INFORINO 2020
Moscow, Russia
14-17 April, 2020

A technique of protocol construction for detecting compromises of secret keys

Speaker:

Svetlana Kuzmicheva

PhD Student

Authors:

- Kiryakina Marina
  Institute of Cyber Intelligence Systems
  National Research Nuclear University MEPhI
- Kuzmicheva Svetlana
  Institute of Cyber Intelligence Systems
  National Research Nuclear University MEPhI
- Zapechnikov Sergey
  Institute of Cyber Intelligence Systems
  National Research Nuclear University MEPhI
  Research Center for Cryptocurrencies and Digital Assets

The purpose and objectives of the study

The purpose of the study:

Increasing the resistance of information protection tools and systems to the effects of an active intruder capable of gaining access to confidential user information.

The object of the study:

The process of ensuring the security of cryptographic keys in the exchange of information.

The subject of the research:

The detection of compromise of cryptographic keys.

The relevance of research

- the inability to detect an attacker in the early stages of the attack
- the inability to detect compromised accounts and subsequent unauthorized access to a system
- high duration and complexity of information security incident investigations

Cryptographic keys can be compromised in various ways:

System compromise

Viruses

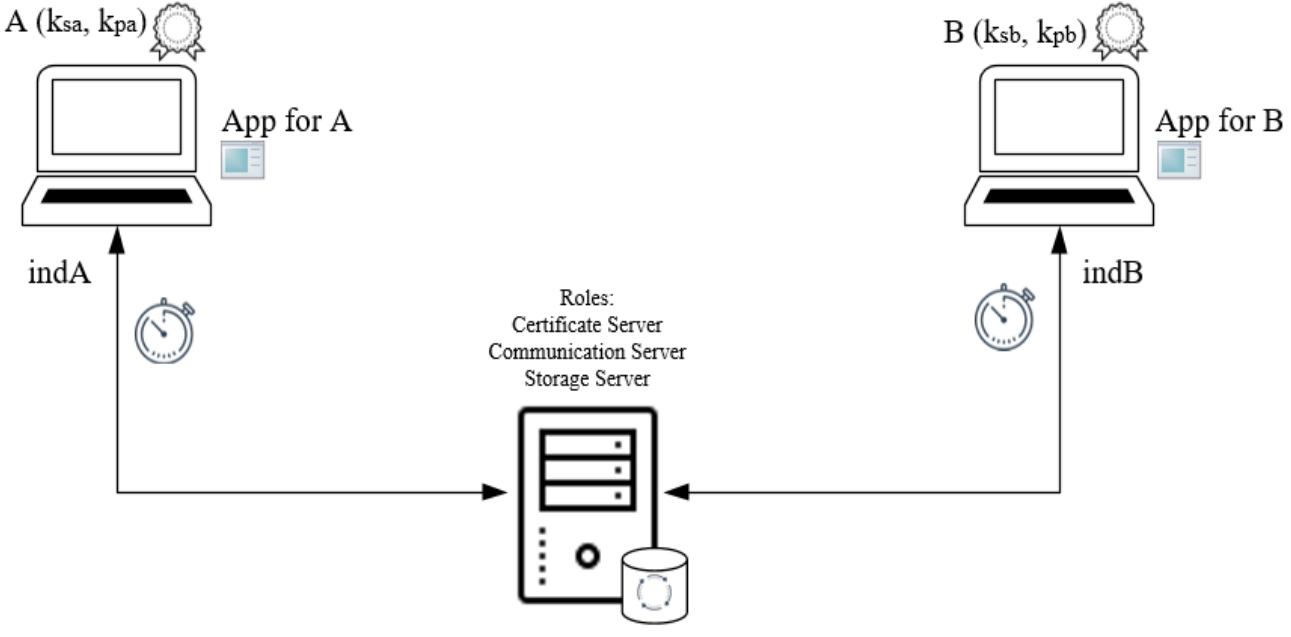
Cryptanalysis

Approaches to identifying compromise on the protocol level

Detection method	Method Features	Disadvantages of the method
Trace-independent inconsistency	A message was received but it isn't specific to the current message set.	The method is theoretical.
Observation of a contradiction	The counter is transmitted in the message, it's allowing participants to control the sequence of messages.	The method gives a false result in case of compromising the key values of both opponents.
Observation of acausality	The message includes a chain of hash-codes of previous messages	• The method allows you to identify an attacker if he left the protocol • Increasing the amount of data transmitted using hash codes

Blockchain-based secret key compromise detection protocol

(sk, pk) – private and a public key of protocol
ind – protocol participant ID



Role Model Messaging Protocol

Client component:

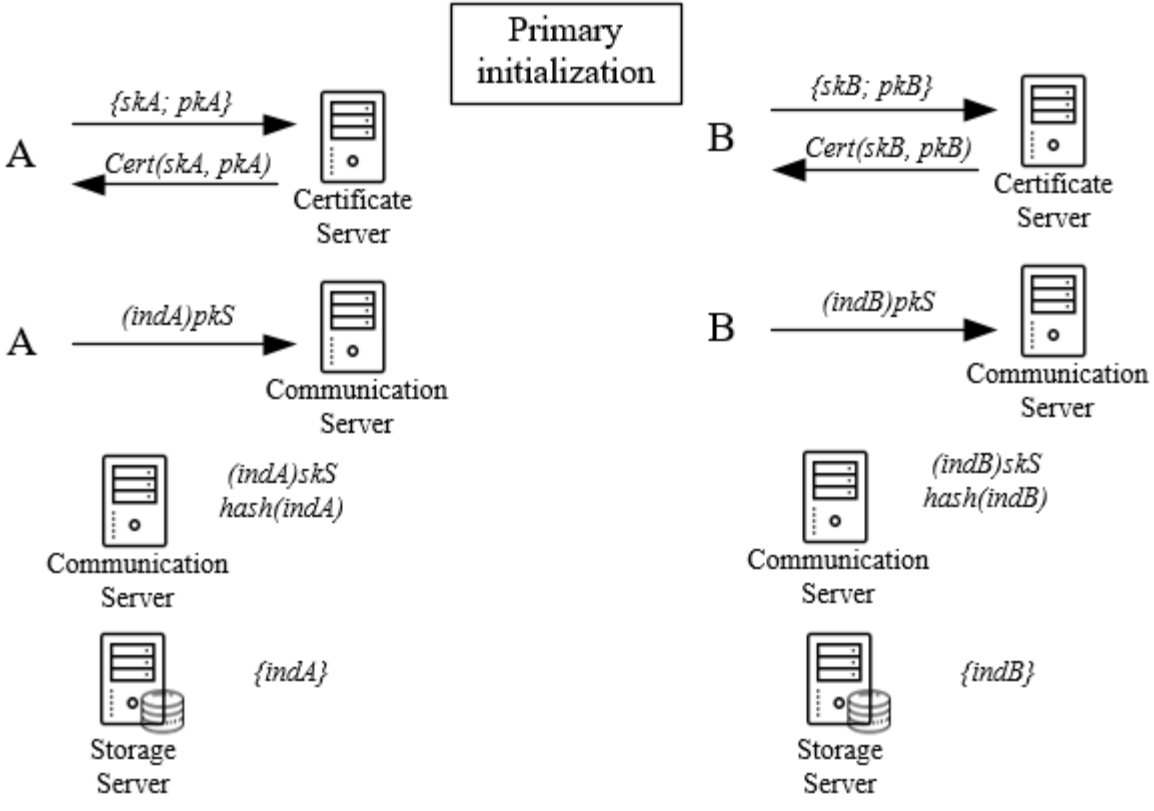
- *The initiator of the sending process* - the role of the device sending the message
- *The recipient of the message* - the role of the device receiving the message

Server component:

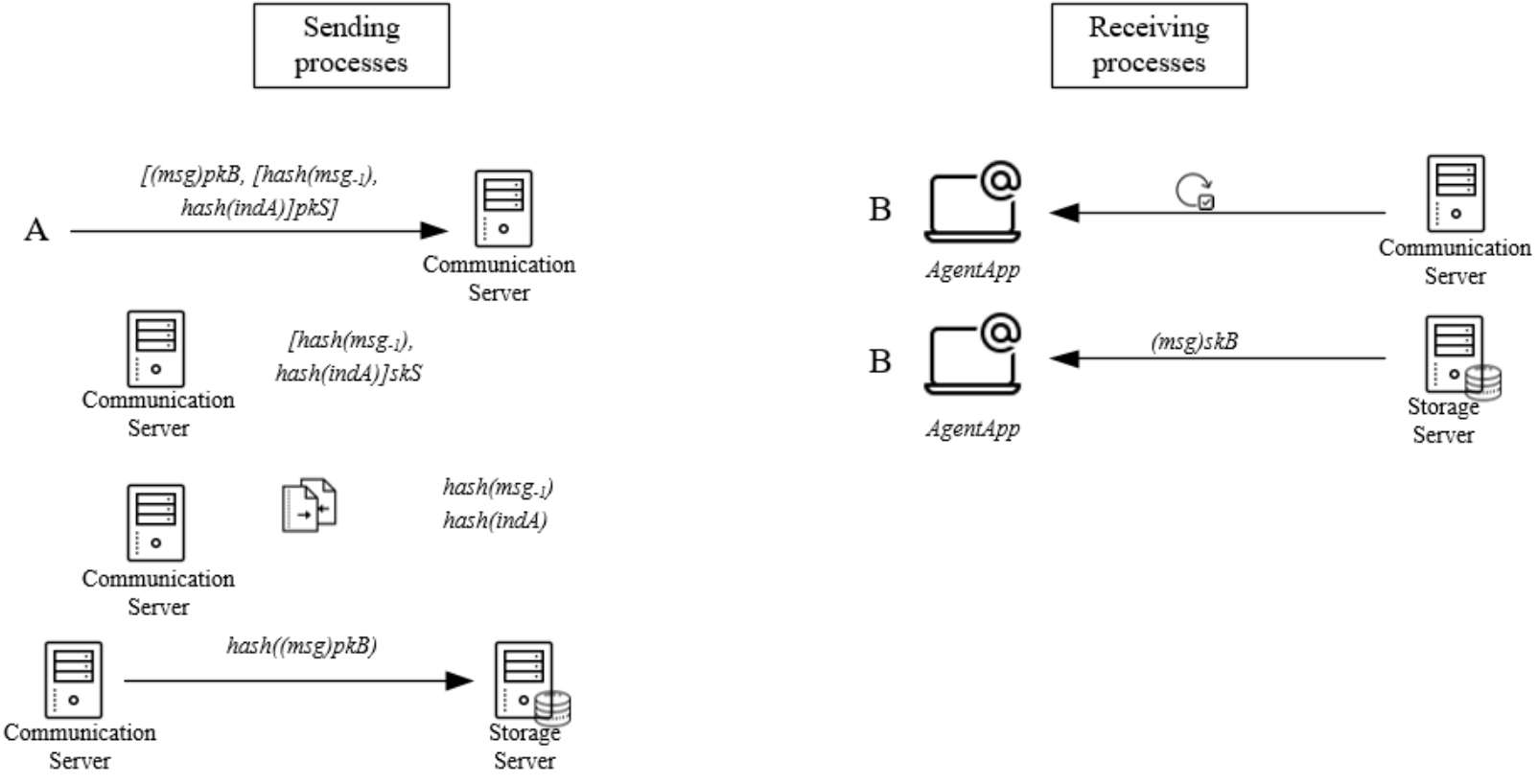
- *Information storage server* - the role of the server component, storing information transmitted between users through blockchain technology.
- *Information transfer server* - the role of the server component, processing the message queue for exchanging information between users.
- *Certification Authority Server* - the role of the server component, combining the roles of a certification authority and a registration center.

Working with keys: primary initialization

- *A* – Initiator
- *B* – Recipient
- *Serv* – server with roles Information storage server, Information transfer server, Certification Authority Server *cert(skS, pkS)*



Sending and receiving messages



Attack Detection Principle

The protocol allows you to detect a compromise of key information in the following cases:

- message sequence mismatch: the hash codes of the current and previous messages are checked in the blockchain
- inability to authenticate a participant by identifier

Modeling in Tamarin Prover

The main properties of the proposed protocol are formulated in the work:

Client authentication - this lemma demonstrates the property of using authentication by an identifier in a simulated protocol;

The correctness of the protocol - this lemma helps us verify the situation when the recipient receives a message without the participation of an attacker;

Secrecy of a client session key - this lemma means the ability to have a session key in secret without the participation of an attacker;

Storage Server Processing Security - this lemma demonstrates the security feature of the interaction of the storage server with data.

Modeling in Tamarin Prover

Using Tamarin Prover utility, a protocol security analysis was performed. Highlighted situations:

- An attacker gains access to one of the client identifiers - the situation does not lead to a compromise of the protocol, the identifier hash is stored

- An attacker gains access to the server's secret key - the situation leads to a compromise of the protocol because the server key is stored in a single place and its additional verification is not performed

Results

As part of the research work, the following tasks were completed:

- ✓ The architecture and description of the protocol for detecting the compromise of cryptographic keys is proposed.
- ✓ Analysis of protocol security by the model in Tamarin Prover is defined.

INFORINO 2020

Moscow, Russia
14-17 April, 2020

Thank you for attention!

Speaker's contacts:

Svetlana Kuzmicheva

PhD Student

tz7sveta@yandex.ru

IEEE

МЭИ NATIONAL RESEARCH UNIVERSITY

CROC