International Journal of IT & Knowledge Management (ISSN: 0973-4414)
July-Dec 2008, Vol 1, Number-2, pp 593-599

Approach to Modern Network Security: Modern Data Encryption

Chhattar Singh Lamba
Research Scholar, Jai Narain Vyas University Jodhpur
kunjean_lamba@yahoo.com

Abstract: In today's information age, communications play an important role which is contributed to the growth of technologies. Communication Security is increasing in importance as a result of the use of electronic communications in more and more business activities. Therefore, a mechanism is needed to assure the security and privacy of information that is sent over the electronic communications media is in need. Whether the communications media is wired or wireless, both can be not protected from unauthorized reception or interception of transmission. The, method of transforming the original information into the unreadable format is called encryption and decryption of information. The study of encryption and decryption is known as Cryptography. Cryptography is the only practical means to provide security services in many applications. Cryptography or communication by using secret code was used by the Egyptians some 4000 years ago. The secure transport of messages was the concern of many early civilizations. However, the science of cryptography was initiated by Arabs since 600s.Cryptography becomes vital in the twentieth century where it played a crucial role in the World War I and 11. This paper focuses on the analysis "**modern data encryption".** The traditional symmetric-key ciphers that we were using are character-orientated ciphers. With the advent of computer, we need bit-oriented ciphers. This is because the information is to be encrypted is not just text; it can also consist of numbers, graphics, audio, and video data. It is convenient to convert these types of data into streams of bits to encrypt the stream, and then to send the encrypted stream. In this paper all the modern data encryption techniques are discuss.

1 INTRODUCATION

Communications security is increasing in importance as a result of the use of electronic communications in more and more business activities. Cryptography is the only practical means to provide security services in many applications.

Research into cryptography has exploded in the last 18 years and a variety of cryptographic algorithms and techniques have emerged.

Symmetric algorithms have been dominated by the Data Encryption Standard since 1976, but a number of replacements are now being proposed.

Security of communications was historically the concern of military and government interests.' However, the importance of communications security in the Architecture' the aim of security measures is to minimize the vulnerability of assets and resources. That document also describes a number of 'security services', such as confidentiality, user and data origin commercial sector has been increasing in recent years and will continue to do so in the future. This is because of the ever greater reliance on electronic communications, particularly data communications, for the running of commerce and industry, which makes valuable commercial resources vulnerable to a variety of threats which have not previously been of concern. Provision of security services can be expensive, particularly if provided on an ***ad*** *hoc* basis for each application separately. An important way to alleviate this cost is through the development of standard security solutions, which can include standardized secure protocols and procedures, as well as cryptographic algorithms. I shall concentrate on standard solutions in this article, by which I mean both techniques which have been approved by formal standardization bodies, and those which are regarded as standard

simply due to wide acceptance. According to the **OS1** (open authentication, dgta integrity and access control(see T1 **).** Each **of these services could be provided** in a number of different ways. For example, confidentiality of data could be provided by physically protecting all communication lines and terminals. It is clear that such a solution is unrealistic in a distributed environment since communications with all end- systems should be possible without regard to the physical situation of cables. In view of this, logical rather than physical security measures are taken, which in the case of provision of confidentiality and authentication services implies the use of Cryptography. Physical measures may still play an important part (possibly even the major part), particularly in providing access control.

However, we can be sure that if comprehensive communications security is required in an open communications environment then cryptography will play a fundamental par .

In the following Section we will examine how cryptography may be used to provide different communications security services. The most common algorithms for conventional secret-key cryptography and the newer public key cryptography are examined in Sections 3 and **4,** respectively. Finally a brief look is taken at some application areas and commercial products illustrating the pervious materials.

T 1. Security Services

- ***Authentication:*** The process of proving one's identity. It is aimed at establishing the identity of a specific individual (The primary forms of host-to-host authentication and the internet today is name-based or address-based, both of which are notoriously weak.)

- ***Privacy/confidentiality:*** Protection against unauthorized disclosure of information. Confidentiality may be applied to whole messages, part of messages and even existence of messages**.** It will ensure that no one can read the message except the intended receiver.

-***Data Integrity:*** Corroboration that a message has not been changed in any way (including alteration, insertion, deletion, re-ordering) since it was sent.

- ***Non-repudiation:*** Prevention of denial that a received message was sent in other words the service provides proof of sending**.**

2. Security Risks in communications,

In recent years, more and more businesses make use of communication networks. Share potential information and therefore sensitive data is located in communications network transmissions that are connected all over the world**.** This commitment to data communication has increased the vulnerability of organization assets. Computer fraud is becoming one of the most popular crimes in our days. Since a network without security mechanisms is like an office building with open doors, the network owner has to make sure to lock those doors and give keys only to those people whom he wants to share the information with. For many people, communications security just means preventing unauthorized access, such as preventing a hacker from breaching into a network. Security is more than that.

3 Cryptographic properties

Confidentiality **and** authentication:

Cryptography concerns the application of transformations, or encodings, of information that depend on a secret key. Application of a cryptographic function is termed encryption and he encrypted data are termed, ciphertext. Usually, but not always, the function is invertible and the application of the inverse transformation is termed decryption. There are two fundamental properties that a cryptographic transformation may possess:

Property I*:* It is infeasible to recover the original information from the cipher text without knowledge of the secret key. By transforming (encrypting) with such a function the *confidentiality* security service is provided.

***Property* 2**: It is infeasible to form the cipher text from the original information without knowledge of

the secret key. By transforming with such a function the *authentication* security service is provided.

To complete these definitions it should be explained what is meant y saying that an operation is ‘infeasible'. In fact this has to depend very much on the details of i.e. transformation used. In certain situations it can mean that there is insufficient information available to perform the operation, so that no matter what resources are available to an attacker the operation cannot be performed. More usually it will mean that the operation requires computing resources that are believed to be beyond the means of an attacker. Cryptography was primarily forth provision of confidentiality. In military and diplomatic communication it is the secrecy of the information conveyed that is paramount. Confidentiality may certainly be of concern for some types of commercial information, for example new product data or market research results. But it is authentication that is the more important use for cryptography in commercial situations. Nowadays many billions of Dollars are transferred electronically every Day between banks. It is far more important that the messages authorizing these transfers can be verified to have come from the claimed source, and are unchanged, than that they are keep secret. In traditional paper-based business practice authentication is built up by a variety of means, including letter heads, signatures, and business cards, personal acquaintance and familiar procedures. **As** we move more towards electronic trading these assurances will disappear and the potential for fraud may increase. Cryptographic authentication must take the place of authentication by humans.

Certain cryptographic algorithms possess both Property 1 and Property 2 and so can be used to provide both the confidentiality and authentication services.

Decryption is the same as encryption, since adding modulo 2 is a self-inverse operation. Now, suppose that we know that the one- time pad is used to secure the amount sent in a funds transfer. Then we may alter any of the bits of cipher text and change the amount sent even though we cannot find what the original amount was. If we know that amounts are usually small then we could alter the most significant bit and expect to increase the amount sent substantially. This simple example shows that the one-time pad on its own provides no authentication even though it provides perfect secrecy.

Symmetric algorithms

Block and stream ciphers

A convenient distinction in the consideration of cryptographic algorithms is between *block* ciphers and *stream* ciphers. If, as is usually the case, we wish to encipher a binary stream of data, then a stream cipher handles each bit separately whereas a block

cipher deals with a block of data, of some predetermined size, simultaneously However, this distinction is rather superficial since logically a block cipher could have a one bit block length. The formal difference between block and stream ciphers is that the stream cipher enciphers each bit according to its position in the data stream, whereas a block cipher (in its basic mode) treats every block equally without regard to what has come before. This difference has important consequences in practical communications. If errors occur during transmission, data encrypted with a binary stream cipher will have errors in the decrypted text exactly where transmission errors have occurred however, if a block cipher was employed a single bit error in transmission will result in the corresponding decrypted block being entirely random. This *error extension* property of block cipher: is an important consideration in choosing a practical cipher. In practice a block cipher is normally not used to encrypt separate blocks of data in a sequential manner. A number of different *modes of operation* have been devised which allow Properties such as efficiency, error Propagation and synchronization to be optimized according to the application. One of these modes allows a block cipher to be used as a binary key stream generator for stream ciphers and this is one of the most common ways of implementing a stream cipher in practice. The best

known symmetric algorithms are block ciphers in their basic form, and we restrict further attention to these in the knowledge that they can be used as stream ciphers if required.

Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a Symmetric-key block cipher published by the national institute of standards and technology.

Goal of DES is to completely scramble the data and key so that every bit of cipher text depends on every bit of data and ever bit of key. It is a block Cipher Algorithm, encodes plaintext in 64 bit chunks, One parity bit for each of the 8 bytes thus it reduces to 56 bits. It is the most used algorithm. DES developed by IBM in the early 1970s. Standard approved by US National Bureau of Standards for Commercial and non classified US government use in 1993.DES was published in the Federal Register in March 1975 as a draft of the Federal information Processing Standard (FIPS).

DES is an iterated block cipher, iterated means multiple repetitions of a simple encryption algorithm. **DES** has 16 rounds. Where Block cipher encrypts in fixed-size blocks. DES uses 64-bit (&byte) blocks. At its simplest level, DES is a combination of the two basic techniques of cryptography: confusion and diffusion. DES follows strict avalanche criteria. Every bit of the key and every bit of the plaintext affects every bit of the cipher text. It has different keys for encryption and decryption. Eavesdropper sees the cipher text and one of the keys. All of the security is in one key; there is none in the algorithm or in the second key.

Alternatives to DES:

Doubts as to the advisability of continued use of the DES have led to the emergence of a number of alternatives. Three of the most prominent candidates are the Fast Encryption Algorithm (FEAL) invented by Japanese experts," the LOKI algorithm pioneered in Australia" and the IDEA (International Data Encryption Algorithm) from two researchers in Switzerland." Each of these algorithms has a 64 bit block length which will make them compatible with DES in many applications. However they all have a larger key length than DES, with FEAL and LOKI having 64 bits and IDEA having 128 bits.

All of these algorithms are relatively new and none has yet received the attention that the DES algorithm was subjected to before it became widely accepted. Each of them appeared in its initial form before differential cryptanalysis became publicly known and each has been affected by it. FEAL, the oldest of the three, was one of the algorithms which proved very vulnerble in the original work of Biham and Shamir. It has also been subjected to a number of other successful attacks. However it continues to be supported in

Japan and a number of different versions of FEAL now exist. As improvements are made the algorithm may become trusted. LOKI and IDEA have both received adjustments to their initial designs to make them more secure against differential cryptanalysis. At present it is not at all clear which algorithm, if any, will emerge as the successor to DES, either formally or as a de ***facto*** standard.

Although the DES has been used on an international basis, the algorithm never became an international standard. Indeed, the International Organization for Standardizations **(ISO)** has committed itself ***not*** to standardize any cryptographic algorithms. The argument over whether standardized algorithms should exist at all is complex. No practical cryptographic algorithms have unconditionally provable security and so worldwide reliance on a single algorithm may be deemed unwise, and an incentive for attackers, even if compromise is deemed unlikely. On the other hand, to permit inter working it is clear the shared algorithms must exist. IS0 has addressed this problem by supporting the development of a register in which algorithms may be identified by a standard naming convention, thus allowing negotiation of a suitable algorithm, even between communicating entities with no prior knowledge of each other.

Asymmetric algorithms

Most asymmetric algorithms base their security on problems from the branch of mathematics known **as** number theory. They use modular (or finite) arithmetic rather than the ordinary unbounded integers. Arithmetic operations such as addition and multiplication work in roughly the same way in modular arithmetic as in ordinary arithmetic. However, it turns out that some functions, such as taking square roots, are trivial in ordinary integers but can be
infeasible (in the sense of being computationally too intensive) in modular arithmetic for large enough examples. This is what makes modular arithmetic suitable for cryptographic algorithms.

The RSA algorithm

Just as with Symmetric algorithms, there is one asymmetric encryption algorithm that is unquestionably the most widely known and talked about. Published by three MIT researchers, Rivest, Shamir and Adleman, in 1978" it is known universally as the RSA algorithm. The mathematics of the algorithm is surprisingly straightforward, and the whole encryption procedure can be explained in one simple equation. To generate a public key a modulus *m* is first chosen which the product of two is large, random, prime numbers p and *q* known only to the owner of the secret key. Once m is chosen integers e and *d* are generated so that
$ed = 1 \bmod (p-l)(q-l)$
The public key then consists of the two values *e* and *m,* while *d* is kept secret. To encrypt a message the sender first encodes it, in a publicly known way, as a positive integer **x** less than ***m.*** The sender then calculates the cipher text *c* using the equation:
$c = x^e \bmod m$
It can be shown using elementary number theory that
$x=c^d \bmod m$
and so x can be recovered by the owner, but not by anybody who does not know the secret key *d.* The modulus *m* is typically hundreds of bits long and varies in implementations from 256 bits to 1024 bits or more. The security of RSA is strongly related to the problem of factorizing large numbers. It can be shown that finding the secret key *d* from knowledge of the public key *e* is as hard as factorizing the modulus *m* into the prime factors *p* and *q.* Since integer factorization is believed to be infeasible for large enough values, this shows that finding the secret key from the public key is also infeasible. Of course the larger the modulus is, the harder it is to factories, and so a 256 bit modulus provides nowhere near the security that a 1024 bit modulus does. Research into the factorization problem is very active and it is impossible to rule out a decisive advance. However, at the current state of knowledge it is believed that it will be at least the end of the century before a 5 12 bit RSA modulus can be routinely factorized and that a 1024 bit modulus is currently sufficient to achieve long-term security to satisfy most applications.
The penalty for the (believed) high security provided by RSA is the complexity of implementation. Despite being based on simple arithmetic, the size of numbers involved makes RSA encryption and decryption computationally expensive procedures. A number of dedicated hardware chips have been developed to ease the problem, but even these typically achieve a throughput of a few kilobits per second.14 In view of this limitation, RSA is not normally recommended for bulk encryption of data. Instead it is more usual to employ RSA to send a secret session key at the start of transmission, and then use this session key with a symmetric algorithm such as the DES. In this way the benefit of not requiring an initial shared key is preserved, but the problem of limited throughput is removed.
Because both the message and the cipher text for RSA are positive integers less than the modulus *m,* the secret and public transformations may be reversed to provide digital signatures. The owner of the secret key simply performs the 'decryption' process on the message to be signed. Anybody with the public key can then 'encrypt' to recover the plaintext of the signed message and thus verify that it was constructed by the owner of the secret key.

Once again this is very time consuming for long messages and in view of this a digest only of the message is usually signed. This digest is produced by a *hash function* which will take a message of any length and return a string of length not greater than the modulus in use. As long as it is not Feasible for anybody to find two messages which hash to the same value, the digest can be signed in place of the message. The hash function is public and so the digest: an be calculated by the signature verifier and then compared with :he value found when verifying the signature with the public key .

In order to be useful with signatures, a hash function must have the *oneway property* that it should be infeasible to find a different message which hashes to be same value as a given message. If this were not the case then it would be possible to use the signature of one message as the in order to be useful with signature of another. A number of suggestions have been made for constructing hash functions from symmetric block ciphers, but they have often proved not to be one-way. Some more recent, specially designed, hash functions appear to be safer, at least so far. In particular, a family of functions designed by Rivest, called MD2,

MD4 and MD5,I5 are still unbroken after a few years of scrutiny. These functions are roughly of similar complexity to symmetric

encryption algorithms.

Alternatives to RSA

There are a number of variations on the RSA theme, all of which rely on the difficulty of the factorization problem for their security. There are a host of other problems existing in the theory of computational complexity which are believed to be infeasible. It is one of the great disappointments of research into public key cryptography that very few of these problems have so far been of use in the designs of new algorithms. People have learnt to be cautious after the spectacular demise of the: lass of algorithms known collectively as *knapsack algorithms.* These algorithms are based on a problem known to be at least as hard as the factorization problem, and have the advantage if being far faster to encrypt with than RSA. Despite their early promise, almost all the knapsack algorithms suggested have proven to be completely insecure; in essence the restrictions needed to make the general problem into a practical cryptosystem restricted .he problem to easy cases. Although there remain one or two in broken knapsack schemes, the idea is widely regarded as unreliable.

The only serious rivals to public key cryptosystems based on the factorization problem are those which use the *discrete logarithm problem* (the DLP) as the basis for their security. The DLP is the problem of finding *x* given

$\mathbf{a}^{x}$ mod p

where *p* is a prime number and *a* is a known value. This looks similar o taking ordinary logarithms, but if performed in large integers it becomes another infeasible problem. The DLP forms the basis of the public key exchange mechanism suggested by Diffie md Hellman in their paper which first described the idea of public key cryptography. In 1985 a full public key cryptosystem based on the problem was published by ElGamal.

Comparison of the benefits of using DSA or RSA for implementing digital signatures is not straightforward and there has been considerable public debate about whether the choice NIST has made for its standard is reasonable.

From the point of view of efficiency, RSA can be made to be much faster when verifying signatures, but DSA is better for forming the signatures in the first place. Which of these is more important depends very much on the area of application. The controversy over the standardization of DES has been paralleled in the recent public debate over the DSA." Inevitably it is often difficult to unravel the technical arguments from the commercial interest. This is largely due to the existence of patents in respect of a number of algorithms. In particular the RSA algorithm is subject to a patent in the USA, although not in other parts of the

world.

5 Applications and implementations

Cryptography is already in wide use in a number of civilian communications areas.
The financial sector is one of the most important. Cryptography is used for authentication in the transfer of funds between banks. Cryptography is also used, behind the scenes, every time we enter our plastic cards into an automatic cash dispenser. Satellite television broadcasts form another pervasive application. Cryptography is open and distributed communications rely on the use of standards. A general format for electronic mail was published in the 1988 CCITTX400 series of standards which includes a wide range of security options implemented through cryptography. The related X500 Directory Systems standards define a method for management of public keys so as to maintain their integrity. It is more use in Internet network. Many dedicated hardware chips exist which implement encryption algorithm. Security products incorporating cryptographic hardware and software are available from a wide variety of vendors. Examples include secure phones, data encryptions, password generators, smart card interfaces, and slot-in cards for PCs.

Conclusion

As electronic communications become more common in everyday business activities, the security of those communications will be of ever increasing importance. The recent explosion of interest in cryptographic research shows no sign of abating. The breathtaking increase in the speed of computers over the last twenty years seems likely to continue, which will result in the need for new and improved algorithms. It is not clear at the moment whether these will be standardized algorithms available for public use, or whether proprietary algorithms will become the norm. In any event, it seems that the struggle between the cryptographer and the cryptanalyst will continue for the foreseeable future.

References

1. www.quadibloc.com/crypto/
2. www,ietf.org/rfc
3. cryptography and network security by Behrouz A.Forouzan
4. Applied Cryptography by Bruce Schneier
5 ADLEMAN, L.: 'A method of Obtaining digital signatures and public-keycryptosystems', *Commun.* ***ACM,*** 1978