SEC-CMAC A New Message Authentication Code Based on the Symmetrical Evolutionist Ciphering Algorithm

Bouchra Echandouri, Faculty of Sciences, Mohammed V University, Rabat, Morocco
Fouzia Omary, Faculty of Sciences, Mohammed V University, Rabat, Morocco
Fatima Ezzahra Ziani, Faculty of Sciences, Mohammed V University, Rabat, Morocco
Anas Sadak, Faculty of Sciences, Mohammed V University, Rabat, Morocco

ABSTRACT

This article describes how the simplicity of data transmission made eavesdropping by malicious people easier. This became one the flaws of computer security that needs to be handled. In order to establish a secure data communication, many data security techniques were developed to ensure privacy, integrity and authenticity. One of the techniques developed was to fulfill authentication with a message authentication code (MAC) that was defined by the National Institute of Standards and Technology. It is still a powerful data integrity and authentication tool that provides better protection than error detection codes or checksums. In this article, the authors propose a new cipher-based message authentication code (CMAC) algorithm. Their proposed algorithm, termed SEC-CMAC, is based on a previously developed symmetric evolutionist ciphering algorithm named symmetrical evolutionist ciphering (SEC). Compared to the well-known previously developed MAC, their suggested algorithm proved to be robust and fulfill some security requirement by resisting an exhaustive key search and mac forgery attacks.

KEYWORDS

Authentication, Cipher Based Message Authentication Code (CMAC), Cryptography, Integrity, Message Authentication Code (MAC), Symmetrical Evolutionist Ciphering (SEC)

INTRODUCTION

Computer networks allowed us to communicate in new ways. They erased physical borders and made the world more interconnected. However, transmitting data over insecure and arbitrary channels (Książak, 2014), makes it subject to interception by malicious entities (Kumari, 2017; Li, 2017a, 2017b, 2017c).

It became necessary to develop tools to establish trustworthy network communications and reliable connection management processes to establish digital identity. This way, the sender and the receiver entities can communicate their private data in a secure fashion (Kumari, 2017; Li, 2017a, 2017b).

In addition, the authenticity of data should be ensured during the transmission, the processing and the storage, so that malicious users or intruders cannot intercept or alter them (Książak, 2014).

Cryptography, the science of encrypting and decrypting messages, can help secure the transmission of data by guaranteeing data authenticity and protecting privacy. One cryptography concept that works toward ensuring both data authenticity and privacy protection is Message Authentication Code (MAC). It was defined by the National Institute of Standards and Technology

DOI: 10.4018/IJISP.2018070102

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
(NIST). In general, a MAC function generates a digit from the plaintext and a secret key. The digit, sent along with the plaintext, is called a tag (see Figure 1). In practice, the MAC functions proved to be hard to break due to their good resistance to forgery (as it is hard to have two messages with the same valid tag) (Bellare, 1996).

There exist two broad families of MAC functions: MAC functions based on cryptographic hash functions or MAC functions based on a cipher. The hash-based MAC functions (or HMAC) use a hash function and a secret key to generate a MAC and are mainly used in network protocols such as SSH, IPsec or TLS (Dang, 2008). The cipher-based MAC functions (or CMAC) use a symmetric key cipher algorithm to generate a MAC (Dworkin, 2005). Their wide use can be explained by their ability to optimize the size of the code. When using a symmetric cipher algorithm, some of the modes used to produce MACs are the Offset Code Book mode (OCB) (Rogaway, 2003), the Cipher Block Chaining mode (CBC-MAC) (Frankel, 2003) and the Cipher-Based mode (CMAC) (Dworkin, 2005). The CBC-MAC mode is no more recommended since it is secure only for fixed-length messages. CMAC is the mode recommended by the NIST and is the secure successor of the CBC-MAC. It guarantees that the MAC generated is as secure as the cipher algorithm upon which it is constructed (Bernstein, 2005).

The main purpose of our work is to design a MAC function using the Symmetrical Evolutionist Ciphering (SEC) algorithm. SEC is one of the first symmetrical encryption algorithms integrating an evolutionary algorithm. Its strength lies in its ability to change plaintext’s characters appearance frequency and positions (Omary, 2006).

The rest of this paper is organized as follows: in Section 2, a highlight of some related work in the literature is described in brief. Then in Section 3, the necessary background on cipher-based MACs and the SEC algorithm is presented. In Section 4, the proposed solution (SEC-CMAC) is detailed. Its analysis and its performance evaluation follow in Section 5.

RELATED WORK

The issues related to authentication in network communications have led to the development of a set of tools and some improvements. One of the most efficient solutions that addresses those issues

Figure 1. General MAC generation

\[ \text{Data Sent} \]

\[ \text{Message M} \quad \text{Tag T} \]

\[ \text{MAC Function} \]

\[ K \]
Related Content

What and Where are the Risks of International Terrorist Attacks: A Descriptive Study of the Evidence
[www.igi-global.com/article/what-and-where-are-the-risks-of-international-terrorist-attacks/127538?camid=4v1a](www.igi-global.com/article/what-and-where-are-the-risks-of-international-terrorist-attacks/127538?camid=4v1a)

A Keystroke Biometric System for Long-Text Input
[www.igi-global.com/article/keystroke-biometric-system-for-long-text/43056?camid=4v1a](www.igi-global.com/article/keystroke-biometric-system-for-long-text/43056?camid=4v1a)
Certification and Security Issues in Biomedical Grid Portals: The GRISSOM Case Study
www.igi-global.com/chapter/certification-security-issues-biomedical-grid/46882?camid=4v1a

Performance and Scalability Assessment for Non-Certificate-Based Public Key Management in VANETs
www.igi-global.com/article/performance-scalability-assessment-non-certificate/64345?camid=4v1a