# Chapter 21
# Denial of Service Resilience of Authentication Systems

**Valer Bocan**
*Alcatel-Lucent, Romania*

**Mihai Fagadar-Cosma**
*Alcatel-Lucent, Romania*

## ABSTRACT

*Cryptographic authentication systems are currently the de facto standard for securing clients access to network services. Although they offer enhanced security for the parties involved in the communication process, they still have a vulnerable point represented by their susceptibility to denial of service (DoS) attacks. The present chapter addresses two important aspects related to the security of authentication systems and their resistance against strong DoS attacks, represented by attack detection and attack prevention. In this respect, we present a detailed analysis of the methods used to evaluate the attack state of an authentication system as well as of the countermeasures that can be deployed to prevent or repel a DoS attack.*

## INTRODUCTION

Denial of service attacks on authentication systems can take two possible forms. On one hand, an attacker can prevent the network from sending the messages that it should normally transmit to its clients. On the other hand, it could force the network into sending messages it should not normally transmit. By far, the most popular DoS attack is server flooding that prevents legitimate clients from obtaining the services they request from that server.

DOI: 10.4018/978-1-4666-2919-6.ch021

One cause for the vulnerability to DoS in authentication systems is that the dialog between peers takes place before even a minimum pre-authentication is performed, which renders the server incapable of distinguishing legitimate from malicious traffic. Enforcing the authentication of all requests would represent a DoS attack by itself, since the server would be busy checking all digital signatures, no matter if these are valid or not. Such a method would be as dangerous as a TCP stack overflow is in case of TCP SYN attacks.

Another vulnerability is the lack of resource accounting. In this respect Spatscheck and Peterson (1999) consider that there are 3 key ingredients

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

for protecting against DoS attacks: accounting all resources allocated to a client, detecting the moment when these resources rise above a predefined threshold and constraining the allocated resources by reducing them to a minimum level in case an attack has been detected and recovering the blocked resources.

The third vulnerability resides in the intrinsic design of the communication protocols, as described by Crosby and Wallach (2003). A new class of low-bandwidth attacks exploits the deficiencies of data structures employed in various applications. For example, hash tables and binary trees can degenerate into simple linked lists when input data is selected accordingly. Using the typical bandwidth of a dial-up modem, the authors have managed to bring a Bro server on the edge of collapsing: 6 minutes after the attack has begun, the server was ignoring 71% of traffic and was consuming its entire computational power.

Taking in consideration the global market tendency towards on-line availability, DoS attacks prove to be more dangerous than initially predicted therefore identifying them as soon as they take place is a decisive aspect. From the moment the attack has begun until it is detected and countermeasures are deployed, the targeted servers are blocked and all legitimate requests are ignored, which can result in significant financial losses. Chained attacks can occur if the communication protocol continues its dialogue with the attacker even after anomalies have been detected. The basic idea behind the so called fail-safe or fail-stop protocols is for the message-exchange to be discontinued with any client that does not follow the normal course of the protocol.

Considering the attack forms and characteristics described above, a resilient authentication system must fulfill two main requirements. First, the system must be able to detect an incoming attack as soon as possible in order to be able to respond accordingly and prevent any possible losses. Second, the system must be able to defend itself against an ongoing attack, either through its intrinsic characteristics or by deploying a set of countermeasures against the attacker. Given these requirements, we have structured this chapter into two main parts. In the first part we address the strategy and the techniques that enable an authentication system to efficiently detect DoS attacks, and their implementation into a detection engine called SSO-SENSE. In the second part we focus on the threshold puzzles concept as an a efficient way to protect against DoS attacks and analyze the case study of the SSL Handshake algorithm from both an implementation and a performance perspective.

## BACKGROUND

### The Client Puzzles Concept

An efficient measure for preventing DoS attacks during the authentication phase would be to ensure that the client allocates its resources proportionally with the resources allocated by the server. As a result, at any time during the execution of the authentication protocol, the computational cost for the client will be higher than that of the server. This can be achieved by asking the client to solve a puzzle with a difficulty established by the server. The solution to the client puzzle should be easily accessible to the server, in order to obtain a low resource usage, while the client should be forced to allocate computational resources into solving the puzzle according to the complexity requested by the server.

Merkle (1978) was the first to come up with the idea of using cryptographic puzzles, but he applied the concept only for key exchange and not for the authentication itself. Later, the client puzzles concept has been successfully applied against TCP SYN attacks by Juels and Brainard (1999), who also outline the vulnerability of SSL protocols against DoS attacks and provide a rigorous demonstration of their security characteristics. Aura, Nikander and Leiwo (2000) have applied

18 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/denial-service-resilience-authentication-systems/75042

## Related Content

The Implications of Alireza Noruzi's Laws of the Web for Library Web-Based Services
Josephine Eruterio Onohwakporand Benson Oghenevwogaga Adogbeji (2011). *Handbook of Research on Information Communication Technology Policy: Trends, Issues and Advancements (pp. 724-733).*
www.irma-international.org/chapter/implications-alireza-noruzi-laws-web/45420

Towards an Enhanced Interoperability Service Utility: An Ontology Supported Approach
Irene Matzakou, João Sarraipa, Ourania I. Markaki, Kostas Ergazakisand Dimitris Askounis (2015). *Standards and Standardization: Concepts, Methodologies, Tools, and Applications (pp. 1605-1632).*
www.irma-international.org/chapter/towards-an-enhanced-interoperability-service-utility/125360

Standardization of Information Technologies in Fundamental Research in Russia
Yuri Gulyaev, Alexander Oleinikovand Eugene Zhuravliov (2009). *International Journal of IT Standards and Standardization Research (pp. 64-81).*
www.irma-international.org/article/standardization-information-technologies-fundamental-research/4049

Selected Barriers to Online International Trade Within the EU: Could Standards and Common Rules Help?
Marta Orviskaand Jan Hunady (2017). *International Journal of Standardization Research (pp. 76-93).*
www.irma-international.org/article/selected-barriers-to-online-international-trade-within-the-eu/202989

Standardization in Enterprise Inter- and Intraorganizational Integration
K. Kosanke (2005). *International Journal of IT Standards and Standardization Research (pp. 42-50).*
www.irma-international.org/article/standardization-enterprise-inter-intraorganizational-integration/2567