St. Joseph's College of Engineering & Technology Palai

Department of Computer Science & Engineering

S8 CS

RT801 Security in Computing

Module 1

Security in Computing - Module 1

Syllabus

Introduction: Security basics, Aspects of network security

Attacks, Different types, Hackers, Crackers

Common intrusion techniques, Trojan Horse, Virus, Worm

Security services and mechanisms

Contents

1 Introduction

Computer security is the generic name for the collection of tools developed to protect data and to prevent hackers in computer systems.

With the introduction of computer networks, distributed systems and Internet, data is to be protected from when it is transported from one computer to a remote computer. Here comes the terms network security and Internet security.

Some examples of security violations are given below:

1. A user A sends a file to user B. User C, who is not authorised to read the file, is able to monitor the transmission.

2. User A sends a message to computer B. Before it reaches computer B, user C gets the message, modifies its contents and sends the file to computer B.

3. User C constructs its own message and sends it to computer B as if it had come from user A. Computer B receives the message as coming from user A.

4. An employee A is fired from a company without warning. The manager B sends a message to a server computer Cto invalidate employee A's account. When the invalidation is complete, server C needs to post a notice to employee A's file as confirmation. But employee A is able to intercept the message and delay it long enough to make a final access to the server to retrieve sensitive information.

5. A customer A sends a message to stock brocker B with instructions for various transactions. Immediately, the investments lose value and the customer denies sending the message.

Part I. Security Attacks

A security attack is an assault on system security that derives from an intelligent threat; ie, an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system. Security attacks are classified into,

passive attacks, and

active attacks.

2 Passive Attacks

A passive attack tries to learn or to use the information present in the computer system, but it does not affect system resources.

Thus passive attacks monitor the transmission of information. The goal of the attacker is to obtain information that is transmitted.

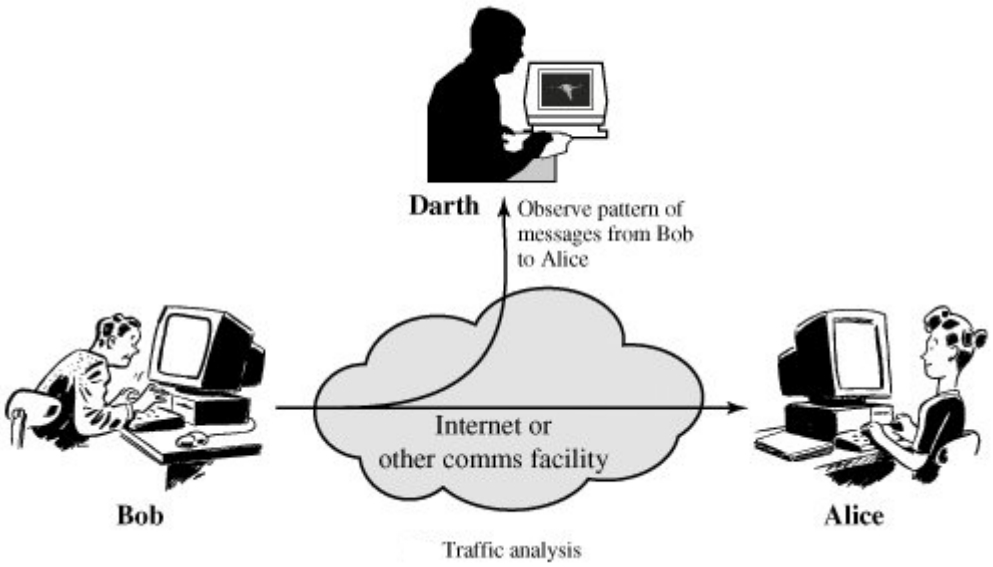
Two types of passive attacks are,

traffic analysis, and

release of message contents.

Traffic Analysis

Suppose we have a mechanism of masking (encrypt) the contents of a message before it is transmitted. A third person even if he got the message cannot extract the information from the message.

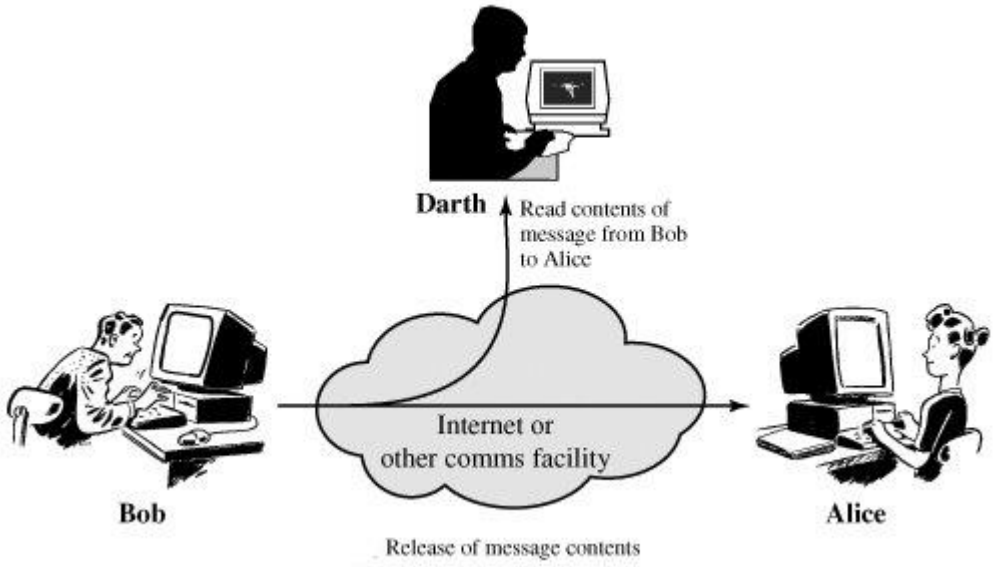


Traffic analysis

Even if we have this masking mechanism, the attacker can observe the pattern of the message. The attacker can find out the location and identity of computers in communication and can observe the frequency and length of messages being transmitted. Using this information, the nature of communication might be guessed.

Release of Message Contents

A telephone communication, email message, and a transferred file may contain sensitive information. Others may be able to see such message contents.



Release of message contents

It is very difficult to detect passive attacks. Normally the message is sent and received between sender and receiver. They do not know that a third party has read the messages or observed the traffic. But it is possible to prevent such attacks becoming successful by means of encryption.

3 Active Attacks

An active attack tries to change system resources and affect their operation. For example, an attacker changes the file contents of a computer system or deletes an entire file.

Thus active attacks involve modification of data or the creation of a false data stream. Active attacks are divided into 4 categories. They are,

masquerade,

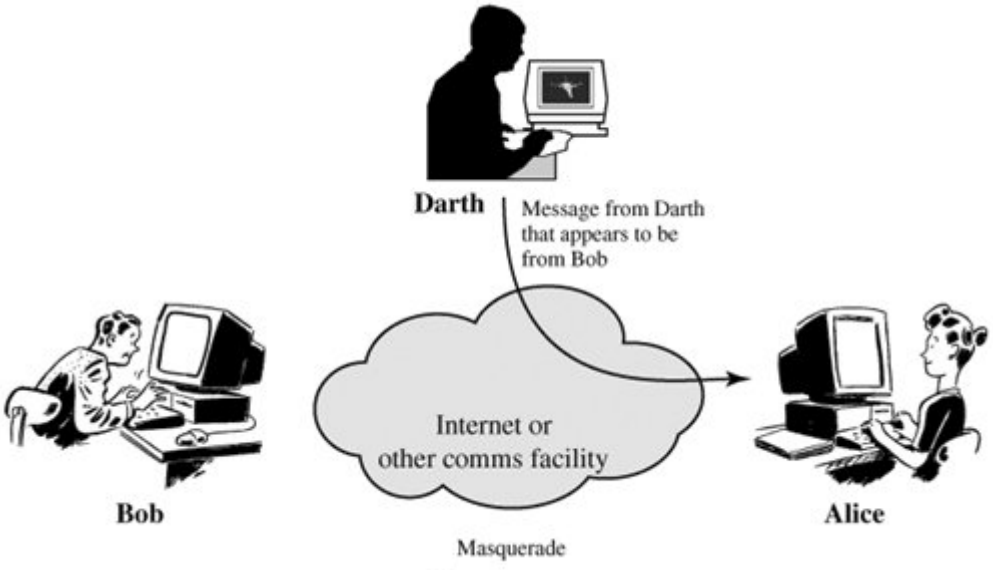
replay,

modification of messages, and

denial of service.

Masquerade

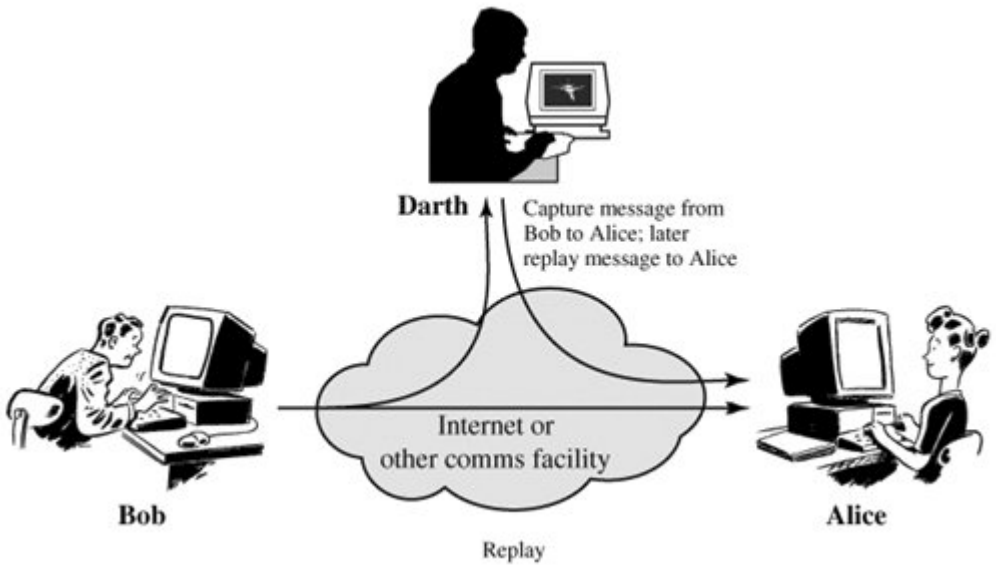
It takes place when one object pretends to be a different object as shown below:



Also authentication sequences (usser names and passwords) can be captured and replayed after a valid authentication has taken place.

Replay

It involves passive capture of a data unit and its subsequent retransmission as shown below:



Modification of Messages

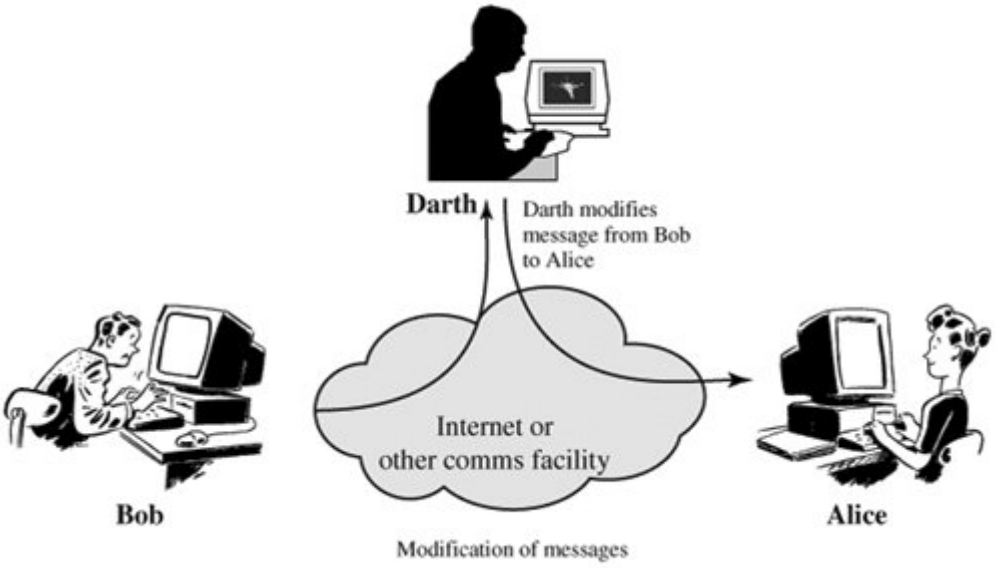
It means that some portion of a message is modified, or the message is delayed or reordered.

For example, a message such as

“Allow Richard Dunphy to read confidential file accounts”.

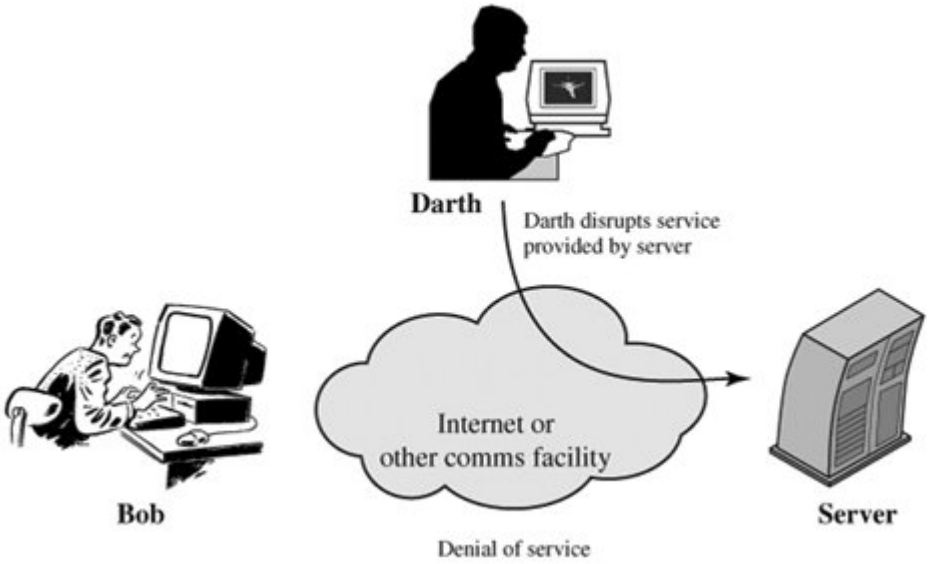
is modified as

”Allow Robert Dunphy to read confidential file accounts”.



Denial of Service

It prevents the normal use or management of communication facilities.



Here an attacker may suppress all messages directed to a particular destination or disrupts the entire computer network.

It is very difficult to prevent active attacks absolutely because of the wide variety of potential physical, software and network vulnerabilities.

4 Hackers

Hacking means finding out weaknesses in a system and exploiting them. Thus a computer hacker is a person who finds out weaknesses in the computer and exploits it. Now hackers have formed an open community.

Usually, hackers use aliases for the purpose of concealing identity, rather than revealing their names.

Hacker Groups and Conventions

Hackers are supported by regular gatherings called hacker conventions. Hacker groups provided access to information and resources, and a place to learn from other members.

Hacker conferences serve as meeting places for hackers and security experts. Common topics of discussion are wardriving, lockpicking, corporate and network security, personal rights and freedoms, new technologies.

4.1 Types of Hackers

Hackers are classified into different groups based on their attitudes. They are,

White hat,

Black hat,

Grey hat,

Elite hacker,

Script kiddie,

Neophyte,

Blue hat, and

Hacktivist.

White hat

A white hat hacker breaks security for non-malicious reasons. for example, they may break security to test their own security system. He is an ethical hacker. Thsi includes persons who perform penetration tests and vulnerability assesments. The international council of electronic commerce consultants has developed certifications, courseware, classes and online training covering the areas of ethical hacking.

Black hat

A black cat hacker violates computer security fro malicousness or for personal gain. They break into secure networks to destroy data or make network unusable for authorised persons to access the network.

Two preliminary steps performed by a black hat hacker to break a network are,

1. targeting, and
2. researc hand information gathering.

1. Targeting Here the hacker determines which network to break into. The hacker may scan the port through which computer receives data from network. Open ports will allow a hacker to access the system.

2. Research and information gathering In this stage, hacker visits the target system in hope of finding out vital information to access the system. This is done using social engineering, Dumpster Diving.

Dumpster Diving

Here hacker will look in the recycle bin (dumpster) in hopes to find documents that users have thrown away, which may contain information a hacker can use.

Grey hat

It is a hybrid of white hat and black cat hacker. A grey hat hacker may surf the Internet and hack into a system for notifying the admin that their system has been hacked.

Elite hacker

This means most skilled. An example for an elite group is Masters of Deception.

Script kiddie

It is a non-expert who breaks in to a computer system by using automated tools developed by others, with little understanding of the concept.

Neophyte

is someone who is new to hacking.

Blue hat

It is a hacker who is used to bug test a system prior to its launch looking for exploits so they can be closed.

Hacktivist

is a hacker who uses the technology to announce a social, religious or political message. This includes website defacements or denial of service.

4.2 Hacking Techniques

The techniques used by hackers to hack are,

Vulnerability Scanner

It is a tool used to quickly check computers on a network for knowing weaknesses. Hackers commonly use port scanners to see which ports on a computer are open.

Password Cracking

Here passwords are recovered from data that has been stored or transmitted by a computer system. An approach is to guess the password.

Packet Sniffer

It is an application that captures network layer packets which can be used to find passwords and other data.

Spoofing Attacks (Phishing)

Here a program or website or a computer system masquerade as another by falsifying data and thereby acts as a trusted system by a user or another program. This is done to fool programs, computer systems, or users into revealing confidential information such as passwords to the attacker.

Rootkit

Rootkit is a malicious software that may include replacements for system binaries so that it is impossible for the real user to detect the presence of the intruder on the system by checking process tables. This software hides the existence of certain processes or programs from normal methods of detection.

Social Engineering

One exampe for social engineering is that a black hat cracker contacts the system administrator and play the role of a user who cannot get access to the system. All the security devices and programs in the world won't keep an organisation safe if an employee gives away a password. A black hat hacker acts as an angry phone supervisor and attacks the person who

answers the phone with threats. Many people at this stage will accept hacker as supervisor and give them the received information.

A hacker can take advantage of a person who has some natural instinct to help someone with a problem.

Another way is that a hacker sends a fax or email to a user in hopes to get a response containing vital information.

Trojan Horses

Viruses

Worms

Keyloggers

It is a tool to record every keystroke on an affected machine. This allows the hacker to gain access to confidential information typed on the system.

5 Crackers

Software cracking is the modification of a software to remove or disable features which are considered undesirable by the person cracking software, usually a serial number, hardware key, date checks. Distribution and use of cracked copies is illegal in all nations.

Software companies, particularly gaming software have depended to complex measures to try to stop unauthorised copying of software.

A common software cracking method is the modification of an application's binary to prevent a specific key branch in the program's execution. This is done by reverse engineering the compiled program code using a debugger such as SoftICE, GDB etc.. until the software cracker reaches the function that contains the primary method of protecting the software. The binary is then modified using the debugger in a manner that replaced the earlier branching opcode with NOP opcode so the key branch will skip over it. Almost all software cracks are a variation of this type.

Software companies are developing methods such as code obfuscation, encryption and self modifying code to make this modification difficult. Even with these measures developers struggle to prevent software cracking.

An example for software crack is that removes the expiration period from a time limited trial of an application.

A mechanism is the use of a special kind of software such as CloneCD to detect the use of a copy protection application. After finding out it, another tool may be used to remove it from the software. This enables another program such as CloneDVD to copy the protected software to a user's hard disk.

Another mechanism is to decompile a program to access the original source code. This is possible with scripting languages and languages using JIT compilation.

An effect of software cracking is the release of fully operable proprietary software without any copy protection.

Password Cracking

It is the process of recovering passwords from data that are stored or sent by a computer system. A common approach is guessing.

Most password cracking methods require computers to produce many passwords using dictionary attacks, pattern checking, word list substitution.

Now tools are available that have the ability to test up to 2.8 billion passwords a second on an ordinary PC using a high end graphic processor.

Part II. Common Intrusion Techniques

The aim of the intruder is to gain access to the system. This requires to get the protected information. Normally, this information is in the form of a password. With the password, intruder can log onto the system.

In a computer system, a password file contains the password associated with each user. If this password file is stored without any protection, then it is easy to access this file. Password file can be protected in two ways.

Oneway Function

Based on the user's password, system stores only the value of a function. When the user enters the password, system converts the password and compares it with the stored value.

Access Control

Password file can be accessed by one or a very few accounts.

To bypass these protection mechanisms, intruders use the following techniques to learn passwords.

1. Try default passwords used with standard accounts.
2. Exhaustively try all short passwords (1 to 3 characters).
3. Try words in the system's online dictionary.
4. Collect information about users such as their family details, office details etc..
5. Try users' phone numbers, SSNs, room numbers etc..
6. Try all vehicle licence plate numbers for this state.
7. Use a Trojan horse to bypass restrictions on access.
8. Tap the line between user and computer system.

Normally, when an intruder enters a password by guessing, a computer can simply reject any login after 3 password attempts. So it is not practical to try more than a few passwords.

If the intruder is able to access the password file, then his strategy is to use the encryption mechanism of that computer system at leisure until a valid password is discovered.

Guessing attacks are feasible and highly effective when guesses can be attempted automatically.

Attack using Trojan Horse is dificult to prevent. An intruder may produce a game program and may invite the system operator to play the game. When the operator plays the game, but in the background a code to copy the password file may be present with the game program. Password file is copied to user.

Line tapping is a matter of physical security. It can be protected using link encryption techniques.

6 Trojan Horse

A Trojan horse is a useful program containing hidden code, when invoked performs some unwanted or harmful function.

Trojan horse programs can be used to attain functions indirectly that an intruder cannot attain directly. A user could create a Trojan horse program that when executed changes the invoking user's file permissions so that the files are readable by any user.

The created program is placed in a common folder and it is named such that it appears to be a useful utility. When user invokes the program, his file permissions are changed and the author gains access to the system.

An example of a Trojan Horse program is a compiler that has been modified to insert additional code into certain programs as they are compiled. For example, a system login program. the code creates a back door in the login program that permits the author to log on to the system with a special password. Such a Trojan Horse can never be discovered.

Another aim for Trojan horse is data destruction. the program seems to be performing a useful function, but it may be quietly deleting user's files.

7 Virus

Virus is a special piece of software that can infect other programs by modifying them; the modification includes a copy of the virus program. The resulting program can infect other programs.

Biological viruses are small pieces of genetic code that can take over the functioning of a living cell and trick it into making thousands of its replicas. Like this, a computer virus contains in its code for making perfect copies of itself. The virus becomes embedded in a program. Whenever the infected computer comes into contact with some software, a fresh copy of virus is passed into the new program. Thus infection can spread from one computer to another.

A virus can do anything that other programs do. A virus attaches itself to another program and executes secretly when the host program is run. When the virus starts execution, it performs functions such as erasing files and programs.

7.1 Phases of a Virus

A virus goes through the following four phases.

Dormant phase,

Propagation phase,

Triggering phase, and

Execution phase.

Dormant Phase

Virus is idle. The virus is eventually activated by some event, such as a date, presence of another program.

Propagation Phase

The virus places an identical copy itself into other programs or into certain system areas on the disk. Each infected program will now contain a copy of the virus.

Triggering Phase

The virus is activated. Triggering phase can be caused by some system event.

Execution Phase

The function is performed. Function may be harmless such as destruction of programs and data files.

7.2 Virus Structure

A virus can be attached to an executable program. When the infected program is called, it will execute the virus code and then execute the original copy of the program.

The general structure of a virus is shown below:

```
1234567;
V()
{
      goto main:
main: infect_executable();
      if( trigger_pulled == true)
            do_damage();
      goto next:

next:
 _
 _
 _
}

void infect_executable()
{
loop: file = get_random_file();
      if (first_line_of_file == 1234567)
            goto loop;
      else
            attach V() to file;
}

void trigger_pulled()
{
```

```
        if (<some condition>)
                return true;
}
```

Above program is a virus infected program. The infected program begins with the virus code.

First line of the file contains a marker (eg. 1234567) used by the virus to detect whether the program has already infected.

Second line jumps to the label 'main'. From there, infect_executable() function is called. This function finds out a file to infect.

Next, virus performs some action, if some condition holds. It calls trigger_pulled() function to check for a condition. If it returns true, do_damage() function performs some action.

Finally virus transfers control to the original program from label 'next'.

7.3 Types of Viruses

Diffferent categories of viruses are,

Parasitic virus,

Memory resident virus,

Boot sector virus,

Stealth virus,

Polymorphic virus, and

Metamorphic virus.

Parasitic virus

is the most common type. It attaches itself to executable files. It then replicates when the infected program is executed.

Memory resident virus

It enters in main memory as part of a resident system program. From there, it infects every program that executes.

Boot sector virus

It infects the master boot record or boot record and spreads when a system is booted from the disk containing virus.

Stealth virus

is explicitly designed to hide itself from antivirus software.

Polymorphic virus

With every infection, the virus mutates. It makes detection by signature impossible. This virus creates copies that perform same function but will have distinct bit patterns. Its aim is to evade detection by antivirus software. The signature of the

virus will vary with each copy. For this, a virus randomly insert instructions or interchange the order of instructions. virus may use encryption also.

Metamorphic virus

It also mutates with every infection. This virus rewrites itself completely at each iteration which increases the difficulty of detection. They change their behaviour as well as appearance.

Virus Creation Toolkit

This toolkit enables a person to create a number of different viruses quickly. These are less sophisticated than those designed from scratch.

Macro Viruses

It is a platform independent virus. Usually they infect microsoft word documents.

They infect documents, not executable code portions.

They are spread through emails.

Microsoft Office applications have macro facility. A macro is an executable program embedded in a word processing document or excel sheet. Usually users use macros in an excel sheet to automate repretitive tasks.

Email Viruses

These viruses are spread through emails. For example, a virus Melissa works as follows:

When a user opens an email attachment such as a word document, the macro stored with the document is activated. Then the virus sends itself to everyone in the user's mail list and does local damage.

More powerful versions of email viruses will get activated when the user just opens an email. This virus uses Visual Basic scripting language supported by the scripting package.

8 Worms

It is a program that replicates itself and send copies to various computers across a network. When it arrives, the worm may be activated and propagate again. also a worm may perform an unwanted function.

The difference between a virus and worm is that virus requires a human to move forward. But a worm without human intervention spread through computers.

To replicate itself, a worm uses a sort of network as a vehicle such as email, remote execution capability and remote login capability.

Email facility

A worm program makes a copy of itself to other systems.

Remote execution capability

A worm program executes a copy of itself in another system.

Remote login capability

A worm program logs on to a remote PC as a user and uses commands to perform functions.

The worm exhibits some features of a virus such as dormant phase, propagation phase, triggering phase and execution phase.

In a computer, a worm may disguise its presence by naming itself as a system process or using some other name.

8.1 Examples

Some examples for worms are,

Morrisworm (1998)

It was designed to spread on UNIX systems. When it gets executed, it discovers other computers that are allowed to be accessed by this computer. For each such computer, worm uses a number of methods to access:

a. It attempts to log on to the remote system as a legitimate user. Worm tries to crack the password files and finds usernames and passwords.

b. It exploited a bug in the finger protocol. Finger protocol is used to report the details of a remote user.

c. It exploited a trap door in the debug option of the remote process that receives and sends mails.

On success, worm communicates with the operating system command interpreter. It sends the interpreter a short bootstrap program. The boot strap program then calls back the parent program and downloads the rest of the worm program. The new worm is then executed.

Code Red Worm (2001)

It exploited a security hole in Microsoft IIS to penetrate and spread. It disables system file checker. One operation is that the worm initiated a denial of service attack by flooding a webserver with a large number of packets. The worm then enters the sleeping phase and reactivated periodically. It attacked around 360,000 servers in 12 hours.

Code Red II

is a worm that targeted IIS servers. In addition to Code Red's functionality, Code Red II allowed a hacker to direct activities of victim computers.

Nimda (2001)

is a worm spreads through emails, network shares, browsers etc.. It modifies web pages and certain executable files.

SQL Slammer Worm (2003)

It exploited a buffer overflow vulnerability in MS SQL Server.

Sobig.f worm (2003)

It exploited open proxy servers to turn computers to spam engines.

Mydoom (2004)

is an email worm. It installed a back door program in a computer and allowed hackers to gain remote access to passwords and credit card numbers.

8.2 State of the Art Worm Technology

Multiplatform

New worms are able to attack not only Windows machines but can attack a variety of platforms such as variants of UNIX systems.

Multiexploit

New worms penetrate against web servers, browsers, email, file sharing and different network applications.

Ultrafast spreading

New worms spread very fast across systems.

Polymorphic

Each copy of the worm has new code generated on the fly.

Metamorphic

They change their behaviour at different stages of propagation.

Transport Vehicles

Worms are ideal for spreading other distributed attack tools such as distributed denial of service zombies.

Zero Day Explicit

Worms exploit unknown vulnerabilities that are discovered only at the launch of a worm.

Part III. Security Services and Mechanisms

9 Security Services

A security service is a processing or communication service that is provided by a system to give a special kind of protection to system resources.

Security services are divided in to 5 categories:

1. Authentication Service,
2. Access Control Service,
3. Data Confidentiality Service,
4. Data Integrity Service, and
5. Non-repudiation Service.

9.1 Authentication Service

This service is concerned with assuring that a connection is authentic. Two authentication services are,

i. Peer entity authentication

Identity of the peer entity is checked at the establishment of or at times of data transfer of a connection.

ii. Data origin authentication

It checks for the source of a data unit. It supports applications like email where there are no prior interactions between sender and receiver.

9.2 Access Control Service

It is the ability to limit and control access to host systems and applications via communication links. For this, each object trying to get access needs to be identified or authenticated.

9.3 Data Confidentiality Service

It is the protection of transmitted data from passive attacks. Several levels of protection can be identified .

i. Connection confidentiality

protection of all user data on a connection.

ii. Connectionless confidentiality

protection of all user data in a single data block.

iii. Selective field confidentiality

confidentiality of selected fields within the user data.

iv. Traffic flow confidentiality

to protect information that can be generated from traffic flow analysis.

9.4 Data Integrity Service

This service is to assure that data received are exactly the data sent by an authorized object (no modification in data).

i. Connection integrity with recovery

It provides for integrity of data on a connection and detects any modification with recovery.

i. Connection integrity without recovery

It provides for integrity of data on a connection and detects any modification without recovery.

iii. Selective field connection integrity

It provides for the integrity of selective fields within the user data of a data block transferred over a connection.

iv. Connectionless integrity

It provides for the integrity of a single connectionless data block.

v. Selective field Connectionless integrity

It provides for the integrity of selcted fields within a single connectionless data block.

9.5 Non-repudiation Service

It prevents either sender or receiver from denying a transmitted message.

Non-repudiation- Origin

When a message is sent, the receiver can prove that sender has sent the message.

Non-repudiation- Destination

When a message is received, the sender can prove that receiver has received the message.

10 Security Mechanisms

Security mechanisms are classified into,

1. Specific Security Mechanisms, and
2. Pervasive Security Mechanisms.

1. Specific Security Mechanisms

They are implemented in specific protocol layer (TCP/IP or OSI).

2. Pervasive Security Mechanisms

They are not specific to any particular protocol layer or security service.

10.1 Specific Security Mechanisms

They are

Encipherment

It uses mathematical algorithms to transform data into another form. that is, it uses encryption.

Digitial signature

Here data is appended to a data unit that helps the receiver to prove the source and protect against forgery.

Access Control

It includes a number of mechanisms to enforce access rights to resources.

Data integrity

It includes a number of mechanisms to assure the integrity of a data unit.

Authentication exchange

It ensures the identity of an object by means of information exchange (username, password).

Traffic padding

Insert padded bits into different parts of a data stream.

Routing control

It enables selection of secure routes for certain data and allows routing changes.

Notarization

It uses a trusted third party to assure certain properties of a data exchange.

10.2 Pervasive Security Mechanisms

Trusted functionality

that which is percieved to be correct with respect to some criteria.

Security label

is a marking on a data unit that names the security attributes of that data unit.

Event detection

Detection of security relevant events.

Security audit trial

Security audit is an independent review and examination of system records and activities.

Security recovery

It takes recovery actions.

Questions

MGU/May2012

1. What is a virus (4marks)?

2. What are the common intrusion techniques (4marks)?

3a. Explain the different security services and mechanisms provided for network security.

OR

b. Explain briefly: i)Trojan Horse ii)Worm (12marks).

MGU/May2010

1. Mention the need for network security (4marks).

2. Discuss the term 'worm' (4marks).

3a. Discuss in detail about the different aspects of network security.

OR

b. Distinguish between hackers and crackers (12marks).

MGU/Nov2009

1. What are hackers? Explain (4marks).

2. Distinguish between virus and worms (4marks).

3a. Explain the different intrusion techniques.

OR

b. Describe the different types of attacks (12marks).

MGU/June 2009

1. Explain Trojan Horse (4marks).

2. List out some security mechanisms (4marks).

3a. Explain the different aspects of network security.

OR

b. Distinguish between Hackers and Crackers (12marks).

MGU/May2008

1. What is a virus (4marks)?

2. What are hackers (4marks)?

3a. Briefly describe the different security services and the different security mechanisms.

OR

b. Describe a typical model for network security (12marks).

MGU/Nov2008

1. Differentiate virus and worm (4marks).

2. What are crackers (4marks)?

3a. Describe the common intrusion techniques.

Or

b. Briefly describe about the different security attacks (12marks).

MGU/July2007

1. What are security services (4marks)?

2. Differentiate virus and worm (4marks).

3a. Explain a typical model for network security.

OR

b. Describe any three common intrusion techniques (12marks).

MGU/Jan2007

1. What are system security threats (4marks)?

2a. Explain the various aspects and meaning of computer security.

OR

b. Describe the various methods of defense in systems against computer crimes (12marks).

MGU/July2006

1. How to classify security services (4marks)?

2. Differentiate hackers and crackers (4marks).

3a. How will you classify that a software is of high quality? How do security aspects fit in the decimation of high quality?

OR

b. Explain common intrusion methods in computing systems (12marks).

References

.

Stallings, W(2006). Cryptography and Network Security. Pearson Education.

website: http://sites.google.com/site/sjcetcssz