample hash protocol

In this part of the lab we make some experiments with the sample hash protocol that was discussed in the lectures.

2.1 Reproducing the results already shown in the classroom

First of all, in order to reproduce the same results shown in the lectures, let's run Proverif on the file hash.pv, which includes the description of the protocol and its secrecy properties:

1. secrecy of s
2. reachability of the end of each process (these are not security queries but sanity checks to verify that each process can really reach the end).
3. resistance to offline guessing of s.

From the Proverif verification report, you can see that properties 1 and 2 are satisfied (note that reachability is satisfied if the queries return false), while 3 is not.

Run again Proverif with the switch -graph, which produces a graphical view of the attack trace found by Proverif and look at the trace. What is the behavior of the attacker in the attack trace?

Solution

As it can be seen from the attack trace reconstructed by Proverif (trace21.pdf), the attacker records the message hash(s) and then it performs offline comparison between hash(s) and hash(g), where g is the guess. If they are equal, the guess is correct.

2.2 Fixing the protocol

There is a simple fix to this protocol, so that it resists to offline guessing attacks. Can you find it and verify that the solution is correct?

Solution

A possible solution is to hash the secret together with another high-entropy secret. See hash_fixed.pv.

3 Defining and verifying a simple signature protocol

In this part of the lab we try to develop and verify the model of a simple protocol to guarantee the authenticity of a software issued by a software vendor.

We model the software by means of a name sw, and its associated description (software name, author, version, etc), by means of another name swd. We use a process to model the issuer of the software, and we assume the issuer issues a software sw and its associated description swd protected by a signature (we assume the issuer has a private/public key pair). On the other side, we model the receiver of the software as another process that checks the signature before accepting the software with its description as authentic.

Assuming that the issuer issues several distinct software packages, each one with its corresponding description, we want to make sure that the receiver will accept as valid only a software with its description as they have been issued by the issuer, and no fake software nor fake descriptions nor other combinations (e.g. right software with wrong description).

Specify the protocol and the property described above in a Proverif script and try to verify it.

Solution

see signature.pv