Computers and Electrical Engineering 47 (2015) 258–274

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Security analysis of socio-technical physical systems ☆

Gabriele Lenzini [a], Sjouke Mauw [a,b], Samir Ouchani [a,*]

[a] Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg
[b] Faculty of Communication and Computer Science, University of Luxembourg, Luxembourg

ARTICLE INFO

Article history:
Received 2 October 2014
Received in revised form 27 February 2015
Accepted 27 February 2015
Available online 6 April 2015

Keywords:
Socio-technical systems
Security assessment
Probabilistic verification
Security model

ABSTRACT

Recent initiatives that evaluate the security of physical systems with objects as assets and people as agents – here called *socio-technical physical systems* – have limitations: their agent behavior is too simple, they just estimate feasibility and not the likelihood of attacks, or they do estimate likelihood but on explicitly provided attacks only. We propose a model that can detect and quantify attacks. It has a rich set of agent actions with associated probability and cost. We also propose a threat model, an intruder that can misbehave and that competes with honest agents. The intruder's actions have an associated cost and are constrained to be realistic. We map our model to a probabilistic symbolic model checker and we express templates of security properties in the Probabilistic Computation Tree Logic, thus supporting automatic analysis of security properties. A use case shows the effectiveness of our approach.

1. Introduction

Surely anyone raises an eyebrow when reading about simple yet canny social engineering attacks like the one first reported in [1] and recently recalled by Schneier in his blog [2]. Without having the key and without breaching the door, an intruder stole a confidential document from a supposed-to-be locked room. This was possible because someone executed what the intruder's note requested: 'please leave the door unlocked'. Actually, the full attack requires some preparatory steps: entering the building during office hours, surreptitiously sticking the message on the door, and re-entering the office space after everyone has left. But all these actions seem less critical than entering a locked door without holding the key. This attack is an example of an intrusion that exploits vulnerabilities in a physical space. It was also possible because it was tolerated that secret reports are left accessible inside the room, optimistically assuming that a locked door was a sufficient protection. This is clearly a deficiency at the level of security policies.

Organizations should be concerned about checking the security of their policies that protect their assets, and the mechanisms guarding the access to the offices should back-up the policies. But checking the effective security of a place is far from being simple. The elements of the game are people, objects which can be moved or stolen and locations that can be locked/unlocked under specific conditions. We call a system with such elements a *socio-technical physical system* (STPS). This term reminds Whitworth and Ahmad's Socio-Technical System [3], which they introduced to describe models about societal and psychological aspects in human computer interactions and problems like mistrust, unfairness and injustice. We consider out

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Joaquin Garcia-Alfaro.

* Corresponding author.
E-mail addresses: gabriele.lenzini@uni.lu (G. Lenzini), sjouke.mauw@uni.lu (S. Mauw), samir.ouchani@uni.lu (S. Ouchani).

http://dx.doi.org/10.1016/j.compeleceng.2015.02.019
0045-7906/

of scope any social-science perspective; still we are interesting in human interactions, and by adding "Physical" we intend to stress that the kind of interactions we look at are those with the physical environments.

We sustain that studying the security underneath STPSs, requires methodologies of analysis as reliable as those developed for the analysis of security protocols (e.g., see [4–6]). Apparent diversities between the two domains, the technical vs. the socio-technical, suggest that the socio-technical security analysis is trickier. Socio-technical systems are made not only of software processes, digital messages and communication channels, but also of people, of physical objects and localities, and of communications that may happen via non-conventional media, such as hand-to-hand, visual, and auditory channels. Despite the increasing interest in the subject, to understand whether formal techniques can help automate the security analysis of STPSs is still on-going research. There is scarcity of tools to figure out whether and how, at what cost and with what probability, an intruder can gain unauthorized access to resources.

Contributions. In this paper, we initiate to develop such an analysis tool. We propose a formalism to model basic elements of STPSs, namely locations, people, and objects. Our formalism contains a rich set of user actions, such as changing locations, manipulating and exchanging objects, locking and unlocking doors and containers. We let actions have a cost and agents act either non-deterministically or probabilistically; actions can be guarded by contextual conditions. We also propose a model of the intruder, as a particular agent able to act maliciously, but according to realistic abilities which it exerts constrainedly depending on physical spaces and costs.

For security analysis, we propose model checking [7,8] to ensure security in STPSs. We define a mapping from STPS models, expressed in the proposed formalism, to the input language of the probabilistic symbolic model checker PRISM [9]. We express security properties in the extended probabilistic computational tree logic (PCTL) [10] and, to overcome the downside of the user-unfriendliness of the logic in expressing natural language security statements, we propose templates for relevant security properties.

Outline. In Section 2 we review the related work. Section 3 describes the formalism that models STPSs and Section 4 details our approach towards security analysis. Experimental results are showed in Section 5. Finally, Section 6 concludes the paper and sketches the future directions.

2. Related work

In this section we survey the most recent initiatives that deal with modeling, formalizing, and analyzing security in STPSs.

Sommestad et al. [11] propose a tool for the analysis of vulnerabilities in computer systems of large organizations and enterprises. The tool, called Cyber-Security Modeling Language (CySeMoL), uses a probabilistic relational model and estimates the probability of success of known attacks which, by experience, are expected to happen. The tool inputs a meta-model of the system, with potential attacks and countermeasures, and estimated attack probabilities of single components. The tool is meant for risk analysis of cyber-security threats, but it is not meant to discover new attacks.

Gunnarsson [12], and Probst and Hansen [13,14] analyze the robustness of control policies ruling access to an organization's building and its IT network. The analysis highlights what credentials an actor needs in order to reach specific locations and to access specific data. It also shows what he could reach if he had specific credentials. Actors can move within the infrastructure and access the resources therein. The system is modeled in "acKlaim", a calculus of the Klaim family [15], and the analysis consists of a reachability check on locations and actions. This approach is further extended by Probst et al. [16] with, amongst others, capabilities and restrictions, allowing an analysis of static and dynamic properties of the system and of the behavior of actors. Dimkov, Pieters and Hartel [17] also present a dialect of acKlaim, called Portunes. They describe attacks across digital, physical and social security alignments. The attacks are generated by searching through actions and preconditions allowed in the organization. Portunes treats people as physical elements that can do physical actions and are assailable to physical attacks.

The models for the infrastructure and for the actors in [12–14,16,17] have been of inspiration for the model we propose in this paper. But differently, we introduce costs and probabilities. We assume that not all possible attacks are necessarily feasible: they in fact have costs of execution and probability of success, which are qualities that depend on factors such as time to move from one place to another, effort to act one way instead of another. Our analysis is thus quantitative, making our security properties more interesting because they are expressed in relation to costs and probabilities.

Algarni et al. [18] propose a social engineering schema to describe threats in social networks. The schema covers the environment, the attacker, the trick, and the victims. The environment includes privacy settings, friendship and connections, and the content of user profiles. The attacker has been characterised by its ability to understand the victim, and to develop and perform an attack plan. A trick has been identified by the quality of the attack plan and its suitability to the targeted. The victim user supports socio-psychological factors, personality types, demographics variables, and motivations and drives.

Doss and Tejay [19] conduct a study by observing a group of security analysts who detect insider attacks. The goal is to determine how security analysts can use current security detection tools such as log analysis tools and intrusion detection systems to detect insider attacks. This study was conducted based upon the situational research approach from Grounded Theory.[1] Following GT, four categories were created: security monitoring, threat assessment, insider evaluation and goal

[1] Grounded Theory (GT) is a systematic methodology in the social sciences involving the discovery of theory through the analysis of data.