**[Abstract and full paper on NETWORK SECURITY AND CRYPTOGRAPHY](http://www.creativeworld9.com/2011/04/abstract-and-full-paper-on-network_13.html)**

WEDNESDAY, APRIL 13, 2011 | TAGS: [ABSTRACT OF MCA IN IEEE FORMAT](http://www.creativeworld9.com/search/label/abstract%20of%20MCA%20in%20ieee%20format), [CRYPTOGRAPHY](http://www.creativeworld9.com/search/label/Cryptography), [DATA LAYER](http://www.creativeworld9.com/search/label/DATA%20layer), [DRAFTS](http://www.creativeworld9.com/search/label/DRAFTS), [MBA/MCA PPT ABSTRACTS](http://www.creativeworld9.com/search/label/MBA/MCA%20%20PPT%20ABSTRACTS), [PHYSICAL LAYER](http://www.creativeworld9.com/search/label/physical%20layer), [SECURE INTERNET COMMERCE](http://www.creativeworld9.com/search/label/Secure%20Internet%20Commerce),[TRANSPOSITION CIPHERS](http://www.creativeworld9.com/search/label/Transposition%20Ciphers)

[DIGG IT](http://digg.com/submit?url=http://www.creativeworld9.com/2011/04/abstract-and-full-paper-on-network_13.html&title=Abstract%20and%20full%20paper%20on%20%20NETWORK%20SECURITY%20AND%20CRYPTOGRAPHY) | [STUMBLE IT](http://www.stumbleupon.com/submit?url=http://www.creativeworld9.com/2011/04/abstract-and-full-paper-on-network_13.html&title=Abstract%20and%20full%20paper%20on%20%20NETWORK%20SECURITY%20AND%20CRYPTOGRAPHY) | [SAVE TO DEL.ICO.US](http://del.icio.us/post?url=http://www.creativeworld9.com/2011/04/abstract-and-full-paper-on-network_13.html&title=Abstract%20and%20full%20paper%20on%20%20NETWORK%20SECURITY%20AND%20CRYPTOGRAPHY)

**NETWORK SECURITY AND CRYPTOGRAPHY**

ABSTRACT

For the first few decades of their existence, computer networks were primarily used by university researchers for sending e-mail and by corporate employees for sharing printers. Under these conditions, security did not get a lot of attention. But now, as millions of ordinary citizens are using networks for banking, shopping, and filing their tax returns, network security is looming on the horizon as a potentially massive problem.

The requirements of information security within an organisation  have undergone two major changes in the last several decades.before the widespread use of data processing equipment ,the security of information felt to be valuable to an organization was provided primarily by physical and administrative means .

.with the introduction of computer  the need for  automated tools for protecting files and other information stored on the computer became an evident .this  is especially the case for a shared system,such as time sharing system and the need is even more acute for systems that can be accessed for a public telephone or a data network..the generic name for the collection of tools to protect data and to thwart  hackers is “computer security”.

Network Security

Security is a broad topic and covers a multitude of sins. In its simplest form, it is concerned with making sure that nosy people cannot read, or worse yet, secretly modify messages intended for other recipients. It is concerned with people trying to access remote services that they are not authorized to use. Most security problems are intentionally caused by malicious people trying to gain some benefit, get attention, or to harm someone. Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication, nonrepudiation, and integrity control. Secrecy, also called confidentiality, has to do with keeping information out of the hands of unauthorized users. This is what usually comes to mind when people think about network security. Authentication deals with determining whom you are talking to before revealing sensitive   information or entering into a business deal. Nonrepudiation deals with signatures.

                                          Secracy: Only the sender and intended receiver should be able to understand the contents of the transmitted message. Because eavesdroppers may intercept the message, this necessarily requires that the message besomehow encrypted (disguise data) so that an intercepted message can not be decrypted (understood) by an interceptor. This aspect of secrecy is probably the most commonly perceived meaning of the term "securecommunication." Note, however, that this is not only a restricted definition of secure communication , but a rather restricted definition of secrecy as well.

Authentication :Both the sender and receiver need to confirm the identity of other party involved in the communication - to confirm that the other party is indeed who or what they claim to be. Face-to-face human communication solves this problem easily by visual recognition. When communicating entities exchange

messages over a medium where they can not "see" the other party, authentication is not so simple. Why, for instance, should you believe that a received email containing a text string saying that the email came from a friend of yours indeed came from that friend? If someone calls on the phone claiming to be your bank and asking for your account number, secret PIN, and account balances for verification purposes, would you give

that information out over the phone? Hopefully not.

Message Integrity: Even if the sender and receiver are able to authenticate each other, they also want to insure

that the content of their communication is not altered, either malicously or by accident, in transmission.

Extensions to the checksumming techniques that we encountered in reliable transport and data link protocols

 Nonrepudiation: Nonrepudiation deals with signatures

 Having established what we mean by secure communication, let us next consider exactly what is meant by an "insecurechannel." What information does an intruder have access to, and what actions can be taken on the transmitted data?

Figure  illustrates the scenario

Alice, the sender, wants to send data to Bob, the receiver. In order to securely exchange data, while meeting the

requirements of secrecy, authentication, and message integrity, Alice and Bob will exchange both control message anddata messages (in much the same way that TCP senders and receivers exchange both control segments and data

segments). All, or some of these message will typically be encrypted. A passive intruder can listen to and record the

control and data messages on the channel; an active intruder can remove messages from the channel and/or itself add messages into the channel.



 Network Security Considerations in the Internet :- Before delving into the technical aspects of network security in the following sections, let's conclude our introduction by relating our fictitious characters - Alice, Bob, and Trudy - to "real world" scenarios in today's Internet



. Let's begin with Trudy, the network intruder. Can a "real world" network intruder really listen to and record passively receives all data-link-layer frames passing by the device's network interface. In a broadcast environment

such as an Ethernet LAN, this means that the packet sniffer receives all frames being transmitted from or to all hostson the local area network. Any host with an Ethernet card can easily serve as a packet sniffer, as the Ethernet interface card needs only be set to "promiscuous mode" to receive all passing Ethernet frames.  These frames can then be passed on to application programs that extract application-level data. For example, in the telnet scenario , the login password prompt sent from A to B, as well as the password entered at B are "sniffed" at host C. Packet sniffing is a double-edged sword - it can be invaluable to a network administrator for network monitoring and management  but also used by the unethical hacker. Packet-sniffing software is freely available at various WWW sites, and as commercial products.

Cryptography:- Cryptography comes from the Greek words for ''secret writing.'' It has a long and colorful history going back thousands of years. Professionals make a distinction between ciphers and codes. A cipher is a character-for-character or bit-for-bit transformation, without regard to the linguistic structure of the message. In contrast, a code replaces one word with another word or symbol. Codes are not used any more, although they have a glorious history

The messages to be encrypted, known as the plaintext, are transformed by a function that is parameterized by a key. The output of the encryption process, known as the ciphertext, is then transmitted, often by messenger or radio. We assume that the enemy, or intruder, hears and accurately copies down the complete ciphertext. However, unlike the intended recipient, he does not know what the decryption key is and so cannot decrypt the ciphertext easily. Sometimes the intruder can not only listen to the communication channel (passive intruder) but can also record messages and play them back later, inject his own messages, or modify legitimate messages before they get to the receiver (active intruder). The art of breaking ciphers, called cryptanalysis, and the art devising them (cryptography) is collectively known as cryptology.

It will often be useful to have a notation for relating plaintext, ciphertext, and keys. We will use C = EK(P) to mean that the encryption of the plaintext P using key K gives the ciphertext C. Similarly, P = DK(C) represents the decryption of C to get the plaintext again.

Two Fundamental Cryptographic Principles:

Redundancy

The first principle is that all encrypted messages must contain some redundancy, that is, information not needed to understand the message.

Cryptographic principle 1: Messages must contain some redundancy

Freshness

 Cryptographic principle 2: Some method is needed to foil replay attacks

One such measure is including in every message a timestamp valid only for, say, 10 seconds. The receiver can then just keep messages around for 10 seconds, to compare newly arrived messages to previous ones to filter out duplicates. Messages older than 10 seconds can be thrown out, since any replays sent more than 10 seconds later will be rejected as too old.

Symmetric key E ncryption model:

                              Beyond that ,the security of conventional encryption depends on the secracy of the key ,not the secrecy of the algorithm. We do not need to keep the algorithm secret, we need to keep only the secret key.

                              The fact that the algorithm need not be kept secret means that manufactures can and have developed low cost chip implementations of data encryption algorithms. these chips are widely available and incorporated in to a number of products.



**Substitution Ciphers**

In a substitution cipher each letter or group of letters is replaced by another letter or group of letters to disguise it. One of the oldest known ciphers is the Caesar cipher, attributed to Julius Caesar. In this method, a becomes D, b becomes E, c becomes F,... , and z becomes C. For example, attack becomes DWWDFN.

The next improvement is to have each of the symbols in the plaintext, say, the 26 letters for simplicity, map onto some other letter. For example,

plaintext: a b c d e f g h i j k l m n o p q r s t u v w x y z

ciphertext: Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

**Transposition Ciphers**:Substitution ciphers preserve the order of the plaintext symbols but disguise them. Transposition ciphers, in contrast, reorder the letters but do not disguise them depicts a common transposition cipher, the columnar transposition.

**M  E  G  A  B  U  C  K**

**7    4   5   1   2   8  3    6**

W   E    L   C   O   M  E   T     **PLAIN TEXT**: WELCOME TO SAfire-2K8,CHIRALA,

O    S    A   f     i     r   e    2     PRAKASAM, AP.

 K   8    C   H    I    R  A  L      **CIPHER TEXT:** CfHAOiIKEeASES8PALACRPT2LA

A    P    R   A    K  A   S  A      WOKAMMrRA

M   A    P

 The cipher is keyed by a word or phrase not containing any repeated letters. In this example, MEGABUCK is the key. The purpose of the key is to number the columns, column 1 being under the key letter closest to the start of the alphabet, and so on. The plaintext is written horizontally, in rows, padded to fill the matrix if need be. The ciphertext is read out by columns, starting with the column whose key letter is the lowest.

Public key algorithm:

While there may be many algorithms and keys that have this property, the RSA algorithm (named after its founders, Ron Rivest, Adi Shamir, and Leonard Adleman) has become almost synonymous with public keycryptography.

In order to choose the public and private keys, one must do the following:

Choose two large prime numbers, p and q. How large should p and q be? The larger the values, the

more difficult it is to break RSA but the longer it takes to perform the encoding and decoding. RSA

Laboratories recommends that the product of p and q be on the order of 768 bits for personal use and

1024 bits for corporate use .

Compute n = pq and z = (p-1)(q-1).

Choose a number, e, less than n, which has no common factors (other than 1) with z. (In this case, e

and z are said to be relatively prime). The letter 'e' is used since this value will be used in encryption.

Find a number, d, such that ed -1 is exactly divisible (i.e., with no remainder) by z. The letter 'd' is

used because this value will be used in decryption. Put another way, given e, we choose d such that the

integer remainder when ed is divided by z is 1. (The integer remainder when an integer x is divided by

the integer n, is denoted x mod n).

The public key that Bob makes available to the world is the pair of numbers (n,e); his private key is the

pair of numbers (n,d).

key distribution: For symmetric key cryptograghy , the trusted intermediary is called a Key Distribution Center (KDC), which is a single, trusted network entity with whom one has established a shared secret key. We will see that one can use the KDC to

obtain the shared keys needed to communicate securely with all other network entities. For public key cryptography, the trusted intermediary is called a Certification Authority (CA). A certification authority certifies that a public key belongs to a particular entity (a person or a network entity). For a certified public key, if one can safely trust the CA that the certified the key, then one can be sure about to whom the public key belongs. Once a public key is certified, then it can be distributed from just about anywhere, including a public key server, a personal Web page or a diskette.

security in the layers:

Before getting into the solutions themselves, it is worth spending a few moments considering where in the protocol stack network security belongs. There is probably no one single place. Every layer has something to contribute.

 physical layer:In the physical layer wiretapping can be foiled by enclosing transmission lines in sealed tubes containing gas at high pressure. Any attempt to drill into a tube will release some gas, reducing the pressure and triggering an alarm. Some military systems use this technique.

 Data link layer:In this layer, packets on a point-to-point line can be encrypted as they leave one machine and decrypted as they enter another. All the details can be handled in the data link layer, with higher layers oblivious to what is going on. This solution breaks down when packets have to traverse multiple routers, however, because packets have to be decrypted at each router, leaving them vulnerable to attacks from within the router.

 Network layer:In this layer, firewalls can be installed to keep good packets and bad packets out. IP security also functions in this layer.

In the transport layer, entire connections can be encrypted, end to end, that is, process to process. For maximum security, end-to-end security is required . Finally, issues such as user authentication and nonrepudiation can only be handled in the application layer.

Since security does not fit neatly into any layer

Secure Internet Commerce :

SET (Secure Electronic Transactions) is a protocol specifically designed to secure payment-card transactions over the Internet. It was originally developed by Visa International and MasterCard International in February 1996 with participation from leading technology companies around the world .SET Secure Electronic Transaction LLC (commonly referred to as SET Co) was established in December 1997 as a legal entity to manage and promote the global adoption of SET



1. Bob indicates to Alice that he is interested in making a credit card purchase.

2. Alice sends the customer an invoice and a unique transaction identifier.

3. Alice sends Bob the merchant's certificate which includes the merchant's public key. Alice also sends the certificate for her bank, which includes the bank's public key. Both of these certificates are encrypted with the private key of a certifying authority.

4. Bob uses the certifying authority's public key to decrypt the two certificates. Bob now has Alice's public key and the bank's public key.

5. Bob generates two packages of information: the order information (OI) package and the purchase instructions (PI) package. The OI, destined for Alice, contains the transaction identifier and brand of card being used; it does not include Bob's card number. The PI, destined for Alice's bank, contains the transaction identifier, the card number and the purchase amount agreed to Bob. The OI and PI are dual encrypted: the OI is encrypted with Alice's public key; the PI is   encrypted with Alice's bank's public key. (We are bending the truth here in order to see the big picture. In reality, the OI and PI are encrypted with a customer-merchant session key and a customer-bank session key.) Bob sends the OI and the PI to Alice.



6.Alice generates an authorization request for the card payment request, which includes the transaction identifier.

7.Alice sends to her bank a message encrypted with the bank's public key. (Actually, a session key is used.) This message includes the authorization request, the PI package received from Bob, and Alice's certificate

.

8.Alice's bank receives the message and unravels it. The bank checks for tampering. It also make ssure that the transaction identifier in the authorization request matches the one in Bob's PI package.

9.Alice's bank then sends a request for payment authorization to Bob's payment-card bank through traditional bank-card channels -- just as Alice's bank would request authorization for any normal payment-card transaction.



  One of the key features of SET is the non-exposure of the credit number to the merchant. This feature is

provided in Step 5, in which the customer encrypts the credit card number with the bank's key.

Encrypting the number with the bank's key prevents the merchant from seeing the credit card. Note that

the SET protocol closely parallels the steps taken in a standard payment-card transaction. To handle all

the SET tasks, the customer will have a so-called digital wallet that runs the client-side of the SET

protocol and stores customer payment-card information (card number, expiration date, etc.)