Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 112 (2017) 147–156

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Knowledge Based and Intelligent Information and Engineering Systems, KES2017, 6-8 September 2017, Marseille, France

Audit expert system of communication security assessment

Henryk Piech[a], Grzegorz Grodzki[b*]

[a] *Czestochowa University of Technology Dabrowskiego 73, 42201 Czestochowa, Poland*
[b] *Czestochowa University of Technology Dabrowskiego 73, 42201 Czestochowa, Poland*

Abstract

The main goal of the research consists in the elaboration of a system concerning the investigation of security communication, which regards a set of security factors, such as: the degree of encryption, the freshness of nonces, intruder activation, the lifetime of keys, secrets, etc. This paper is devoted to the presentation of systematization formalisms describing the functioning of a security model. In our variant, we investigate the changes of all chosen factors (security attributes) during the realization of protocol operations. The security attributes should be systematically corrected in this process. It changes the general security level of communication. The audit system strategy leads us to one of the most noticeable security in fluence characteristics that refer to time parameters. We can introduce the notation concerning the lifetime of elements (key, message, nonces, secret, etc.). When the value of time activity of an element exceeds its lifetime, then the communication security is definitely threatened. By using special rules presented in the works of Burrows, and Needham[2], among other authors, and by creating additional logic formulas, we can estimate intermediate security probability parameters. Finally, we propose a certain kind of probability time automata in order to investigate and predicate different types of communication threats. These automata are built on the basis of a colored Petri net. In addition, this investigation consists in checking communication security (or a kind of threats) and making a threat prediction about possible cases that are connected with losing information. We also included in the model a procedure of security modification with respect to time (the activity of some parameters depends on time). We define the finite set of states by using the LU - technique (interval attribute activity) of a date notation. The proposed system resolves security problem in more comprehensive (multifaceted) way. Ingredient security factors can be grouped in different combinations. This approach increased the range of investigated threaten structures to even unknown hacker algorithm inventions.

Peer-review under responsibility of KES International

Keywords: audit expert system, communication security, Petri nets, protocol security, auditing system, probability time automata;

1. Introduction

The cryptography protocol structures consist of operations that regard sending and receiving, and a simulation concerning the interception of open and encrypted information. There is also a different kind of investigation models.

* Corresponding author. Tel.: +48-34-3250-589; fax: +48-34-3250-589.
E-mail address: grzegorz.grodzki@icis.pcz.pl

1877-0509
Peer-review under responsibility of KES International
10.1016/j.procs.2017.08.188

They are based on time automata (TA), probability-timed automata (PTA), time Petri nets (TPN), colored Petri nets (CPN) [13] etc. The feature of these models is connected with the possibility of realization concerning transition state procedures [11,14]. The state may describe protocols, message, keys, users [5,7], etc., and their security aspects. The modeling based on automata and nets has an advantage that consists in the possibility of chronological state observation and checking transition constrains. In the case of security modeling, a disadvantage appears that is connected with the necessity regarding the lifetime pre-evaluation of timed attributes. It should be realized with the help of experiments that ultimately approve the realistic and useful values of lifetime parameters. The confirmation of experience results may take place as even the cases concerning message multi-encryption can be taken into account in a simple way [4]. The chronologic protocol operation sequences will be analyzed from the perspective of forthcoming threats. The proposed variants of security investigation preserve the general and detailed character of the multi-aspect security analysis. The method adapted to a concrete situation may be used in an intelligent system of dynamic data mining features [6]. The interesting part of the research refers to the calculation probabilities of state transition and the reachability of a given state or its set [8]. The semantic formalisms of communication security state is presented in other our work [12]. The system structure is built on the basis of selected models of communication state transition that are described in sections 2.1-2.3. Finally, we accomplish the main part of example results concerning the functioning of the expert system (section 3).

2. Artifact structure model of expert system functioning

Expert system is built on the basis of probability timed automata (PTA) or the colored Petri net (CPN) that is converted to them. The communication security states are described by communication cryptography parameters and with the help of logic rules (presented in BAN, PCL or Horae communication logics [2]. We propose to use the convention of homomorphic mapping probabilities with respect to the state description in the artifact set of binary tokens of security estimation. The inferring mechanism leads us to the assessment of communication threats and provides the sets of information about different global factors regarding security, like: selected protocols, keys, messages, nonces, secrets, etc., which are preliminary defined by users.

2.1. Fundamental predicates of communication BAN logic used for the description of knowledge distribution in the network

Formalisms describing protocol authentication contain information about:

- elementary protocol operations regarding messages, users, and keys,
- protocol modeling rules,
- assertions about authentication, i.e. the confirmation of believing in user honesty and jurisdiction over messages.

The motivation for the communication situation analysis, which is described by formalisms, consists in the need for the verification of the security situation that is presented in the form of honesty and jurisdiction states after every operation and correction. For example, this can be connected with checking attributes with respect to the shared key, secret, freshness of information, honesty of a sender and receiver. The standard form of formalism contains many security aspects, but apart from the unambiguity of their logic characters it is not possible to determinate the level of security attributes. Forms expressing believing and assertion rather suggested the usage of probability parameters and correction coefficients. The simplest, atomic communication logic elements contain quantifiers and complementary operators [2]:

$A \leftrightarrow^{K} B$ - users A, B communicate via the shared key K,
$\rightarrow^{K} A$ - user A has K as its public key,
$A \Leftrightarrow^{Y} B$ - users A and B share Y as a secret,
$\{X\}_K$ - the message X is encrypted by key K,
$\{X\}_K{}^A$ - the message X is encrypted by key K by user A,
$< X >_Y$ - the message X with an attached secret Y,
$A| \equiv X$ - user A believes the message X,
$A \triangleright X$ - user A sees the message X,
$A \triangleleft X$ - user A sends the message X once,