Proceedings of STPIS'15

# Modelling and Analysing Socio-Technical Systems

Zaruhi Aslanyan, Marieta G. Ivanova,
Flemming Nielson and Christian W. Probst

DTU Compute, Technical University of Denmark, Denmark
{zaas,mgiv,fnie,cwpr}@dtu.dk

Modern organisations are complex, socio-technical systems consisting of a mixture of physical infrastructure, human actors, policies and processes. An increasing number of attacks on these organisations exploits vulnerabilities on all different levels, for example combining a malware attack with social engineering. Due to this combination of attack steps on technical and social levels, risk assessment in socio-technical systems is complex. Therefore, established risk assessment methods often abstract away the internal structure of an organisation and ignore human factors when modelling and assessing attacks. In our work we model all relevant levels of socio-technical systems, and propose evaluation techniques for analysing the security properties of the model. Our approach simplifies the identification of possible attacks and provides qualified assessment and ranking of attacks based on the expected impact.

We demonstrate our approach on a home-payment system. The system is specifically designed to help elderly or disabled people, who may have difficulties leaving their home, to pay for some services, *e.g.*, care-taking or rent. The payment is performed using the remote control of a television box with a contactless payment card (see Figure 1). When a transfer is initiated, a password is needed in order to authenticate the owner of the card.

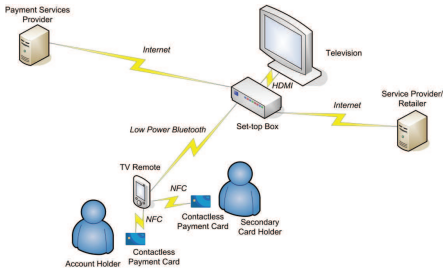


**Fig. 1.** System overview.

## Model

Our model is based on work by Probst et al. [1] and Dimkov et al. [2]. To facilitate formal methods, the model represents the infrastructure of organisations - the

©Copyright held by the author(s)

physical as well as the digital world - as nodes in a directed graph. In this directed graph nodes that are physically or virtually connected are linked by directed edges. The nodes represent different elements in the modelled organisation such as locations, assets, and actors. Nodes may belong to different domains. Domains are used to restrict operations being allowed on the nodes. For example, human actors are only allowed to move within the nodes from the physical domain. Some nodes are associated with policies, which are used for regulating the access to locations and assets, but also for defining actors' expected behaviour in the organisation. Policies consist of two parts - required credentials and enabled actions. The actor needs to fulfill the required credentials in order to be permitted to perform the enabled actions on the respective node.

The example scenario, also shown in Figure 2, represents an actor Alice, who receives a care-taking service provided by an actor Charlie. The company Charlie works for has a policy that forbids the employees to take money from the customers. The locations modelled in this scenario are Alice's home, a bank with an ATM, and a bank computer. Alice's payment card, the pin it contains, and the pin Alice knows for her card are modeled as assets. An example for a node associated with a policy is the bank computer, where the policy requires a bank account and a matching password.

In order to identify the possible attacks based on the model, our approach does not analyse only the technical infrastructure but also takes into consideration the human factor. Social attacks, *e.g.*, social engineering, are an essential component as attack threats could be easily underseen when only technical attacks are considered. The human factor modelling in technical systems is also formally presented using Isabelle theorem prover [3].

### Analysis

Our analysis is carried out on attack trees, a suitable tool for presenting socio-technical threats and conveying security information to non-experts. Attack trees, introduced by Schneier [4], are a widely used graphical tool for representing attack scenarios. They are used to evaluate the security of complex systems in a structured, hierarchical way. The root of a tree represents the main goal of the attacker, while the leaves are the attacker's basic actions. Internal nodes illustrate how the basic actions have to be combined in order to achieve the overall goal. Standard attack trees combine basic actions either *conjunctively*, meaning that all actions should be satisfied in order the tree to be satisfied, or *disjunctively*, meaning that at least one action should be satisfied in order the tree to be satisfied.

Attack trees are analysed by assigning values to the basic actions and propagating them from the leaves to the root of the tree. Most attack tree analyses consider attack trees with one parameter and optimise one particular aspect of a scenario, such as likelihood of success *or* difficulty of a hack, in terms of time or cost of an attack. Moreover, in most attack tree models with multiple parameters values are propagating from the leaves to the root based on local decision strategies, i.e., in each step of the evaluation optimisation is made with respect

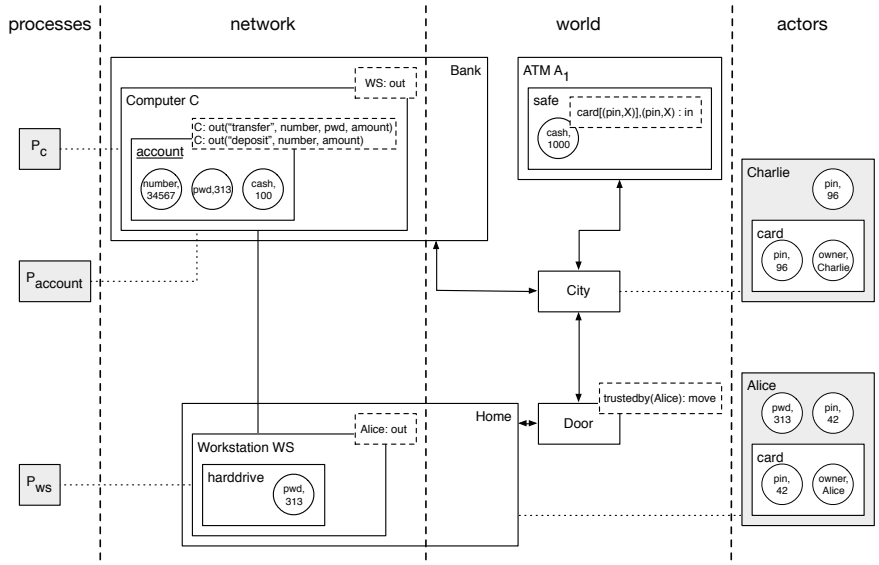


**Fig. 2.** Graphical representation of the example system. The white rectangles represent locations or items, the gray rectangles represent processes and actors; actors contain the items or data owned by the actor. The round nodes represent data. Solid lines represent the physical connections between locations, and dotted lines represent the present location of actors and processes. The dashed rectangles in the upper right part of some nodes represent the policies assigned to these nodes.

to one parameter. In case of incomparable values, however, this approach may yield sup-optimal results.

In order to overcome this limitation and evaluate complex attack scenarios, we present evaluation techniques that consider attack trees where basic actions are assigned with more than one parameter, such as, likelihood of success *and* cost. Our evaluation techniques try to optimise all parameters at once. However, optimisation of multiple parameters might lead to incomparable values, e.g., maximising likelihood *while* minimising cost. Even worse, a best solution does not always exist. We handle this issue by computing the set of optimal solutions [5], defined in terms of Pareto efficiency. A solution is called Pareto efficient if it is not dominated by any other solution [6].

## Evaluation

We illustrate the evaluation techniques on the attack scenario where an attacker wants to steal money from the card-holder by forcing him/her to pay fake services. Our evaluation techniques answer the questions, such as "Can an attacker successfully steal money from the card-holder?" or "What is the maximum likelihood of success of an attack?". Moreover, we associate with each basic action a

©Copyright held by the author(s)

cost of an attack, and detected the attacks with maximum likelihood *and* minimum cost. We compute the set of all Pareto optimal solutions, displayed in Figure 3, where each point shows a likelihood of success with the corresponding cost.

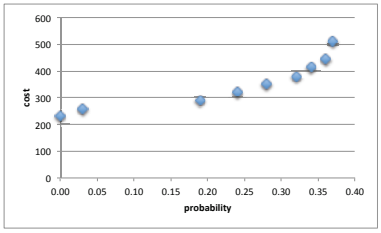


**Fig. 3.** Pareto optimal solutions.

As future work, we plan to introduce countermeasures to the model. Besides the identification of possible socio-technical threats, we would like to determine the corresponding defender actions and evaluate attack and defence scenarios.

***Acknowledgment:*** Part of the research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318003 (TREsPASS). This publication reflects only the authors' views and the Union is not liable for any use that may be made of the information contained herein.

## References

1. Probst, C.W., Hansen, R.R.: An extensible analysable system model. Information Security Technical Report **13**(4) (November 2008) 235–246
2. Dimkov, T., Pieters, W., Hartel, P.: Portunes: representing attack scenarios spanning through the physical, digital and social domain. In: Proceedings of the 2010 joint conference on Automated reasoning for security protocol analysis and issues in the theory of security, Springer (2010) 112–129
3. Boender, J., Ivanova, M.G., Kammüller, F., Primiero, G.: Modeling human behaviour with higher order logic: Insider threats. In: STAST'14, IEEE (2014) co-located with CSF'14 in the Vienna Summer of Logic.
4. Schneier, B.: Attack Trees: Modeling Security Threats. Dr. Dobb's Journal of Software Tools **24**(12) (1999) 21–29
5. Aslanyan, Z., Nielson, F.: Pareto efficient solutions of attack-defence trees. In: Principles of Security and Trust - 4th International Conference, POST. (2015) 95–114
6. Legriel, J., Guernic, C.L., Cotton, S., Maler, O.: Approximating the pareto front of multi-criteria optimization problems. In: TACAS. (2010) 69–83