Project 1 Report

Junwei YANG (470167205)1, Chenhao HUANG (450524013)2

{1jyan5990, 2chua5342}@uni.sydney.edu.au

# Introduction

In this project, we implement a botnet system which enable bots to communicate with each other securely. Before two bots communicate with each other, they first agree on a key using Diffie-Hellman Key Exchange method. The messages are encrypted using Advanced Encryption Standard (AES) with Cipher Feedback (CFB) mode. HMAC with a one-time token is also used to ensure the integrity of the message and prevent the replay attack.

The report is organized as follows. Section 2 introduces the Diffie-Hellman Key Exchange including parameter choice. Section 3 records message encryption and modes of operation. Message integrity mechanism and the replay attack prevention methods are documented in Section 4. Section 5 provides some discussions.

# Diffie-Hellman Key Exchange

To defend from eavesdropper when the bots in the botnet are communicating with each other, we use symmetric encryption of the messages. Concretely, whenever two bots would like to transfer messages to each other, they will use Diffie-Hellman Key Agreement [[1](#_ENREF_1)] method to share their keys.

In the implementation of DH key exchange, the 2048-bit group is selected [[2](#_ENREF_2)]. The generator is 2. The choice of the key length is the trade-off between security and computational cost. Since the codes will be run on unknown computers, we hope our code to be secure. On the other hand, we also want our program to be fast. As a result, we choose the 2048-bit group.

# Confidentiality

In order to guarantee that the communication between bots remain confidential, we use cipher to encrypt our message. Concretely, the state-of-the-art Advanced Encryption Standard (AES) [[3](#_ENREF_3)] with Cipher Feedback (CFB)[[4](#_ENREF_4)].

The Advanced Encryption Standard (AES) is the substitution of Data Encryption Standard (DES) established by the U.S. National Institute of Standards and Technology (NIST) in 2001. The cipher AES is used here, as it overcomes the security vulnerabilities in DES. Using AES in our botnet can guarantee that it would be difficult for others to understand the communication between bots.

Cipher Feedback (CFB) mode is used here to split the messages of arbitrary length into blocks and then encrypt them using AES. In CFB mode, we first calculate a randomized Initialization Vector (IV). The hash value of the shared key between two communicating bots will be used as seed of the PRNG. The plaintext is first split into blocks, and each block is XOR’ed with the combination of previous ciphertext and the key, except for the first piece of the message, which is XOR’ed with the combination of key and the Initialization Vector (IV). (See Figure 1)

Cipher Feedback mode is selected because of high security level, parallelizable during decryption, and supporting random read access.

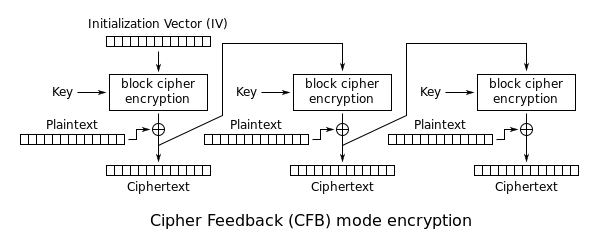


Figure 1 Cipher Feedback (CFB) mode (from [[4](#_ENREF_4)])

# Integrity and Replay Attack Prevention

To prevent attackers from tampering with messages in transit, a HMAC is attached each time with the message. SHA-256 is used here, as the already known security breach in SHA-1.

To prevent replay attack, we randomly generate a one-time session token, and then update the HMAC with this token. In this case, the eavesdropper can no longer use replay attack.

# Discussion

In our botnet, a centralized web server (i.e. pastebot.net) is used to distribute files. There are some advantages, such as easy version and consistency control of the files, partition tolerance (when the bot sending the file is down, other bots can still read the file). However, the disadvantages are also obvious. The centralized web server is likely to be biggest target for other hackers. If they are able to hack this web server, they can read all our files. Moreover, the central web server might be the bottleneck of the whole system.

[Controlled by hackers? To be added!]

# Reference

[1] E. Rescorla, "Diffie-hellman key agreement method," 1999.

[2] T. Kivinen and M. Kojo, "RFC 3526: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)," ed: May, 2003.

[3] J. Daemen and V. Rijmen, *The design of Rijndael: AES-the advanced encryption standard*: Springer Science & Business Media, 2013.

[4] (2017, Apr). *Cipher Feedback (CFB)*. Available: https://en.wikipedia.org/wiki/Block\_cipher\_mode\_of\_operation#Cipher\_Feedback\_.28CFB.29