Blowfish and its Successors

Cameron Stark

CS 428 - Applied Cryptography

Table of Contents

Introduction

Throughout history long perform the words computer science even were thought of together, people have had a need to encrypt data to protect from enemies they are at war with or control and segment information such is the case with Roman Empire and Caesar. Caesar created the Caesar cipher which was a form of encrypting whereby the message is letter shifted by a chosen letter, where the message is shifted in the alphabet by that value. Another prominent form of encryption was the Enigma machine encryption used by the Germans in World War 2. The encryption made use of letter substitution depending on how the machine was set up at the initial step. Both of these encryption methods suffered from being breakable and leaked information because the keys and encryption methods were not completely random or the way they were created are prone to being broken by a brute force attack. Many of the earlier computer scientists in the field of encryption started off with variations of past methods, however quickly discovered that as computer processing power increased the vulnerabilities of contemporary encryption methods became apparent. One of the attempts to create a new algorithm for encrypting information was the Blowfish algorithm, which was built as a replacement to the aging DES algorithm.

Who Created Blowfish?

Blowfish was created by a Computer Scientist named Bruce Schneier in 1993, as a general purpose algorithm for encryption to replace DES and the problems associated with other algorithms of the time. Bruce Schneier worked at various companies where he worked in the field of computer security, such as IBM when they acquired another company where he was the CTO at, and is also a fellow at the Berkman Center for Internet & Society at Harvard as well as a program fellow at the Open Technology Institute. Bruce Schneier also wrote many papers and articles on the topic of data governance and security both during his times at American University and University of Westminster, where he received degrees in Computer Science. Bruce Schneier was a part of the creation of many types of encryption algorithms in different categories with blowfish being a block cipher, he contributed to some hash functions, stream ciphers, Pseudo-random number generators and the successors to blowfish.

What is Blowfish and Why Create it?

Blowfish is a type of block cipher, that makes use of a symmetric key, which is a system where the same key is used for encryption and decryption, where in practice the key represents a shared secret. This can be a drawback of this type of encryption because it requires that both parties have direct access to the secret key, whereas with public-key encryption both parties aren't required to have access to the key. Blowfish was created because many

of the other encryption algorithms at the time were expensive because their inherent overhead to run them or the licensing to use them was expensive because a company or person would have the algorithm under a patent and restricted use of it. Bruce Schneier created Blowfish with the intention of free access and use therefore it is not patented, which thrusted Blowfish into the public domain. The algorithm works similar to a Feitstel Cipher, which is a type of cipher with the characteristics of round based XOR between the two halves of the plaintext, with it alternating between which side goes through the function before being a part of the XOR, the ciphertext is returned as the result of the XOR with the Right going before the left side. The blowfish algorithm follows this same process, but goes for 16 rotations, thereby increasing the security and complexity.

In practice blowfish is a really fast encryption algorithm and has very specific uses as a result of its key changing process which is the main drawback of the algorithm because it is very slow when compared to other block ciphers at that time. However this slow key changing process has a good application in a process that needs more protection from dictionary attacks because the longer key changing time provides protection requiring more computational effort. Another drawback of blowfish is the footprint it has in terms of size, for computers and laptops the 4kb of RAM needed to run it is not normally an issue however for some smaller embedded systems the RAM requirement can be a limitation. Blowfish was outdone by its successors

because of the limitations that its 64-bit block size has, such as being very vulnerable to various attacks, most notably the birthday attack, which has caused the algorithm to fall out of use, with many even the creator favoring twofish.

Successors To Blowfish

The main prominent alternative to blowfish, which is also recommended by Bruce Schneier is Twofish, which is also a block cipher with symmetric keys but has an increased block size and key size. The aspects of two fish that distinguish it from its predecessor Blowfish is the pre-computed S-Boxes that are key dependent, which are used in the XOR process, and complex key schedule. Twofish was a finalist for the AES (Advanced Encryption Standard) Contest, but was beaten by Rijndael which has caused Twofish to lag behind in adoption and speed because hardware is being set to the standard of AES. Twofish, unlike Blowfish employs a Maximum Distance Separable matrix, which is a type of matrix that has useful applications in cryptography because it represents a function that has diffusion properties.

What Was Learned?

Learned a lot about the AES methods of choosing the standard for encryption methods, which twofish was in the running for but ended up

losing the standard contest. Also learned a lot about how the different encryption methods work and why they work the way they do.

Conclusion

Blowfish was an influential encryption algorithm because of its lack of patents and restrictions allowed it to be known in the public domain and get widespread use allowing everyone to encrypt their information without having to be a large company to be able to buy the license for an encryption algorithm. The successors to Blowfish, being Twofish and also Threefish, to this day have not officially been broken as an encryption algorithm, therefore they are still viable methods of encryption methods outside of the AES standard and they are both unpatented which allows for the general public to make use of the method.

References

https://www.schneier.com/academic/blowfish/

https://www.schneier.com/academic/twofish/