available at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Probabilistic model checking for the quantification of DoS security threats

Stylianos Basagiannis, Panagiotis Katsaros, Andrew Pombortsis, Nikolaos Alexiou*

Department of Informatics, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece

ARTICLE INFO

Article history:
Received 3 March 2008
Received in revised form
6 September 2008
Accepted 7 January 2009

Keywords:
Denial of service
Secure authentication
Probabilistic model checking
Resource exhaustion
Attacker model

ABSTRACT

Secure authentication features of communication and electronic commerce protocols involve computationally expensive and memory intensive cryptographic operations that have the potential to be turned into denial-of-service (DoS) exploits. Recent proposals attempt to improve *DoS resistance* by implementing a trade-off between the resources required for the potential victim(s) with the resources used by a prospective attacker. Such improvements have been proposed for the Internet Key Exchange (IKE), the Just Fast Keying (JFK) key agreement protocol and the Secure Sockets Layer (SSL/TLS) protocol. In present article, we introduce probabilistic model checking as an efficient tool-assisted approach for *systematically quantifying DoS security threats*. We model a security protocol with a fixed network topology using probabilistic specifications for the protocol participants. We attach into the protocol model, a probabilistic attacker model which performs DoS related actions with assigned cost values. The costs for the protocol participants and the attacker reflect the level of some resource expenditure (memory, processing capacity or communication bandwidth) for the associated actions. From the developed model we obtain a Discrete Time Markov Chain (DTMC) via property preserving discrete-time semantics. The DTMC model is verified using the PRISM model checker that produces probabilistic estimates for the analyzed DoS threat. In this way, it is possible to evaluate the level of resource expenditure for the attacker, beyond which the likelihood of widespread attack is reduced and subsequently to compare alternative design considerations for optimal resistance to the analyzed DoS threat. Our approach is validated through the analysis of the Host Identity Protocol (HIP). The HIP base-exchange is seen as a cryptographic key-exchange protocol with special features related to DoS protection. We analyze a serious DoS threat, for which we provide probabilistic estimates, as well as results for the associated attacker and participants' costs.

1. Introduction

Formal techniques for verifying the absence of secrecy and authentication failures in cryptographic protocols have been effective in discovering design flaws that allow a malicious intruder to subvert a protocol's guarantees. All these approaches adopt the basic assumptions of a general intruder model introduced by Dolev and Yao (1983). These assumptions are: (i) The encryption method used is unbreakable; (ii) The intruder can prevent any message from reaching its

* *Corresponding author*. Tel.: +30 2310 998532; fax: +30 2310 998419.
E-mail addresses: basags@csd.auth.gr (S. Basagiannis), katsaros@csd.auth.gr (P. Katsaros), apombo@csd.auth.gr (A. Pombortsis), nalexiou@csd.auth.gr (N. Alexiou).
0167-4048/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2009.01.002

destination and (iii) The intruder can create messages of his own. However, an attacker with the mentioned abilities can also subvert the *availability* of the protocol participants and in the related bibliography there are only a few recent works that address the quantitative analysis of availability threats and the alternative countermeasures.

Our proposal introduces a probabilistic attacker model with assigned cost values that reflect the level of some resource expenditure (memory, processing capacity or bandwidth) for his actions. The model combines *attack tactics* selected from the formalized open-ended intruder model introduced by us in 2007 (Basagiannis et al., 2007). The analyzed DoS threat is expressed as a *probabilistic reachability property* that is automatically verified (according to Kwiatkowska et al. (2007) and Kwiatkowska (2007)) with respect to an appropriate Discrete Time Markov Chain (DTMC) representing the protocol participants and attacker models. The overall analysis takes place in a probabilistic model checking toolset called PRISM (PRISM, 2008). This improves the usability of the analysis by the protocol designers and automates the generation of sensitivity results. It is thus possible to compare implementations with alternative parameter choices, for optimal resistance to the analyzed threat.

Our approach is described in terms of the performed analysis for the Host Identity Protocol (HIP) base-exchange. HIP aims to provide a ''secure'' multiaddressing mechanism that separates the two conflicting roles of host identifiers and network locations that IP addresses play in current Internet. The assigned costs quantifying the protocol's processing workload are based on related HIP performance studies (InfraHIP project, 2007). We realized that an attacker model embedding three basic attack tactics that successfully represent the combined effects of *N zombie participants* breaks the utilized DoS resistance mechanism. Appropriate queries expressed in Probabilistic Computation Tree Logic (PCTL) provide illuminating probabilistic estimates together with the attacker and victim's costs for the analyzed DoS threat. Our analysis concludes with a sensitivity study of the obtained estimates with respect to the used model parameters.

In Section 2 we review the few works found in related bibliography, in order to point out the differences with the proposed analysis approach. Section 3 provides a brief introduction to probabilistic model checking and defines the *DoS resistance property*, in terms of an appropriate probabilistic attacker model. Section 4 presents the PRISM model for the HIP base-exchange and comments on the results of the performed PCTL queries. We conclude with a summary of the overall analysis approach and a comment on its usability and its potential impact.

2. Related work

Design of protocols that manage the available resources effectively in the presence of DoS attacks is a complex task. Interesting techniques that reduce memory storage and processing costs for the responder in a protocol session have been introduced in the works of Aura and Nikander (1997) and Castelluccia et al. (2008). The *client puzzles* that were first proposed by Aura et al. (2001) introduce time consuming and verifiable proofs of work that artificially increase the computational workload of initiators in protocol sessions. This strategy aims to assure that initiators have expended a predetermined level of computational effort prior to a responder committing resources, but as we will see in the case of the HIP base-exchange it has the potential to introduce new DoS exploits. Other techniques like the *cookies* (Karn and Simpson, 1999) are used to weakly assure the origin of requests, before applying stronger cryptographic operations that implement the protocol's service. However, a gradually strengthening authentication can be successful only when its design is based on a careful analysis of the server resource usage.

The importance of enabling availability analysis for a given cryptographic protocol was first shown by Meadows (2001). In that work the author examines DoS in the context of the resource intensive task of authentication and develops a framework for weighting the cost to the defender against the cost to the attacker. The paper concludes with descriptions of potential integration scenarios of the proposed framework into the automated security analysis tools that were available at that time. In Smith et al. (2006) the authors exploit Meadows's framework to analyze the Just Fast Keying (JFK) protocol (Aiello et al., 2002), in order to demonstrate its DoS prevention capabilities. Recently, the approach of Meadows (2001) formed the basis for the analysis framework of Tritilanunt et al. (2006) that according to the authors provides a more accurate representation of computational cost. However, quantitative evaluation takes place by simulation of the developed Timed Colored Petri Net model, without having exploited the formal analysis capabilities of the used toolset.

An interesting stochastic modeling approach for quantifying the availability of software systems under DoS threats is the one introduced by Madan et al. (2002). In that work, the authors formulate the analyzed system in terms of an appropriate semi-Markov process (SMP). Starting with the SMP model it is then possible to derive the embedded DTMC that involves only the considered state transition probabilities. After having computed the steady-state DTMC probabilities, the assumed sojourn time distributions for the model's states are used to compute the SMP's steady-state probabilities. This makes possible to calculate the system's availability and subsequently perform parametric sensitivity analysis in order to examine the sensitivity of the computed availability. The overall approach requires stochastic modeling and analysis skills, since it is not carried out within an automated analysis tool like PRISM. Furthermore, the performed system-level analysis does not take into account the resource expenditure for the considered states and thus it is not possible to evaluate the message processing costs for DoS threats upon a security protocol model.

The most closely related work found in the bibliography is the one published in Agha et al. (2005). In that work, the authors specify in *probabilistic rewriting logic* a DoS resistant 3-way handshaking in the Transmission Control Protocol (TCP). Similarly to our approach, the developed specification includes a number of honest participants and a simple attacker, flooding the protocol model with spurious requests at a specific rate (parameter of an exponential distribution). In the VESTA toolset (Sen et al., 2005a), the developed algebraic specification generates a timed probabilistic model, which is