WHAT CAN BE DONE FROM THE BEJUCAL BASE BESIDES ELECTRONIC ESPIONAGE?

MANUEL CEREIJO

JUNE 2001

From the Bejucal base in Cuba, besides the listening to telecommunication channels in the United States, they can also produce attacks on the security of the United States' computer systems or networks. The general categories of attack are:

- Interruption: An asset of the system is destroyed or becomes unavailable or unusable. This is referred to as an attack on availability. Examples include destruction of a piece of hardware, such as a hard disk, the cutting of a communication line, or the disabling of the file management system.
- Interception: They get access to an asset. This is referred to as an attack on confidentiality. Example is the unauthorized copying of files or programs
- Modification: The attacker tampers with an asset. This is referred to as an attack on integrity. Examples include changing values in a data file, altering a program so that it performs differently, and modifying the content of messages being transmitted in a network
- Fabrication: The attacker inserts counterfeit objects into the system. This is referred to as an attack on authenticity. Examples include the insertion of spurious messages in a network or the addition of records to a file.

CATEGORIES OF ATTACKS

A useful categorization of these attacks is in terms of passive attacks and active attacks. Passive attacks are in the nature of monitoring of transmissions. The goal of the attacker is to obtain information that is being transmitted. Two types of passive attacks are(1) release of message content;(2) traffic analysis. A release of message content is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.

The second passive attack, traffic analysis, is more subtle. Suppose that we had a way of masking the contents of a message or other

information traffic so that Cuba, even if they capture the information, could not extract the real information because of the use of encryption. The attacker could after a period of time extract the information and messages, defeating the encryption process.

The second major category of attack is active attacks. These attacks involve some modification of the data stream or the creation of a false stream. It can be subdivided into four categories: masquerade, replay, modification of message, denial of service.

A masquerade takes place when the attacker, under certain entity, pretends to be a different entity, and therefore enabling an authorized entity to obtain extra privileges. Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

Modification of service simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. The denial of service prevents or inhibits the normal use or management of communications facilities. This is a very important and serious possible attack. It could disrupt an entire network, either by disabling the network or by overloading it with messages so as to degrade performance. The attacker could target airports, financial centers, power companies, dams control centers, etc. It is quite difficult to prevent active attacks. The goal is to detect them and to recover from any disruption or delays caused by them.

INTRUDERS

There are three classes of intruders:

- Masquerader: the intruder is not authorized to use the computer and penetrates a system's access controls to get inside. This can be done from the Bejucal base
- Misfeasor: A legitimate user who access data, programs, or resources for which is not authorized. This can be done by an insider, not from the Bejucal base
- Clandestine: the intruder seizes supervisory control of the system. Can be done from inside or from the Bejucal base

The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system. The intruder must acquired information that should have been protected. In most cases, this information is in the form of a password. The password file can be protected by one way encryption or by limiting the access control to the file. What are the most common techniques used so far to truy to break

into a system?

- Try words on the system's online dictionary
- Collect information about the users. Full names, spouses' names, children's names, pictures in their offices, books in their offices, etc (Here the operating personnel in Bejucal needs inside information)
- Users' phone numbers, social security numbers, room numbers, license plate numbers, etc (inside information is also needed)
- Use a Trojan horse
- Tap the line between a remote user and the host system

SUMMARY

Network security has assumed increasing importance. Individuals, corporations, government agencies, must heighten their awareness to protect data and messages, and to protect systems from network-based attacks. The disciplines of cryptography and network security have matured, leading to the development of practical, readily available applications to enforce network security.

Guaracabuya
Organo Oficial de la
Sociedad Económica de Amigos del País