Available online at www.sciencedirect.com

SCIENCE DIRECT®

Computer Standards & Interfaces 27 (2005) 457–466

COMPUTER STANDARDS & INTERFACES

www.elsevier.com/locate/csi

On a formal framework for security properties

Sigrid Gürgens*, Peter Ochsenschläger, Carsten Rudolph

Fraunhofer Institute for Secure Information Technology SIT Rheinstrasse 75, D-64295 Darmstadt, Germany

Available online 17 February 2005

Abstract

A new approach to property-based characterisation of security requirements is presented. The main goal is to provide a framework for the specification of a wide variety of security requirements with formal semantics in terms of security properties of a discrete model of a system. In contrast to previous approaches it is not focused on a special type of security property. The classical concept of "properties" comprising safety and liveness properties is extended to include security properties. Formalisations of authenticity, different types of non-repudiation and confidentiality are presented within the framework. Several examples illustrate the flexibility of this approach.

Keywords: Security requirements; Formal security models; Security properties

1. Introduction

Nowadays it is no longer necessary to accentuate the need for security in all types of computing systems. It is widely accepted that security issues are essential in particular for tele-cooperation systems, mobile communication systems or other types of distributed systems, and that security needs to be considered in all phases of the development cycle of such systems. This paper concentrates on the requirements specification phase of the development process. A wide variety of approaches to security requirement specification have been developed. Among these one can distinguish two main approaches. In the first, a security model is used to express either an abstract view of a particular desired (secure) behaviour of a system or to specify undesired behaviour. In the second approach, formally characterised security properties are used to specify security requirements. One classical approach of the first category is the multi-level security model by Bell and La Padula [2]. The Bell–La Padula model and other related security models, like the more recent work by McLean [11], define models for access control and therefore do not meet all kind of security requirements of complex distributed or tele-cooperating systems. The integrity model by Clark and Wilson [5] formulates restrictions on how data items might be altered. Other approaches are based on the specification of misuse cases describing threats by malicious agents or threat scenarios [9].

Concerning security properties, a large part of research work concentrates on information flow control and non-interference. The underlying trace based

* Corresponding author.
E-mail addresses: guergens@sit.fraunhofer.de (S. Gürgens).

0920-5489/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2005.01.004

system models for some of these notions [15,10] are closely related to the model presented in this paper. Non-interference and information flow properties can be used to describe various confidentiality properties. The underlying formal models are often highly complex and therefore accurate confidentiality requirements specification is error-prone and difficult. Another emphasis of research on security properties lies on authenticity and non-repudiation. Starting with the work on authentication logics [3], a wide variety of notions of authenticity has been published. Most of the formalisations are tailored for special cases like authentication protocol analysis while others provide more general definitions [13]. A wide variety of other fomalisations of security properties has been proposed, but there exists no framework in which different security requirements can be specified based on a single representation of a system.

In this paper we present a new approach to property-based characterisation of security requirements. In contrast to previous approaches it is not focused on a special type of security property. The main goal is to provide a framework for the specification of a wide variety of security requirements with formal semantics in terms of security properties of a single discrete model of the system. In addition to security requirements specification, property preserving abstractions by alphabetic language homomorphisms are used to transport the security properties from higher to lower levels of abstraction. We show that previously published formal definitions of authenticity and proof of authenticity [6b] and parameter confidentiality [6c] provide the foundation for the specification of many useful security properties.

The underlying formal model describes system behaviours as (sets of) traces of actions, where these actions are associated with agents in the systems. This type of specification is very common, but for security properties additional information is required. First, satisfaction of security properties depends on the agents' view of the system. In our framework, this view has to be specified for each system as an alphabetic language homomorphism on traces of actions. Agents' views are used in other approaches as well (e.g. by Wedel and Kessler for the semantics of the authentication logic AUTLOG [14], or by Heisel et al. [7], defining the window to a system). However, agents' views in our approach are more flexible, as will be demonstrated in Section 3. Second, for each agent the knowledge about the global system has to be part of the system specification. Obviously, satisfaction of confidentiality depends on the initial knowledge of the attacker. Furthermore, trust on underlying security mechanisms, such as cryptographic algorithms, are described as knowledge about the system. Although satisfaction of security properties depends on the particular knowledge of agents about the system, this is neglected in all existing system models for security properties.

Our framework was used for the design of secure e-commerce protocols in the project CASENET [4] funded by the European Commission.

In this paper, we first describe and explain our model framework based on formal languages. This framework is transparent with respect to any particular notion of system actions. Formal definitions for authenticity, proof of authenticity and parameter confidentiality have been previously proposed for such a framework [6b,6c]. We present a variety of possible instantiations in order to demonstrate the flexibility of the approach. Further, for every definition we determine the parameters necessary to accurately specify a particular security requirement. Examples illustrate that the formalisations are both accurate and understandable.

2. System behaviour specification and agents' knowledge about a system

The *behaviour* S of a discrete system can be formally described by the set of its possible sequences of actions (traces). Therefore $S \subseteq \Sigma^*$ holds where Σ is the set of all actions of the system, and Σ^* is the set of all finite sequences of elements of Σ, including the empty sequence denoted by ε. This terminology originates from the theory of formal languages, where Σ is called the alphabet, the elements of Σ are called letters, the elements of Σ^* are referred to as words and the subsets of Σ^* as formal languages. Words can be composed: If u and v are words, then uv is also a word. This operation is called the concatenation; especially $\varepsilon u = u\varepsilon = u$. A word u is called a prefix of a word v if there is a word x such that $v = ux$. The set of all prefixes of a word u is denoted by $\mathrm{pre}(u)$; $\varepsilon \in \mathrm{pre}(u)$