NETWORK SECURITY AND CRYPTOGRAPHY

Rushikesh D. Bulbule

Department of Computer Science and Engineering, College of Engineering

Third Year Engineering Student

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 organization 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.

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?

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 and data messages (in much the same way that TCP senders and receivers exchange both control segments and data segments). All or some of these messages 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 hosts on 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

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.

Beyond that, the security of conventional encryption depends on the secrecy 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.