From:h draft-ietf-iesg-tftp-00
Network Working Group
Request for Comments: 9138
Updates: 1350
Category: Standards Track

Proposed Standard
F. Bocca
UACH
October 2021

TFTP+ AES Encryption Extension

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

The Trivial File Transfer Protocol [1] is a simple, lock-step, file transfer protocol which allows a client to get or put a file onto a remote host. This document describes a simple extension to TFTP to allow AES encryption to the file transfer increasing security.

Introduction

The AES encryption mechanism proposed in this document is a light modification to the TFTP protocol, It allows file transfer but with encrypted data packages using symmetric encryption, generating an AES key in the client and host side using the same keyword and initialization vector to obtain an identical key to encrypt and decrypt the file transferred.

Acknowledgements

The protocol was originally designed by Noel Chiappa, and was redesigned by him, Bob Baldwin and Dave Clark, with comments from Steve Szymanski and then improved by the MIT in 1992 . This actual modification was requested by Christian Lazo, professor of the UACH to his students of the Networks Course, who requested an improvement in the security of the protocol, being the author of this document the person who managed to increase the security in the protocol inspired by the popular instant messaging providers.

Security Issues

One current problem of this protocol is that all data is sent in clear text, that means if someone intercept the communication between client and host, it would be able to see all the information without any problem to decrypt it. In order to avoid this exploit, encryption of data is a must.

Encryption Protocol Specification

Once the WRQ has been acknowledged, the file to be transfer follows its normal course, being divided into 512-byte chunks, but before being added to a data packet, the chunks should be encrypted, but for that, his length must be a 16 byte multiple (because of how AES algorithm works), so the length of the packet is checked first, and if the packet length is not multiple of 16 bytes, it has to be padded, and only then the chunk can be encrypted and added to the packet. Chunks are always 512 bytes long (a 16 bytes multiple), so padding is almost always required for the last chunk only. The encryption uses the port chosen for the transfer as an integer variable with the TID provided by the udp protocol for the initialization vector and key respectively, once the data packet is encrypted is sended to the client by the host.

On the client side, if the data packet arrives without any issues, the decryption process begins, being followed by a de-padding process as well. Then the ack packet is sended to the host as usual.

For the RRQ operation the process is the same, only this time, the encryption process starts on the client side and the decryption process happens on the host side.

The key generated is created per file only once a port for communication is chosen.

References

[1] Sollins, K., "The TFTP Protocol (Revision 2)", STD 33, RFC 1350, October 1992.

Security Considerations

In this document a security layer has been added to the TFTP protocol, however login or access control mechanisms are still missing in this protocol, care must be taken in the rights granted to a TFTP server process so as not to violate the security of the server hosts file system. With that in mind TFTP should be installed with controls such that only files that have public read access are available via TFTP and writing files via TFTP is disallowed.

Author's Address

Franco Bocca Epple
Universidad Austral de Chile
Instituto de Ingeniería Civil en Informática
General Lagos 2086, Edificio 10000
Valdivia, XIV Región, Chile

Phone: (+56) 632-221439

EMail: FRANCO.BOCCA@ALUMNOS.UACH.CL