Phase 2.1 by Group 23

Designing an efficient CCA-secure protocol, using block ciphers, to simultaneously achieve confidentiality AND message integrity.

Overview

In this report, we will discuss ways in which message integrity and confidentiality can be achieved when communicating on an open, insecure channel.

Introduction

Communicating on an open channel can lead to serious problems, especially when sending and receiving confidential messages or other sensitive information. Authenticated Encryption (AE) models are forms of encryption that can help to alleviate this problem by ensuring the confidentiality and integrity of data. In addition to this, there exist Authenticated Encryption models that are secure from chosen ciphertext attacks (CCAs) as they allow the recipient to recognise improperly-constructed or tampered messages and refuse to decrypt them.

Authenticated Encryption involves two main functions; an encryption algorithm and a hash algorithm. These produce a ciphertext and a message authentication code (MAC). The ciphertext and MAC are combined and sent through the open channel.

Number of efforts have been made to implement Authenticated Encryption models. We have chosen the Encrypt-then-MAC (EtM) model for our problem as it has been proven to be secure against CCAs, earning the attribute of "unforgeable encryption" through cryptanalysis by Bellare, Khono, and Namprempre in 2000. We will give a summary of the chosen AE method below, along with a brief comparison to other AE models.

Encrypt-then-MAC

The EtM method involves 1) an encryption algorithm that takes the message in plaintext and a key as input, producing a ciphertext as output, and 2) a hashing algorithm that takes the resulting ciphertext and a key as input, producing a MAC as output. The resulting ciphertext and MAC are then appended and sent through the open communication channel. The encryption provides confidentiality and the MAC provides integrity of messages as it takes the ciphertext as input.

Compared to the EtM model, the MAC-then-Encrypt model does not provide any integrity on the ciphertext as its integrity is not known until the message is decrypted. This is because the message is encrypted *after* the MAC has been formed from the plaintext, forcing the recipient to decrypt the whole message before being able to authenticate the message, using the MAC.

Similarly, the Encrypt-and-MAC model provides no integrity on the ciphertext since the MAC takes the plaintext as input. A popular application of this model, SSH, has been proven to be insecure by Bellare, Kohno, and Namprempre as shown in section 4 of *Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the Encode-then-Encrypt-and-MAC paradigm*.

By learning from past cryptanalysis, such as one by Bellare, Khono, and Namprempre, EtM proves to be the most suitable AE model for CCA-secure data communication on an open channel.

It is important to note that an AE is only CCA-secure under two conditions; 1) the encryption method is semantically secure under a chosen plaintext attack, and 2) the MAC is unforgeable under a chosen ciphertext attack. We have accomplished condition 2 via choosing the EtM method. To achieve condition 1, AES (Advanced Encryption Standard) can be chosen as it is the first (and only) publicly accessible cipher approved by the U.S. National Security Agency (NSA) for top secret information and has been the standard for symmetric encryption for a number of years.

References

- Bellare, M., Khono, T. and Namprempre, C. (2004). Breaking and Provably Repairing the SSH Authenticated Encryption Scheme: A Case Study of the Encode-then-Encrypt-and-MAC Paradigm. Retrieved November 3, 2021 from https://homes.cs.washington.edu/~yoshi/papers/SSH/ssh.pdf
- D. McGrew (2008). An Interface and Algorithms for Authenticated Encryption. Retrieved November 1, 2021 from https://datatracker.ietf.org/doc/html/rfc5116
- Kavun, E., Mihajloska, H., and Yal, T (2019). Authenticated Encryption – A Hardware Designer's Perspective. Retrieved November 1, 2021 from https://eprint.iacr.org/2019/739.pdf