Trusted Cryptographic Tools Locking

VADIM N.TSYPYSCHEV

Full version

- V.N.Tsypyschev
- Trusted Cryptographic Tools Locking
- CSOC'2018

Problems

- How to deactivate cryptographic components embedded into complex IT security product without its cutting and erasing?
- How to activate cryptographic components back if it is necessary?

Method of Locking

- To obfuscate the software of cryptographic components going to be deactivated in such way that it capability will depend on the content of text file significantly complicated by cryptographic tools
- To hide this text file from customers of reduced IT security product

Method of Activation of Cryptographic Components

- To provide legal customer of reduced IT security product by special license
- To create Installer as a local entity executing an Activation Protocol
- To create a Trusted License Server as Trusted Third Party entity executing an Activation Protocol
- To create a cryptographically secure Activation Protocol between legal customer, Installer and Trusted License Server providing in result locked cryptographic components by the content of that text file needed for entire IT secure product validity

Trusted Locking of Cryptographic Tools is a widespread problem

- If this question is under jurisdiction of TC26 it could be very useful to provide community by technical recommendation about how trustworthy lock cryptographic components embedded in IT security systems