NETWORKING AND DATA SECURITY

***Nalini.L**
Asst.Prof, BMS College for Women,
Basavanagudi, Bengaluru-04

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 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".

Keywords: *Authentication, Integrity, Secrecy, Hacker, Non-repudiation,*

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, non-repudiation, 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. Non-repudiation deals with signatures.

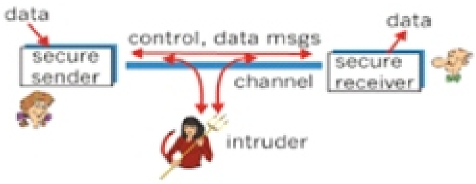
Secrecy: Only the sender and intended receiver should be able to understand the contents of the transmitted message. Because eavesdroppers may intercept the message, this necessarily requires that the message besomehow encrypted (disguise data) so that an intercepted message cannot be decrypted (understood) by an interceptor. This aspect of secrecy is probably the most commonly perceived meaning of the term "secure communication". 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 cannot "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 maliciously or by accident, in transmission. Extensions to the check summing techniques that we encountered in reliable transport and data link protocols.

Non-repudiation: Non-repudiation deals with signatures having established what we mean by secure communication; let us next consider exactly what is meant by an "insecure channel." 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 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.

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 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

Prevention

1. Prevention can be broken into two parts: approving security changes and monitoring security of your network.

Approving Security Changes

Security changes are defined as changes to network equipment that have a possible impact on the overall security of the network. Your security policy should identify specific security configuration requirements in non-technical terms. In other words, instead of defining a requirement as "No outside sources FTP connections will be permitted through the firewall", define the requirement as "Outside connections should not be able to retrieve files from the inside network". You'll need to define a unique set of requirements for your organization.

The security team should review the list of plain language requirements to identify specific network configuration or design issues that meet the requirements. Once the team has created the required network configuration changes to implement the security policy, you can apply these to any future configuration changes. While it's possible for the security team to review all changes, this process allows them to only review changes that pose enough risk to warrant special treatment.

Response

Response can be broken into three parts: security violations, restoration, and review.

Security Violations

When a violation is detected, the ability to protect network equipment, determine the extent of the intrusion, and recover normal operations depends on quick decisions. Having these decisions made ahead of time makes responding to an intrusion much more manageable.

The first action following the detection of an intrusion is the notification of the security team. Without a procedure in place, there will be considerable delay in getting the correct people to apply the correct response. Define a procedure in your security policy that is available 24 hours a day, 7 days a week.

Next you should define the level of authority given to the security team to make changes, and in what order the changes should be made. Possible corrective actions are:

- Implementing changes to prevent further access to the violation.
- Isolating the violated systems.
- Contacting the carrier or ISP in an attempt to trace the attack.
- Using recording devices to gather evidence.
- Disconnecting violated systems or the source of the violation.
- Contacting the police, or other government agencies.
- Shutting down violated systems.
- Restoring systems according to a prioritized list.
- Notifying internal managerial and legal personnel.

Restoration

Restoration of normal network operations is the final goal of any security violation response. Define in the security policy how you conduct, secure, and make available normal backups. As each system has its own means and procedures for backing up, the security policy should act as a meta-policy, detailing for each system the security conditions that require restoration from backup. If approval is required before restoration can be done, include the process for obtaining approval as well.

References

1. Network Security: History, Importance, and Future University of Florida Department of Electrical and Computer Engineering BhavyaDaya

2. Cisco IBSG, 2011.

3. U.S. Census Bureau, 2010; Forrester Research, 2003.

4. Wikipedia, 2010. 5. Sources: Cisco IBSG, 2010; U.S. Census Bureau, 2010. 6. While no one can predict the exact number of devices connected to the Internet at any given time, the methodology of applying a constant (Internet doubling in size every 5.32 years) to a generally agreed-upon number of connected devices at a point in time (500 million in 2003) provides an estimate that is appropriate for the purposes of this paper.

5. "Planetary Skin: A Global Platform for a New Era of Collaboration," Juan Carlos Castilla-Rubio and Simon Willis, Cisco IBSG, March2009,http://www.cisco.com/web/about/ac79/docs/pov/Planetary_Skin_POV_vFINAL_spw _jc_2.pdf

6. World Internet Stats: Usage and Population Statistics, June 30, 2010. 9. Sources: Cisco, 2010; HP, 2010.

7. 'Challenges in Management education- A teacher's perception'published in MSRIM JournalVol.III, Issue 2. July-Dec.2011. international refereed journal 'M S Ramaiah Management Review'