Protocol name

Author(s): Authors, institutions... 0, 1988
Submitted by Editor December 24, 2002
Last modified December 24, 2002

Summary: Short description of the protocol goals (authentification, key exchange...) and of the cryptographic needs (symmetric or public keys algorithms, one-way functions, server...).

Protocol specification (in common syntax)

```
Var1, Var2,... :  type

label.   Sender  ->  Receiver   :    contents
label.   Sender  ->  Receiver   :    {contents}key
```

Description of the protocol rules

Explanation of the steps of the protocol, defined in the above section. It can refers to the messages labels and to the identifiers used in the protocol definition.

Requirements

The properties that the protocol is supposed to ensure, written in natural language.

References

This section cites the work where the protocol was originally defined, and optionally also some other important references.

The references are given with bibtex commands like e.g. [**?**].

Claimed proofs

This section list some known works where the protocol has been proved to satisfy one of the properties given above, with bibtex commands.

Claimed attacks

This section cites some known works where the protocol has been shown **not** to satisfy one of the properties given above, it is good to give here also a scenario of each attack, following the examples in [CJ97]:

```
label.     Sender    ->  I(Receiver)  :    contents
label.   I(Sender)   ->    Receiver   :    {contents}key
```

The references are given with bibtex commands.

Remark

A few remarks can be added about e.g. the protocol versions or related works on this protocol that do not fit in one of the three above categories.

See also

Cross references to other protocols of the library, using the command Protocol name (here, the cross reference points on the same file, for the example purposes).

Citations

[CJ97] John Clark and Jeremy Jacob. A survey of authentication protocol literature : Version 1.0., November 1997.