Thesis Defense

Securing the Authcoin Protocol Using Security Risk-oriented Patterns

Author: Benjamin Leiding
First Examiner: Dieter Hogrefe
Second Examiner: Alexander Horst Norta

March 21, 2017

Overview

Introduction

Authcoin

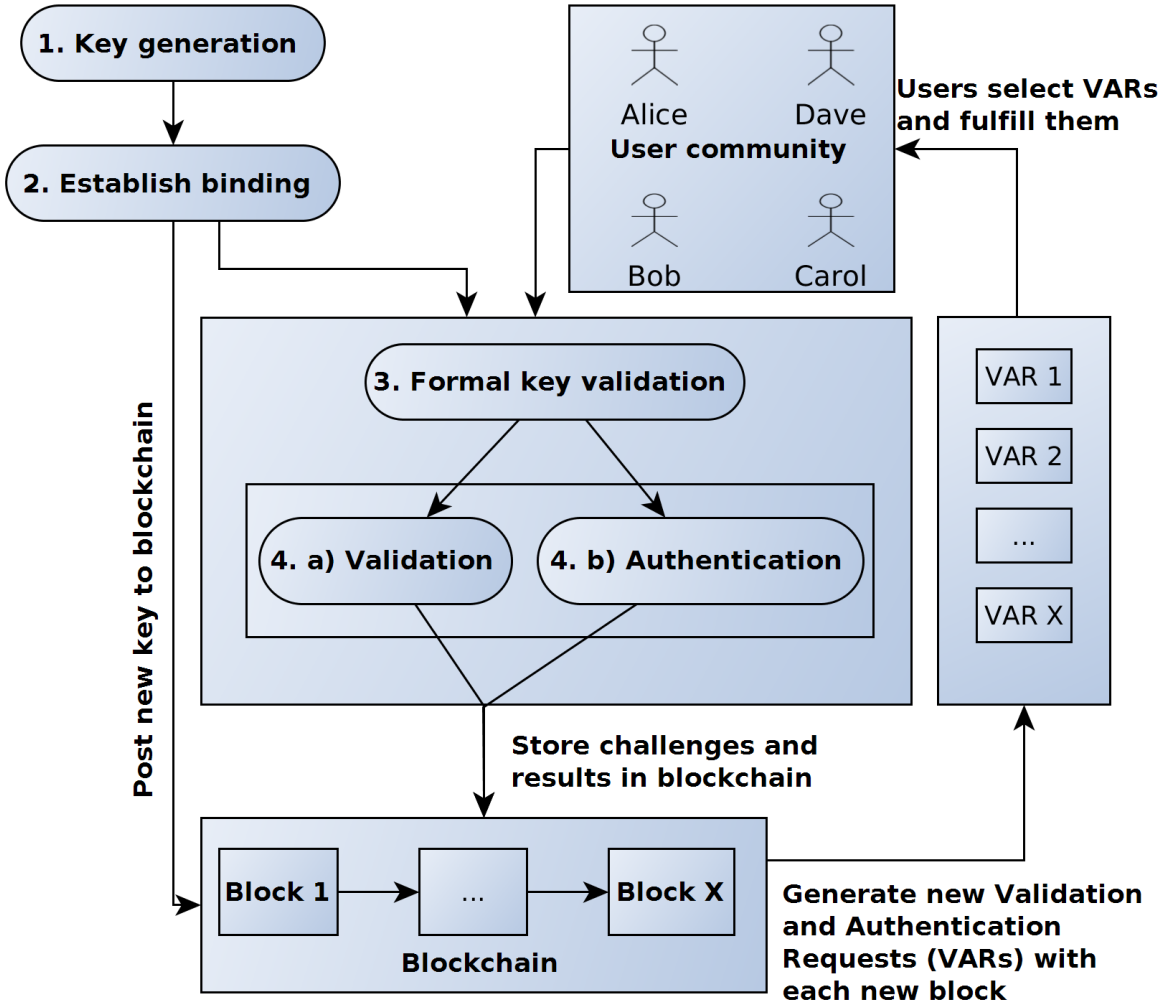


Figure: Abstract overview on the workflow of the Authcoin protocol

Security Patterns

Definition

A security pattern is "a particular recurring security problem that arises in specific contexts and presents a well-proven generic scheme for its solution" [2].

Security Risk-Oriented Patterns (SRPs)

- Introduced by Ahmed et al. [3][4]
- Based on understanding security risks that arise within business processes
- Enable business analysts to design secure business processes either on their own or with security analysts
- Five existing SRPs available
- So far only applied to business processes

Research Methodology

Research Gap

- Provide a complete and correct formal specification of the Authcoin protocol
- Apply security risk-oriented patterns to the formal models of Authcoin

- Using the Design Science Research (DSR) methodology for Information Systems (IS) research [5]
- Create new and innovative artifacts (constructs, models, methods and utility)

Research Questions

Research Questions

RQ: How to secure the Authcoin protocol by employing formal techniques combined with applying security risk-oriented patterns?

- RQ-1: How to formalize the Authcoin protocol?
- RQ-2: How to analyze security threats to the Authcoin protocol?
- RQ-3: How to apply security risk-oriented patterns to the Authcoin protocol?

RQ-1: How to formalize the Authcoin protocol?

Colored Petri Nets (CPNs)

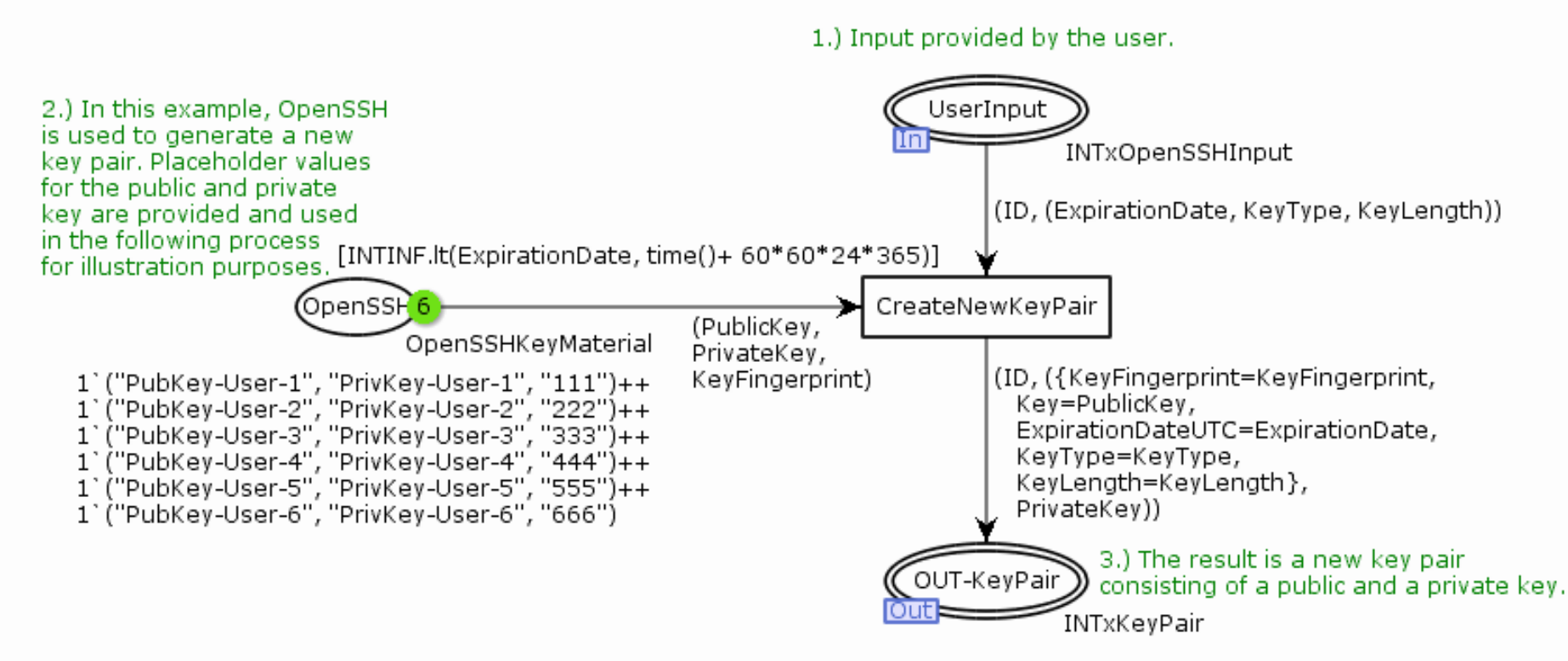


Figure: CPN model of the "CreateNewKeyPair" module

Modeling Methodology

Agent-oriented Modeling (AOM)

- Authcoin organizes V&A between entities (agents)
- Mahunnah et al.[6] introduce mapping heuristics from agent models to CPN models based on Sterling's and Taveter's [7] methodology for Agent-Oriented Modeling (AOM)
- Goal models and behavior interface models

Goal Model

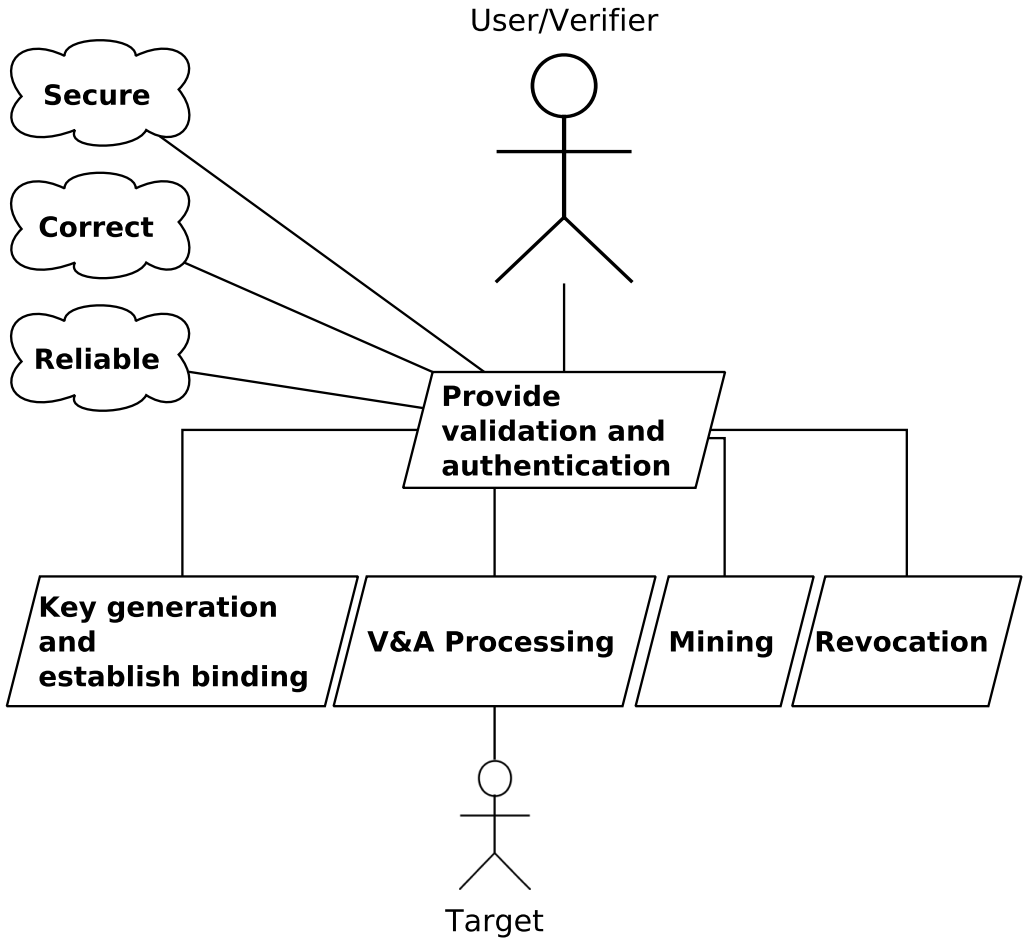
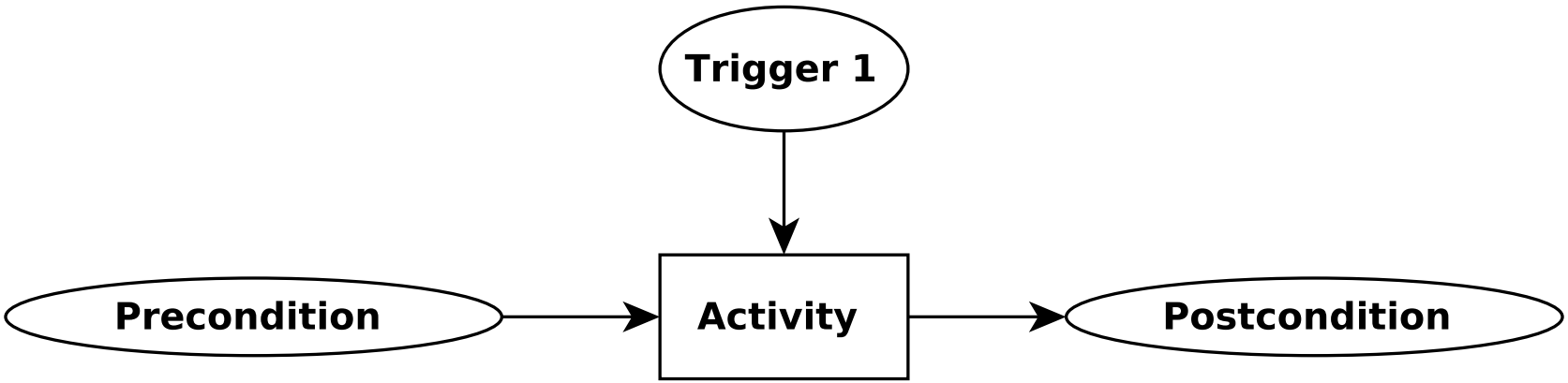


Figure: Authcoin - Top level goal model

Behavior Interface Model



Authcoin - Top-Level CPN Model

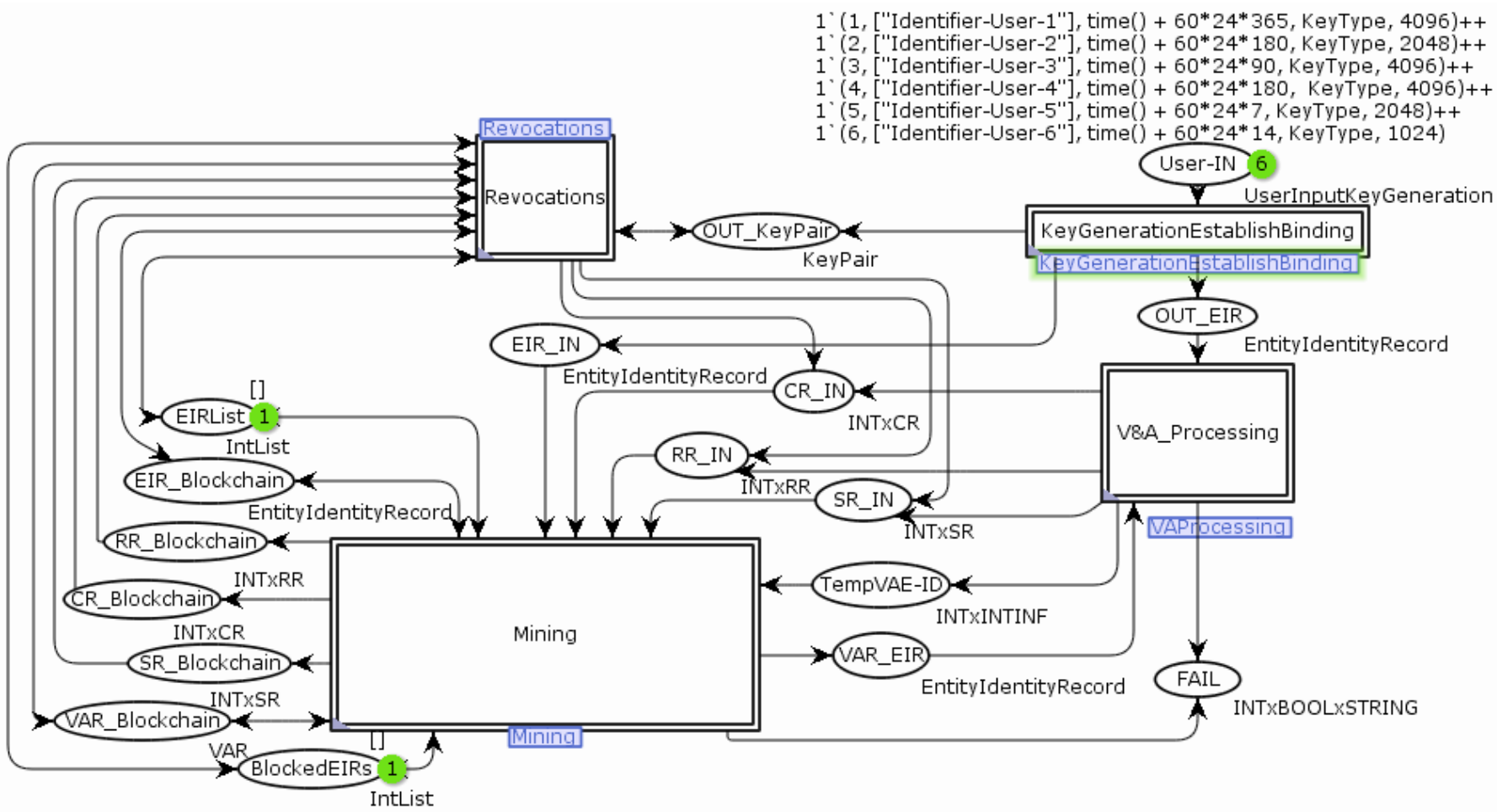


Figure: Authcoin - Top level CPN model

RQ-2: How to analyze security threats to the Authcoin protocol?

Information Systems Security Risk Management (ISSRM) Domain Model

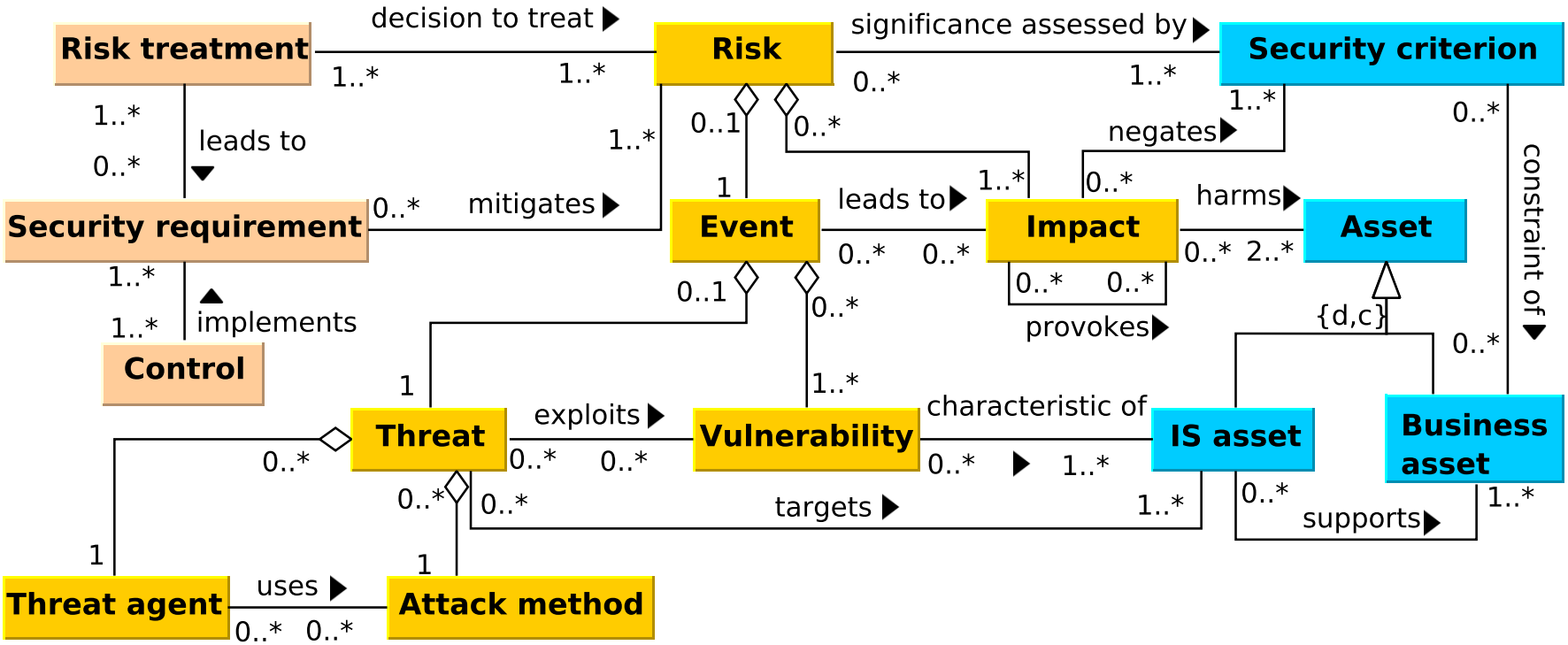


Figure: ISSRM domain model (Adapted from: [8])

Identification of Assets

Information System Assets

Systems:

- Messaging system
- Blockchain
- User devices and operational software
- Underlying communication network

Processes:

- Send - Send information to other entities
- Receive - Receive information from other entities
- Post - Post information to the blockchain

Business Assets

Exchanged data records (Challenges, Responses, Signatures, etc.)

Analysis Results

Risk 1

Risk of data record manipulation during the process of posting information to the blockchain.

Risk 2

Risk of data record manipulation during the process of exchanging V&A related information during the protocol execution.

Risk 3

Risk of a local or global DDoS attack on Authcoin's users or infrastructure.

Risk Treatments

Risk treatment	Risk reduction
Security requirement	Integrity checks of submitted records
Controls	Signed hashes

Table: Treatment of risk 1 (Post) and risk 2 (Send/Receive)

Risk treatment	Risk reduction
Security requirement	Mitigate service disruption
Controls	Decentralization, load distribution and balancing

Table: Treatment of risk 3 (DDoS)

RQ-3: How to apply security risk-oriented patterns on the Authcoin protocol?

Integration and Implementation of Existing SRPs

SRP 1

Secures the data transmission between business entities with focus on preventing the loss of data, confidentiality and its integrity. The pattern proposes to make the data unreadable before transmitting, calculate checksum values and utilize transmission mediums that cannot be intercepted.

- Review existing SRPs and select appropriate ones
- Identify SRP occurrences
- Update goal models, behavior interface models and CPN models

Evaluation

State Space Analysis Results

Module	**Loop(s)**	**Dead marking(s)**	**Dead transition(s)**
Key Generation Establish Binding	No	Yes*	No
Formal Validation	No	Yes*	Yes*
Validation & Authentication	No	Yes*	Yes*
VAR Creation	No	Yes*	No
Process VAR	No	Yes*	Yes*
Revocations	No	Yes*	Yes*

Table: Selected state space analysis results of the CPN models.

Conclusion and Future Work

Conclusion

Conclusion

- Formalized Authcoin using CPNs, based on an AOM methodology
- Performed a risk and threat analysis using the ISSRM domain model and identified three risks
- Implemented SRP 1 and mitigated two risks
- Performed state space analyses before and after integrating SRP 1 into the CPN models of Authcoin

Future Work

Future Work

- Overcome modeling limitations
- Implement Authcoin
- External penetration testing and security feedback
- Automated pattern occurrence detection
- Identification of unknown SRPs
- Further vetting and analysis of existing SRPs

Questions?

Bibliography I

- A. Norta, P. Grefen, and N. C. Narendra, "A Reference Architecture for Managing Dynamic Inter-organizational Business Processes," Data & Knowledge Engineering, vol. 91, pp. 52–89, 2014.
- M. Schumacher, "Security Engineering with Patterns: Origins, Theoretical Models, and New Applications," 2003.
- N. Ahmed, R. Matulevičius, and N. H. Khan, "Eliciting Security Requirements for Business Processes Using Patterns," in Proceedings of the 9th International Workshop on Security in Information Systems (ICEIS 2012), 2012, pp. 49–58.
- N. Ahmed and R. Matulevičius, "Securing Business Processes Using Security Risk-oriented Patterns," Computer Standards & Interfaces, vol. 36, no. 4, pp. 723–733, 2014.

Bibliography II


A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," MIS quarterly, vol. 28, no. 1, pp. 75–105, 2004.


M. Mahunnah, A. Norta, L. Ma, and K. Taveter, "Heuristics for Designing and Evaluating Socio-technical Agent-Oriented Behaviour Models with Coloured Petri Nets," in Computer Software and Applications Conference Workshops (COMPSACW), 2014 IEEE 38th International. IEEE, 2014, pp. 438–443.


L. Sterling and K. Taveter, The Art of Agent-oriented Modeling. MIT Press, 2009.

Bibliography III


É. Dubois, P. Heymans, N. Mayer, and R. Matulevičius, "A Systematic Approach to Define the Domain of Information System Security Risk Management," in Intentional Perspectives on Information Systems Engineering. Springer, 2010, pp. 289–306.