Chapter 6
Application of Verification Techniques to Security: Model Checking Insider Attacks

Florian Kammüller
DTU Copenhagen, Denmark

Christian W. Probst
Middlesex University, UK

Franco Raimondi
Middlesex University, UK

ABSTRACT
In this chapter, the authors give a short overview of the state of the art of formal verification techniques to the engineering of safe and secure systems. The main focus is on the support of security of real-world systems with mechanized verification techniques, in particular model checking. Based on prior experience with safety analysis—in particular the TWIN elevator (ThyssenKrupp) case study—the current case study ventures into the rising field of social engineering attacks on security. This main focus and original contribution of this chapter considers the security analysis of an insider attack illustrating the benefits of model checking with belief logics and actor system modeling.

INTRODUCTION
The high density of our population today requires efficient use of any resources like energy and space. The use of IT system in all but few domains of everyday life is a reality we have all learned to accept. In this symbiotic new lifestyle, safety and security of technical systems are of utmost importance. Safety can be informally defined as the protection of humans and goods from malfunctioning of technical systems, for examples trains, airplanes, or nuclear reactors. Security on the other side can be understood as the protection of computer systems from malicious humans.
In order to guarantee safety and security, application of standards is today common practice. Safety standards are widely applicable and often already include explicit use of formal techniques, whereas for security the use of formal specification and verification is still beyond the reach of everyday industrial practice. The most widely accepted global security standard, the Common Criteria –CC (Bundesamt fuer Sicherheit in der Informationsgesellschaft BSI, 2005), demands in its highest levels, above and including EAL5, the use of formal techniques and even completely mechanized formal proofs of properties in EAL7. However, apart from big enterprises – Microsoft’s Windows 2003 has a CC-EAL4 accreditation – the application of CC is beyond the reach of everyday practice for small and medium size enterprises; reaching the highest levels seems even out of reach for large companies.

Systematic application of formal modeling for a mechanized verification is never independent from the nature of the system we investigate. System characteristics, like safety or security sensitivity, time dependent behavior, interaction patterns, and complexity issues of relevant control parts must be taken into account when deciding on the selection of a formalism for rigorous modeling and a method for automated analysis. This chapter makes a case for model checking (Clarke, Grumberg & Peled, 1999), of safety and security sensitive systems. Past experiments have shown that model checking is perfectly capable of proving safety-critical systems. For example, the elevator system Twin of ThyssenKrupp has been successfully modeled and all safety requirements have been verified using the SMV model checker [KP07]. This is particularly interesting as the Twin system operates two cabins in one elevator shaft; one driving above the other with collisions in principle possible as illustrated by the admissible routes in Figure 1.

The case study thus proves the capabilities of model checking in industrial scenarios. It is an example of a typical state-based, reactive system. Therefore, it is not very difficult to encode it in the standard model checker SMV (McMillan, 1992; McMillan, 1995), once the right abstraction of the system specification and the safety requirements is found.

More recently, research efforts started increasing to repeat the same success story in the domain of security. However, as has early on been recognized classical security properties, e.g. confidentiality, are fundamentally different properties from safety properties. Whereas a safety property can be expressed as a predicate over a single path composed of state transitions, confidentiality quantifies over a set of paths: intuitively, confidentiality of a system means that all observable

![Figure 1. Safe routes of upper (U) and lower (L) cabin are shaded (Kammüller, F. & Preibusch, S., 2007)](image)