Servers Configuration and Testing for Secure Exchange of Information over the Internet

Gabriel PETRICĂ
EUROQUALROM, University POLITEHNICA of Bucharest, Romania
gabriel.petrica@upb.ro

Abstract

A digital certificate is a mechanism that provides authentication (for example, in e-mail communications), ensures data integrity (for Microsoft Office or PDF documents), and secures communications transmitted on insecure computer networks such as the Internet. Using a SSL digital certificate is considered to be a mandatory requirement in all security guidelines relating to electronic commerce, but also for websites that store confidential information or perform various financial transactions. This paper highlights the importance of the SSL digital certificate to identify a legitimate Web server and presents the steps for creating a self-signed SSL digital certificate using the openssl command.

Index terms: digital certificate, SSL, digital signature, openssl, browser security

References:

[1]. Ioan-Cosmin Mihai, Gabriel Petrică, Costel Ciuchi, and Laurenţiu Giurea, Provocări şi strategii de securitate cibernetică, Editura Sitech, Craiova, 2015, ISBN 978-606-11-4951-3.

[2]. Peter Gutmann, Engineering Security, April 2014, available online https://www.cs.auckland.ac.nz/~pgut001/pubs/book.pdf

[3]. OpenSSL Cryptography and SSL/TLS Toolkit, https://www.openssl.org/

[4]. Secure Website Certificate, https://support.mozilla.org/en-US/kb/secure-website-certificate, accessed 12 August 2016.

[5]. Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition, Wiley, 2008, ISBN: 978-0-470-06852-6.

[6]. Public Key Infrastructure, https://en.wikipedia.org/wiki/Public_key_infrastructure, accessed 15 July 2016.

[7]. Let's Encrypt: Delivering SSL/TLS Everywhere, https://letsencrypt.org/2014/11/18/announcing-lets-encrypt.html, accessed 10 September 2016.

[8]. NMAP Reference Guide, https://nmap.org/book/man.html, accessed 1 September 2016.