Protocol for detection of hidden discredit of signature secret key

VADIM N.TSYPYSCHEV

S-TERRA CSP

Task

- Let's suggest that we exploit IPSec VPN.
- Partially, we exploit PKI to mutual authentication of terminals.
- The authentication fail if intruder get access to signature generation of secret key.
- The problem to solve is that: how to detect the case if intruder get access to secret key?

Purpose

- **To detect the case if intruder get access to secret key of signature generation and at least once has used it.**

Method

- We create special Distributed Ledger reflecting the history of connections between IPSec terminals of the network.
- During the process of Security Association creation we analyse it and investigate the fact that two different terminals have used the same secret key for authentication.

Limitations

- **We can investigate ONLY standard method of ISAKMP-Protocol.**