International Journal of Research in Engineering, Science and Management
Volume-1, Issue-12, December-2018
www.ijresm.com | ISSN (Online): 2581-5792

Network Security with Cryptography

Chaitanya Tejas[1], K. D. Mithun Kumar[2], B. V. Brindashree[3], V. Aruna kumari[4], Chanchal Antony[5]
[1,2,3,4]*Student, Department of Computer Science Engineering, Alva's Inst. of Engg. and Tech., Moodbidri, India*
[5]*Senior Assistant Professor, Dept. of Computer Science Engg., Alva's Inst. of Engg. and Tech., Moodbidri, India*

***Abstract*: All components work together to increase the overall security of the computer network. Network Security & Cryptography is a concept to protect network and data transmission over wireless network. Data Security is the main aspect of secure data transmission over unreliable network. Security of data can be done by a technique called cryptography. So one can say that Cryptography is an emerging technology, which is important for network Security. The model for Cryptosystem using Neural Network supports high security.**

***Keywords*: computer networks, cryptography, Cryptosystems, Ciphers, Encryption, Decryption.**

1. Introduction

Cryptography is an emerging Technology, which is important for network security. The field network and internet security consists of measures to deter, prevent detect and correct security violations that involve the transmission of information. With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer became evident. This is especially the case for a shared system, such as a time-sharing system, and the need is even more acute for systems that can be accessed over a public telephone network, data network, or the Internet. The generic name for the collection of tools. Designed to protect data from hackers is computer security.

2. CRYPTOGRAPHIC ALGORITHMS

Cryptography at its very core is math. Pure, simple, undiluted math. Math created the algorithms that are the basis for all encryption. And encryption is the basis for privacy and security on the internet. This cryptosystem is responsible for creating the key(s) that will be used to encrypt and then decrypt the data or message. A number of signing algorithms have been created over the years to create these keys, some of which have since been deprecated as computing power has increased.

A. Brute force attack

A brute force attack or a dictionary attack as it's also known is a trial and error method of obtaining the private key of an encrypted packet of data. The trial and error is done by a computer so the higher the computational power, the more "tries" it can have in a short space of time. As computing power and performance increases, the ability to find the private key increases, unless you increase the length of the key so that a higher number of possibilities exist.

B. Encryption key sizes

Key size or key length refers to the number of bits in a key used by a cryptographic algorithm. Only the correct key can decrypt a cipher text (output) back into plaintext (input). As CPU power gets more advanced, the computational time required to brute force an encryption key gets less and less. As such, keys have had to become longer. For many years the limit was 40-bits, but today we are seeing up to 4096-bit key lengths in cryptography.

C. Symmetric key algorithms

A symmetric key algorithm (also known as a secret key algorithm), uses the concept of a key and lock to encrypt plaintext and decrypt cipher text data. The same "key" is used to both encrypt and decrypt the file. They are sub-classified by stream ciphers and block ciphers. A stream cipher is where plaintext digits are combined with a pseudo-random cipher digit stream. Block ciphers take the number of bits and encrypt them as a single unit (known as rounds), padding the plaintext so that it's a multiple of a block size. The algorithm itself is not kept a secret and the sender and receiver of communication must both have copies of the secret key in a secure place. The use of the same key is also one of the drawbacks of symmetric key cryptography because if someone can get hold of the key, they can decrypt your data.

D. Asymmetric algorithms

Asymmetric cryptography is also known as public key cryptography and is based on the principle of having a pair of mathematically-related keys for encryption and decryption: a public key and a private key. The public key pair can be shared with anyone, while the private key must be kept secret. Anyone with the public key can encrypt a message but only the holder of a private key can decrypt it. Security depends on secrecy of the private links.

E. RSA

The Rivet-Shammir-Adelman algorithm, better known as RSA, is now the most widely used asymmetric cryptosystem on the web today. RSA is based on the factorization of prime numbers, because working backwards from two multiplied prime numbers is computationally difficult to do, more so as the prime numbers get larger. The challenge of breaking RSA is known as the 'RSA problem. RSA is a slow algorithm and because of this, it is used to encrypt and decrypt the symmetric

keys which in turn, encrypt and decrypt the communications. The symmetric keys perform the bulk of the work, while RSA creates a strong and secure channel.

F. Wireless security

It is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are wired equivalent privacy (WEP) and wifi protected access (WPA). WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP is an old IEEE 802.11 standard from 1999, which was outdated in 2003 by WPA, or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP.

G. Model for network security

The model in which, a message is to be transferred from one party to another across some sort of internet. The two parties, Who are in this transaction, must cooperate for the exchange to take place. A logical Information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals. Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

- A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender
- Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the
- Message before transmission and unscramble it on reception. A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

H. Secure hash algorithm

The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology. (NIST) and published as a federal information processing standard (FIPS 180) in 1993; a revised version was issued as FIPS 180-1 in 1995 and is generally referred to as SHA-1. The actual standards document is entitled Secure Hash Standard. SHA is based on the hash function MD4 and its design closely models MD4. SHA-1 is also specified in RFC 3174, which essentially duplicates the material in FIPS 180-1, but adds a C code implementation. SHA-1 produces a hash value of 160 bits

I. MD5

The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. The MD5 hash function was originally designed for use as a secure cryptographic hash algorithm for authenticating digital signature. MD5 has been deprecated for uses other than as a non-cryptographic checksum to verify data integrity and detect unintentional data corruption. The algorithm takes as input a message of arbitrary length and produces as output a 128-bit 'fingerprint' or 'message digest' of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be 'compressed' in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA as earlier explained.

J. Web security

The World Wide Web is fundamentally a client/server application running over the Internet and TCP/IPintranets. As such, the security tools and approaches discussed so far in this book are relevant to the issue of Web security.

- The Internet is two way. Unlike traditional publishing environments, even electronic publishing systems involving teletext, voice response, or fax-back, the Web is vulnerable to attacks on the web servers over the Internet.
- The Web is increasingly serving as a highly visible outlet for corporate and product information and as the platform for business transactions. Reputations can be damaged and money can be lost if the Web servers are subverted.
- A Web server can be exploited as a launching pad into the corporation's or agency's entire computer complex. Once the Web server is subverted, an attacker may be able to gain access to data and systems not part of the Web itself but connected to the server at the local site.

3. Conclusion

Security in the Internet is improving. The increasing use of the Internet for commerce is improving the deployed technology to protect the financial transactions. Extension of the basic technologies to protect multicast communications is possible and can be expected to be deployed as multicast

becomes more widespread. Control over routing remains the basic tool for controlling access to streams. Implementing particular policies will be possible as multicast routing protocols improve. Cryptography is a tool which may alleviate many of the perceived problems of using the Internet for communications. However, cryptography requires the safe implementation of complex mathematical equations and protocols, and there are always worries about bad implementations.

References

[1] Cryptography and Network Security Principles and Practices, Fourth Edition By William Stallings
[2] Cryptography for Network Security: Failures, Successes and Challenges Bart Preneel Katholieke Universiteit Leuven and IBBT Dept. Electrical Engineering-ESAT/COSIC,
[3] Kasteelpark Arenberg 10 Bus 2446, B-3001 Leuven, Belgium Network Security with Cryptography.