SmartRight view-only

Author(s): Jean-Pierre Andreaux, Sylvain Chevreau, Eric Diehl 2001
Submitted by Thomas Genet March 6, 2003
Last modified March 6, 2003

Summary: This *view-only* protocol is part of the SmartRight system designed by Thomson for copy protection for the Digital Video Broadcasting technology. Its purpose is to ensure that the digital content broadcasted can be view only once. It uses symmetric key cryptography with nonces and xor.

Protocol specification (in common syntax)

```
CC, TC :                 principal
VoKey, VoR, VoRi, CW :   number
Kc :                     key
h :                      number -> number

1.   CC  ->  TC  :   {VoKey, CW+VoR}Kc
2.   TC  ->  CC  :   VoRi
3.   CC  ->  TC  :   VoR, {h(VoRi)}VoKey
```

Description of the protocol rules

The above presentation and these explanations are extracted from [GTTT03]:

The protocol is deployed between two smartcards: `CC` (Converter Card) and `TC` (Terminal Card), respectively in an access device (i.e. a digital receiver) receiving a scrambled digital content and a presentation device (i.e. a television) which is supposed to descramble the content before rendering it. The keys used to scramble the content are called *control words* `CW`.

The cards `CC` and `TC` share a secret symmetric encryption key `Kc`.

`CC` generates first the random values `VoKey` and `VoR`, and sends them encrypted to `TC` (in message `1`), together with a `CW` which has been received (by the access divice) with the scrambled content. The operator `+` is xor.

`TC` then sends in return a random challenge `VoRi` (message `2`). The message `3` is the answer of `CC` to the challenge. After receiving the message `3`, `TC` checks if the answer is correct, by comparing the hashed value `h(VoRi)` with its own value, and if so, it extracts `CW` and uses it to descramble the content.

Note on memory management:

- After sending the message `3`, `CC` deletes `VoR` and `VoKey` from its memory.
- After receiving and accepting the message `3`, `TC` deletes `VoRi` from its memory.

This is very important (with respect to the property below) because of the control aspects given below.

Note on control: The principal `CC` and `TC` switch to the next state only once they have received the next message expected (and not once they have send a message as usual). More precisely:

- After sending message `2`, `TC` will continue to accept a (new) message `1` and reply by a (new) `VoRi` (message `2`) until it receives the message `3` and accepts it.
- After sending message `2`, `TC` will process all the messages `3` it shall receive until it receives a new message `1`.

Requirements

cited from [GTTT03]: The control word `CW` may be extracted by `TC` only once at the time where the protocol is played.

References

[Tho01], [GTTT03].

Claimed proofs

The above property is proved in [GTTT03] in an automated way on a term rewriting model using Timbuk, a verification tool using abstract interpretation over tree automata domains.

Citations

[GTTT03] Thomas Genet, Yan-Mei Tang-Talpin, and Valérie Viet Triem Tong. Verification of copy-protection cryptographic protocol using approximations of term rewriting systems. In *Proc. of WITS'03, Workshop on Issues in the Theory of Security*, 2003.

[Tho01] Thomson. Smartright technical white paper v1.0. Technical report, Thomson, october 2001. http://www.smartright.org.