Acta Scientific COMPUTER SCIENCES

Volume 4 Issue 7 July 2022

Short Communication

Cyber Security Term Series - Nonce

Mario Barnard*

Department of Electrical and Computer Engineering, Oakland University, Rochester, MI, USA

***Corresponding Author:** Mario Barnard, Department of Electrical and Computer Engineering, Oakland University, Rochester, MI, USA.

Received: June 03, 2022

Published: June 16, 2022

Keywords: Computer Security; Cyber Security; Network Security; Automotive Security; Automotive Cyber Security; Nonce

Nonce overview

A Cryptographic Nonce or nonce as defined by the National Institute of Standards and Technology (NIST) is "a time-varying value that has at most a negligible chance of repeating, for example, a random value that is generated anew for each use, a timestamp, a sequence number, or some combination of these" [1].

Other definitions according to NIST are as follows. A randomly generated value can be used to defeat playback types of attacks in communication protocols. The sender or first party can randomly generate a nonce and then send it to a receiver or second party. The receiver or second party can in turn encrypt the nonce via an agreed upon secret encryption key. Then, the receiver or second party returns it to the sender or first party [1].

Since the introduction of automotive cyber security and automotive security, nonces are being used in this type of industry as well in terms of security of vehicles modules and components. The National Institute of Standards and Technology (NIST) discourages the reuse of nonces. Nonces can be used to prevent replay attacks in private communications [2].

An example of a nonce is shown in figure 1.

In conclusion, nonces are another method used to protect against malicious attacks. Nonces are not only used in computer and networking cyber security, but also has been gaining interest in the automotive industry to protect consumers information especially pertaining to the area of electric vehicles (EVs). This is just one of many ways that cyber security professionals are mapping techniques that are implemented in computer cyber security and applying that knowledge and lesson learned to protect these electrified vehicles.

Nonce example

Figure 1: Nonce Example.

Client

A client is a computer on the network that requests network services [3].

Server

A server is a computer that provides a dedicated file, print, messaging application, or other services to the client computers [3].

getNonce()

This is the command in order to obtain the nonce that was used.

Nonce

A nonce is a security protocol value that is not ever repeated with the same encryption key. A counter, timestamp, or a message number can be used as a nonce [6].

Login

The login information consists of the user_name, cnonce, and hash. The hash consists of a nonce, cnonce, and password. The user_name can be either the user's email, a user created user name, or a company defined user name. A cnonce is a client nonce where the "c" denotes client. The cnonce aids in the security improvement as implemented in digest access authentication. Digest Access Authentication (DAA) is a method which a web server can use to negotiate the user's login credentials, such as the username/ password, to confirm the user's identify before sending sensitive information. A hash, according to NIST, "is a function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: it is computationally infeasible to find for a given output an input which maps to this output; and it is computationally infeasible to find for a given input a second input which maps to the same output" [4].

Token

A token in networking is a specific series of bits that flows around a token-ring network," according to Webopedia. Computers connected to the network can grab the token as it circulates. The token works in the same way as a ticket, allowing its owner to transmit a message across the network. Because each network has only one token, there is no way for two computers to send messages at the same time [5].

Bibliography

1. National Institute of Standards and Technology (NIST) Information Technology Laboratory Computer Security Resource Center (CSRC). "Nonce" (2022).
2. HYPR Security Encyclopedia. "Digest Access Authentication". (2022).
3. Lisa Donald, MCSA/MCSE .NET JumpStart, First Edition, Sybex, January 2 (2003).
4. National Institute of Standards and Technology (NIST) Information Technology Laboratory Computer Security Resource Center (CSRC). "Hash". (2022).
5. Webopedia. "Token". (2022).
6. William Stallings. "Crytography and Network Security: Principles and Practice". Seventh Edition, Pearson Education, Inc., (2017).