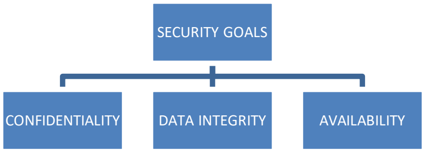
UNIT-1(C&NS)

Computer Security-generic name for the collection of tools designed to protect data and to thwart hackers

Network Security-measures to protect data during their transmission.This area covers the use of cryptographic algorithms in network protocols and network applications.

Cryptographic algorithms: This is the study of techniques for ensuring the secrecy and/or authenticity of information

SECURITY GOALS:



CONFEDENTIALITY:

- hiding information from an authorized access
- information while exchange should remain secret

DATA INTEGRITY:

- preventing information from un authorized modification
- need techniques to ensure the integrity of the data
    - preventing the modification
    - detect any modification made

AVAILABILITY:

- should be easily available to authorized users
- data must be available to authorized users

cryptographic algorithms are used to achieve the above goals

THE OSI SECURITY ARCHITECTURE

The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as

• **Security attack:** Any action that compromises the security of information owned by an organization.

• **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

• **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

SECURITY ATTACKS

Generic types of attacks

- Passive attacks
- Active attacks

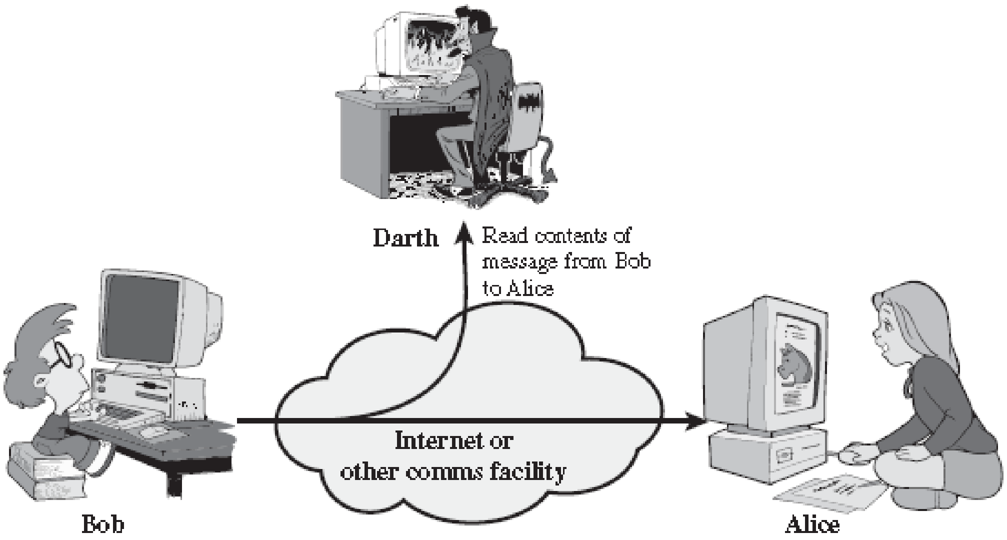
. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation.

Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are the release of message contents and traffic analysis.

1) **Release of message contents:**

The **release of message contents** is easily understood .A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.We would like to prevent an opponent from learning the contents of these transmissions.

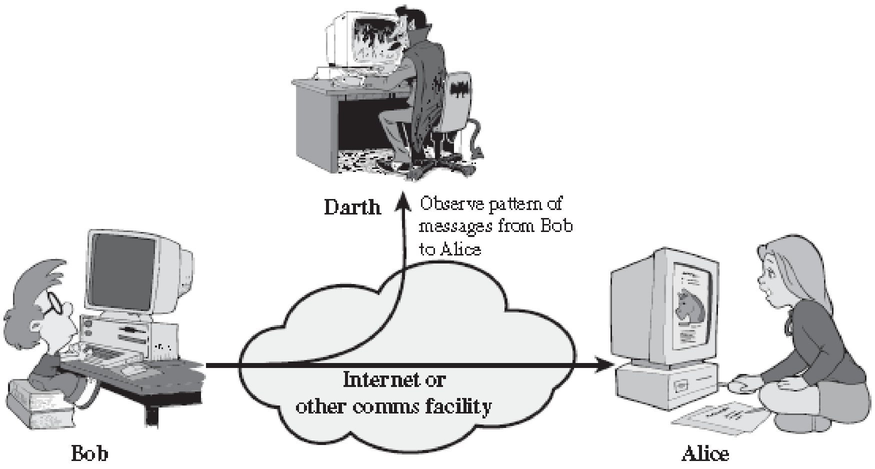

Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

(a) Release of message contents

2) **Traffic analysis:**

A second type of passive attack, **traffic analysis**, is subtler .Suppose that we had a way of masking the contents of messages or otherinformation traffic so that opponents, even if they captured the message, couldnot extract the information from the message. The common technique formasking contents is encryption. If we had encryption protection in place, anopponent might still be able to observe the pattern of these messages. Theopponent could determine the location and identity of communicating hosts andcould observe the frequency and length of messages being exchanged. Thisinformation might be useful in guessing the nature of the communication thatwas taking place.

Passive attacks are very difficult to detect, because they do not involve anyalteration of the data.


Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

(b) Traffic analysis

Active attack: An active attack attempts to alter system resources or affect their operation. Active attacks involve some modification of the data stream or the creation of a false stream.

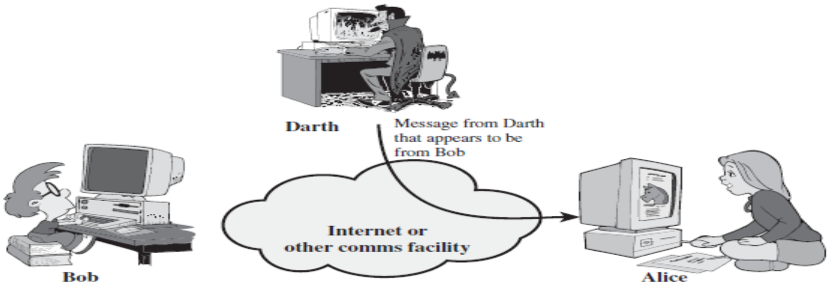
Active attacks can be subdivided into four categories:

- masquerade,
- replay,
- modification of messages, and
- Denial of service.

Masquerade:

A **masquerade** takes place when one entity pretends to be a different entity (Figure:). A masquerade attack usually includes one of the other forms of active attack.

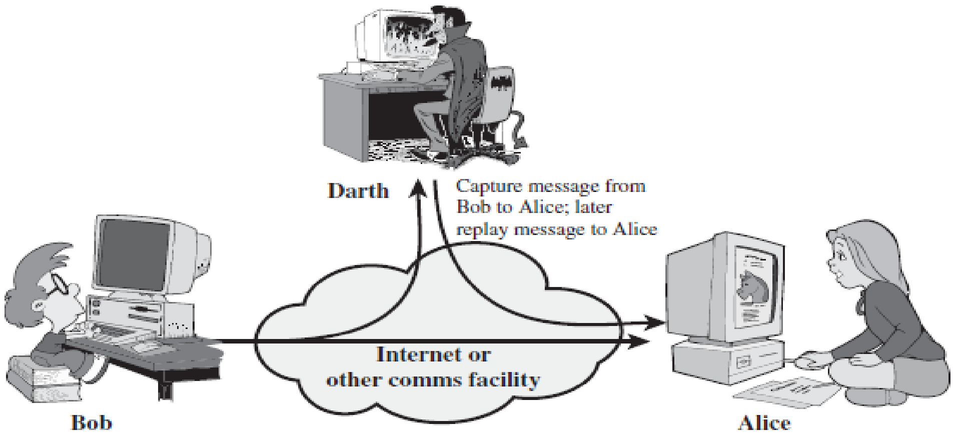
For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

(a) Masquerade

Replay :

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

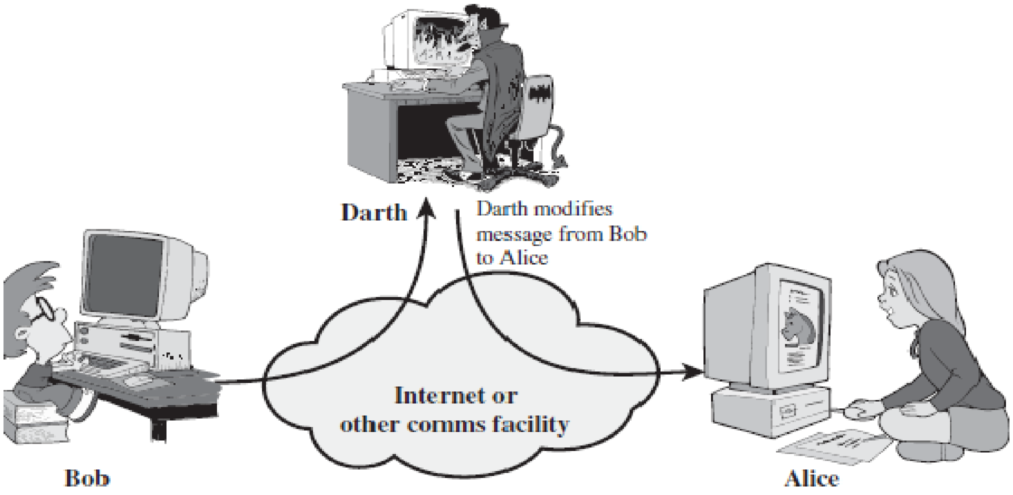

Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

(b) Replay

Modification of messages:

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (Figure: c).

For example, a message meaning “Allow John Smith to read confidential file accounts” is modified to mean “Allow Fred Brown to read confidential file accounts


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

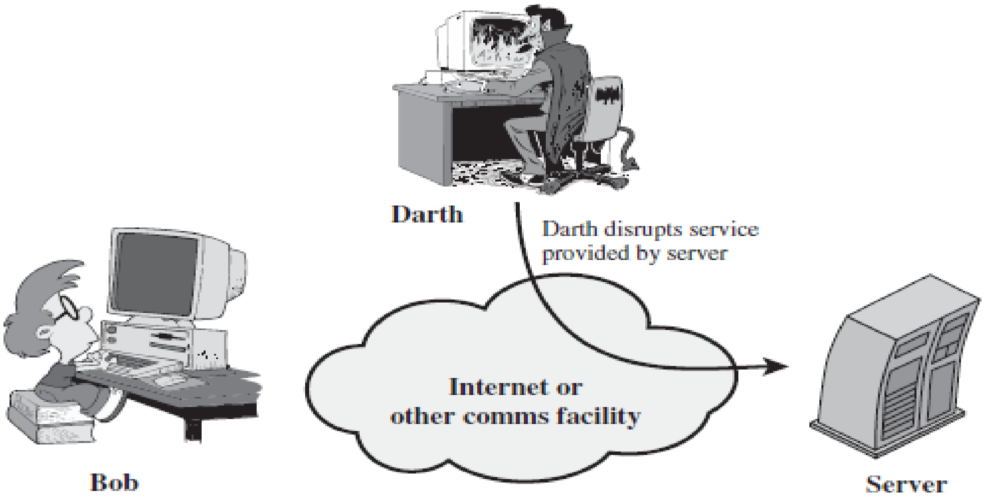
(c) Modification of messages

Denial of service:

The **denial of service** prevents or inhibits the normal use or management of communications facilities (Figure d). This attack may have a specific target;

For example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service).

Another form of service denial is the disruption of an entire network—either by disabling the network or by overloading it with messages so as to degrade performance


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

(d) Denial of service

1.7 SECURITY SERVICES

The classification of security services are as follows:

CONFIDENTIALITY: Ensures that the information in a computer system and transmittedinformation are accessible only for reading by authorized parties. Confidentiality is the protection of transmitted data from passive attacks. For example, when a TCP connection is set up between two systems, this broad protection prevents the release of any user data transmitted over the TCP connection.

Connection Confidentiality

The protection of all user data on a connection.

Connectionless Confidentiality

The protection of all user data in a single data block

Selective-Field Confidentiality

The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality

The protection of the information that might be derived from observation of traffic flows.

AUTHENTICATION: The authentication service is concerned with assuring that a communication is Authentic. The assurance that the communicating entity is the one that it claims to be. Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

Peer Entity Authentication

Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication

In a connectionless transfer, provides assurance that the source of received data is as claimed.

INTEGRITY: Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.

NON REPUDIATION: Requires that neither the sender nor the receiver of a message be able to deny the transmission. when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message

ACCESS CONTROL: Requires that access to information resources may be controlled by the target system . access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated

AVAILABILITY: Requires that computer system assets be available to authorized parties when needed

SECURITY MECHANISMS

One of the most specific security mechanisms in use is cryptographic techniques.

Encryption or encryption-like transformations of information are the most common means of providing security. Some of the mechanisms are

1 ENCIPHERMENT

2 DIGITAL SIGNATURE

3 ACCESS CONTROL

ENCIPHERMENT: It refers to the process of applying mathematical algorithms for converting data into a form that is not intelligible. This depends on algorithm used and encryption keys.

DIGITAL SIGNATURE: The appended data or a cryptographic transformation applied to any data unit allowing to prove the source and integrity of the data unit and protect against forgery.

ACCESS CONTROL: A variety of techniques used for enforcing access permissions to the system resources.

DATA INTEGRITY: A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

AUTHENTICATION EXCHANGE: A mechanism intended to ensure the identity of an entity by means of information exchange.

TRAFFIC PADDING: The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

ROUTING CONTROL: Enables selection of particular physically secure routes for certain data and allows routing changes once a breach of security is suspected.

NOTARIZATION: The use of a trusted third party to assure certain properties of a data exchange

GENERAL TERMS:

An original message is known as the **plaintext**, while the coded message is called the **ciphertext**.The process of converting from plaintext to ciphertext is known as **enciphering** or **encryption**; restoring the plaintext from the ciphertext is **deciphering** or **decryption**. The many schemes used for encryption constitute the area of study known as **cryptography**. Such a scheme is known as a **cryptographic system** or a **cipher**. Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of **cryptanalysis**. Cryptanalysis is what the layperson calls “breaking the code.”The areas of cryptography and cryptanalysis together are called **cryptology**.

SYMMETRIC CIPHER MODEL:

Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the same key. It is also known as conventional encryption. Symmetric encryption, also referred to as conventional encryption or single-key encryption.

A symmetric encryption scheme has five ingredients

• **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.

• **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.

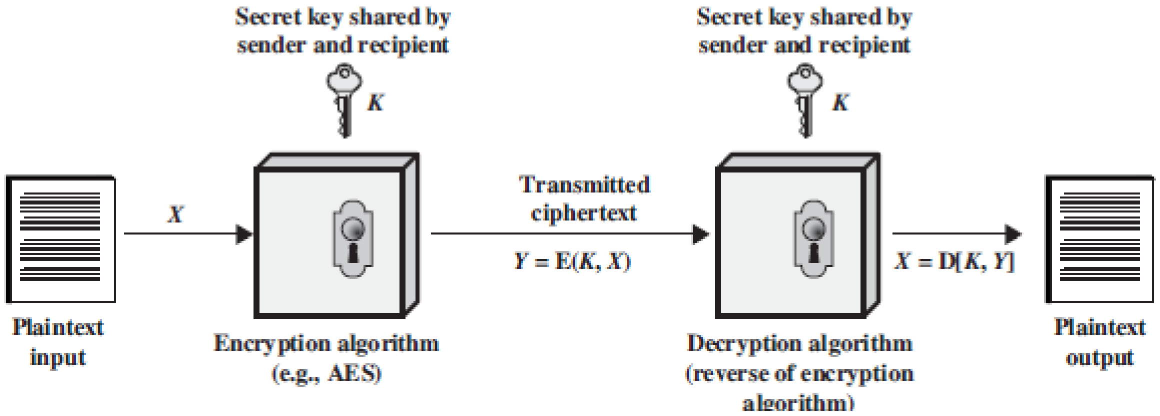
• **Secret key:** The secret key is also input to the encryption algorithm.The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time.The exact substitutions and transformations performed by the algorithm
depend on the key.

• **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. • **Decryption algorithm:** This is essentially the encryption algorithm run inreverse. It takes the ciphertext and the secret key and produces the originalplaintext.

There are two requirements for secure use of conventional encryption:

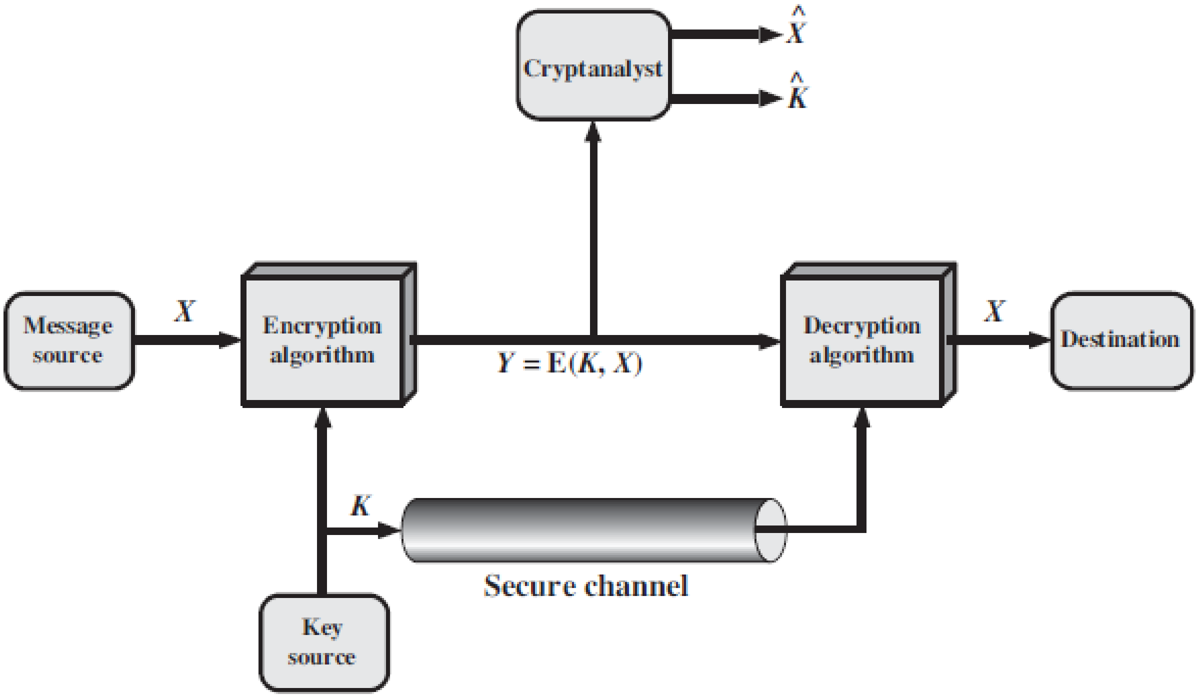
1. We need a strong encryption algorithm. At a minimum, we would like thealgorithm to be such that an opponent who knows the algorithm and hasaccess to one or more ciphertexts would be unable to decipher the ciphertextor figure out the key.

2.Sender and receiver must have obtained copies of the secret key in a securefashion and must keep the key secure.


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Simplified Model of Symmetric Encryption

Let us take a closer look at the essential elements of a symmetric encryption scheme, using below Figure. A source produces a message in plaintext, . The elements of are letters in some finite alphabet. Traditionally, the alphabet usually consisted of the 26 capital letters. Nowadays,the binary alphabet {0, 1} is typically used. For encryption, a key of the form is generated. If the key is generated at the message source, then it must also be provided to the destination by means of some secure channel. Alternatively, a third party could generate the key and securely deliver it toboth source and destination



Model of Symmetric Cryptosystem

With the message and the encryption key as input, the encryption algorithm forms the ciphertext .We can write this as This notation indicates that is produced by using encryption algorithm E as a function of the plaintext , with the specific function determined by the value of the key .

The intended receiver, in possession of the key, is able to invert the transformation:

$$X=D(K,Y)$$

Cryptographic systems are characterized along three independent dimensions:

1. The type of operations used for transforming plaintext to ciphertext. All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost (that is, that all operations are reversible).

2. The number of keys used. If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.

3. The way in which the plaintext is processed. A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

SUBSTITUTION TECHNIQUES

1)Caesar cipher (or) shift cipher

The earliest known use of a substitution cipher and the simplest was by Julius Caesar. TheCaesar cipher involves replacing each letter of the alphabet with the letter standing 3 placesfurther down the alphabet.

plain: meet me after the toga party

cipher: PHHW PH DIWHU WKH WRJD SDUWB

Note that the alphabet is wrapped around, so that letter following „z" is „a".

Then the algorithm can be expressed as follows. For each plaintext letter , substitute

The cipher text letter

$$C = E(3, p) = (p + 3) \bmod 26$$

A shift may be of any amount, so that the general Caesar algorithm is

$$C = E(k, p) = (p + k) \bmod 26$$

Where K takes on a value in the range 1 to 25.The decryption algorithm is simply

$$p = D(k, C) = (C - k) \bmod 26$$

Drawbacks

- There are only 25 keys totry.
- The language of the plaintext is known and easily recognizable

2)Monoalphabetic Ciphers:

With only 25 possible keys, the Caesar cipher is far from secure. A dramatic increase in the key space can be achieved by allowing an arbitrary substitution. Before proceeding, we define the term permutation. A **permutation** of a finite set of elements is an ordered sequence of all the elements of , with each element appearing exactly once. For example, if , S = {a, b, c} there are six permutations of S :

abc, acb, bac, bca, cab, cba

In general, there are 3! permutations of a set of elements, because the first element can be chosen in one of n ways, the second in ways, the third in ways, and so on.

Recall the assignment for the Caesar cipher:

plain: 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

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

If, instead, the "cipher" line can be any permutation of the 26 alphabetic characters, then there are 26! or greater than $4 * 10^{26}$ possible keys.

Such an approach is referred to as a **monoalphabetic substitution cipher**, because a single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message.

3)Playfair Cipher

The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertextdigrams. The Playfair algorithm is based on the use of a 5 □□5 matrix of letters constructed using a keyword.

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

In this case, the keyword is *monarchy*. The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom,and then filling in the remainder of the matrix with the remaining letters in alphabetic order. The letters I and J count as one letter. Plaintext is encrypted two letters at a time, according to the following rules:

1. Repeating plaintext letters that are in the same pair are separated with a fillerletter, such as x, so that balloon would be treated as ba lx lo on.

2. Two plaintext letters that fall in the same row of the matrix are each replaced bythe letter to the right, with the first element of the row circularly following thelast. For example, ar is encrypted as RM.

3. Two plaintext letters that fall in the same column are each replaced by the letterbeneath, with the top element of the column circularly following the last. Forexample, mu is encrypted as CM.

4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in itsown row and the column occupied by the other plaintext letter. Thus, hsbecomes BP and ea becomes IM (or JM, as the encipherer wishes).

example

Plaintext = meet me at the school house

Splitting two letters as a unit => me et me at thesch oxolho us ex

Corresponding cipher text => CL KL CL RS PD IL HY AV MP HF XL IU

Strength of playfair cipher

Playfair cipher is a great advance over simple mono alphabetic ciphers. Since there are 26 letters, 26x26 = 676 diagrams are possible, so identification of individual diagram is more difficult.

4)Polyalphabetic ciphers

a)Vigenere cipher:

To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword. For example, if the keyword is **deceptive**, the message “we are discovered save yourself” is encrypted as

Key : deceptivedeceptivedeceptive

plaintext: wearediscoveredsaveyourself

ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Expressed numerically, we have the following result.

Key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
Plaintext	22	4	0	17	4	3	8	18	2	14	21	4	17	4
ciphertext	25	8	2	21	19	22	16	13	6	17	25	6	21	19

Key	19	8	21	4	3	4	2	4	15	19	8	21	4	
Plaintext	3	18	0	21	4	24	14	20	17	18	4	11	5	
ciphertext	22	0	21	25	7	2	16	24	6	11	12	6	9	

Strength of Vigenere cipher

- There are multiple cipher text letters for each plaintext letter.
- Letter frequency information is obscured.

b)Vernam cipher

Theultimatedefenseagainstsuchacryptanalysisistochooseakeywordthatisaslongastheplaintextandhasnostatisticalrelationshiptoit.SuchasystemwasintroducedbyanAT&TengineernamedGilbertVernamin1918.Hissystemworksonbinarydata(bits)ratherthanletters.Thesystemcanbeexpressedsuccinctly as follows

$$c_i = p_i \oplus k_i$$

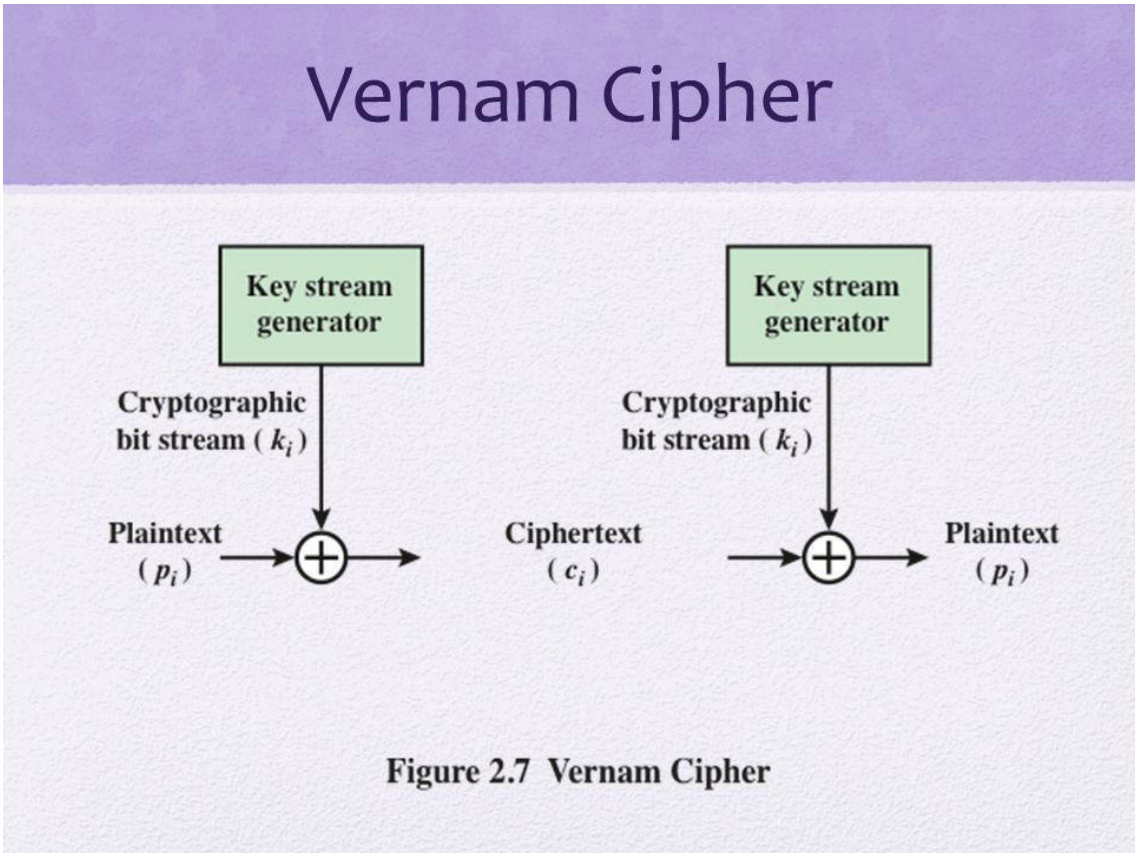
where

p_i=ithbinarydigitofplaintext

k_i =ithbinary digit ofkey

c_i =ithbinary digit ofciphertext

$\oplus$ = exclusive-or (XOR)operation



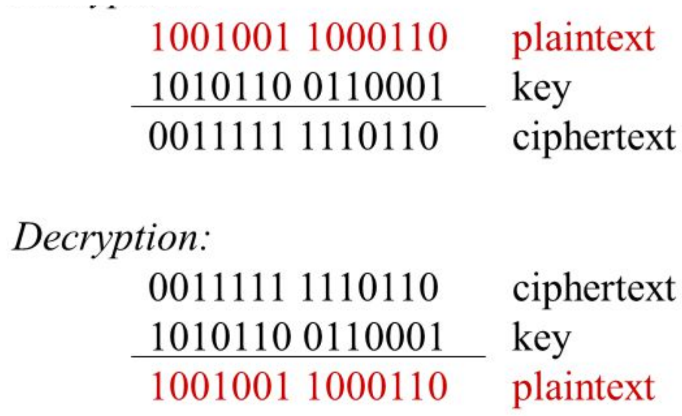
Vernam Cipher

Figure 2.7 Vernam Cipher

Thus, the ciphertext is generated by performing the bitwise XOR of the plaintext and the key. Because of the properties of the XOR, decryption simply involves the same bitwise operation:

$$p_i = c_i \oplus k_i$$

Example :



1001001 1000110	plaintext
1010110 0110001	key
0011111 1110110	ciphertext

Decryption:

0011111 1110110	ciphertext
1010110 0110001	key
1001001 1000110	plaintext

c)One Time Pad:

It is an unbreakable cryptosystem. The key is of same length as the message. Once a key is used, it is discarded and never used again.

An example should illustrate our point. Suppose that we are using a Vigenère scheme with 27 characters in which the twenty-seventh character is the space character, but with a one-time key that is as long as the message. Consider the ciphertext

ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

We now show two different decryptions using two different keys:

ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

key: PXLMVMSYDOFUYRVZWCTNLEBNECVGDUPAHFZZLMNYIH

plaintext: MR MUSTARD WITH THE CANDLESTICK IN THE HALL

ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

key: MFUGPMIYDGAXGOUFHKLLLMHSQDQOGTEWBQFGYOVUHWT

plaintext: MISS SCARLET WITH THE KNIFE IN THE LIBRARY

Suppose that a cryptanalyst had managed to find these two keys.Twopausible plaintexts are produced. How is the cryptanalyst to decide which is the correct decryption?

TRANSPOSITION TECHNIQUES:

a) Rail fence

Rail fenceis simplest of such cipher, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

For example, to encipher the message “meet me after the toga party” with a rail fence of depth 2, we write the following:

m e m a t r h t g p r y

e t e f e t e o a a t

The encrypted message is

MEMATRHTGPRYETEFETEOAAT

b) Row Transposition Ciphers:

A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of columns then becomes the key of the algorithm.

For example,

Key: 4 3 1 2 5 6 7
Plaintext: a t t a c k p
o s t p o n e
d u n t i l t
w o a m x y z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext.

Buffer Overflow & Format String Vulnerabilities

Vulnerability: Vulnerability is an inherent weakness in design, configuration, implementation ormanagement of a network or system that renders it susceptible to a threat. Vulnerabilities are what make networks susceptible to information loss and downtime. Every network and system has some kind of vulnerability.

Buffer Overflow: A buffer overflow occurs when a program or process tries to store moredata in a buffer than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Though this may occur accidentally because of a programming error, at present it is an increasingly common type of security attack on integrity.

It happens when the attacker intentionally enters more data than a program was written to handle. The data runs over and overflows the section of valid data like part of programming instructions, user files, confidential information etcthere by enabling the attacker’s data to overwrite it. This allows an attacker to overwrite data that controls the program and can take over control of the program to execute the attacker’s code instead of programmer’s code.

Example:

```
#include<stdio.h>
#include<conio.h>
```

```
#include<strings.h>
int main(intargc,char *argv[])
{
        Overflow_finction(*++argv);
        Return (0);
}

Void Overflow_finction(char *b)
{
        Char c[8];
        Syrcpy(c,b);
        Return;
}
```

In this C program, we can see the use of the **strcpy**function.data is taken from argv[1].then copid into array of 8 bytes.since no size checking is performed on either variable,ehich results in a buffer over flow.

Example 2:

```
#include<stdio.h>
#include<conio.h>
#include<strings.h>
int main()
{
        Char buffer[8];          /*an 8 charecter buffer */
        Strcpy(buffer,"AAAAAAAAAAAAAAAAAAAA")
                                                        /*copy 20 bytes of A into the buffer*/
                                                       /*this will cause stack corruption*/
Return 1;
}
```

A SAMPLING OF PROBLEMATIC FUNCTIONS IN C

1)STRCPY(dest,src)   this function will copy a string from source to destination

2)strcat(dest,src)   this function adds a string to the end of another string in a buffer

3)gets(buffer)   gets a string of input from the stdin stream and stores it in buffer

Consequences

- Availability: Buffer overflows generally lead to crashes. Other attacks leading to lack of availability are possible, including putting the program into an infinite loop.
- Access control (instruction processing): Buffer overflows often can be used to execute arbitrary code which is usually outside the scope of a program's implicit security policy

Defences

- To minimise the chance of a successful BOF exploit,the programmer could develop his application in atype safe language such as Java or C#
- One recommendation is to avoid the use of dangerous functions such as strcpy(),and sprint();

FORMAT STRING VULNERABILITY

A format string vulnerability occurs when programmers pass externally supplied data to a *printf*function as or as part of the format string argument.

Format string attacks can be used to crash a program or to execute harmful code. The problem stems from the use of unfiltered user input as the format string parameter in certain C functions that perform formatting, such as printf().

A malicious user may use the %s and %x format tokens, among others, to print data from the stack or possibly other locations in memory

List of standard printf functions in C

The below functions can lead to format string vulnerability if misused

1)printf()-this function allows a formatted string to be created and written to the standard I/O stream

2)fprintf()-this function allows a formatted string to be created and written to a FILE I/O stream

3)sprint()-this function allows a formatted string to be created and written to a location in memory

4)snprintf()-this function allows a formatted string to be created and written to a location in memory with maximum string size

EXAMPLE:

```
#include<stdio.h>

#include<conio.h>

void main(intargc, char **argv)

{

        char *s;

        char *c1="This is secret one!";

        char *c1="this is  secret two";

        clrscr();

        printf("enter a string");

        scanf("%s",s);

printf("the string you entered is");

        printf(s);

        getch();

}
```

```
Ouput1:enter a string  hi

        the string you entered is          hi

Ouput2:enter a string  %S
```

```
          the string you entered is          this is  secret two

Ouput3:enter a string  %S %S

          the string you entered is          this is  secret two this is  secret one
```

Format string vulnerability attacks fall into three categories: denial of service, reading and writing.

Format string vulnerability denial of service attacks are characterized by utilizing multiple instances of the %s format specifier to read data off of the stack until the program attempts to read data from an illegal address, which will cause the program to crash.

Format string vulnerability reading attacks typically utilize the %x format specifier to print sections of memory that we do not normally have access to. This is a serious problem and can lead to disclosure of sensitive information.

PHISHING AND DEFENSIVE MEASURES

Phishing is a fraudulent process, which attempts to acquire sensitive information, such as usernames, passwords, credit card numbers, and SSNs, by masquerading as a trustworthy entity in an electronic communication. Spear-phishing emails have a high success rate because they mimic messages from an authoritative source, such as a financial institution, a communications company, or some other easily recognizable entity with a reputable brand.

Pharming is yet another technique in which the DNS tables are poisoned so that a victim's address, e.g., www.amazon.com, points to the phishing site.

DEFENSES

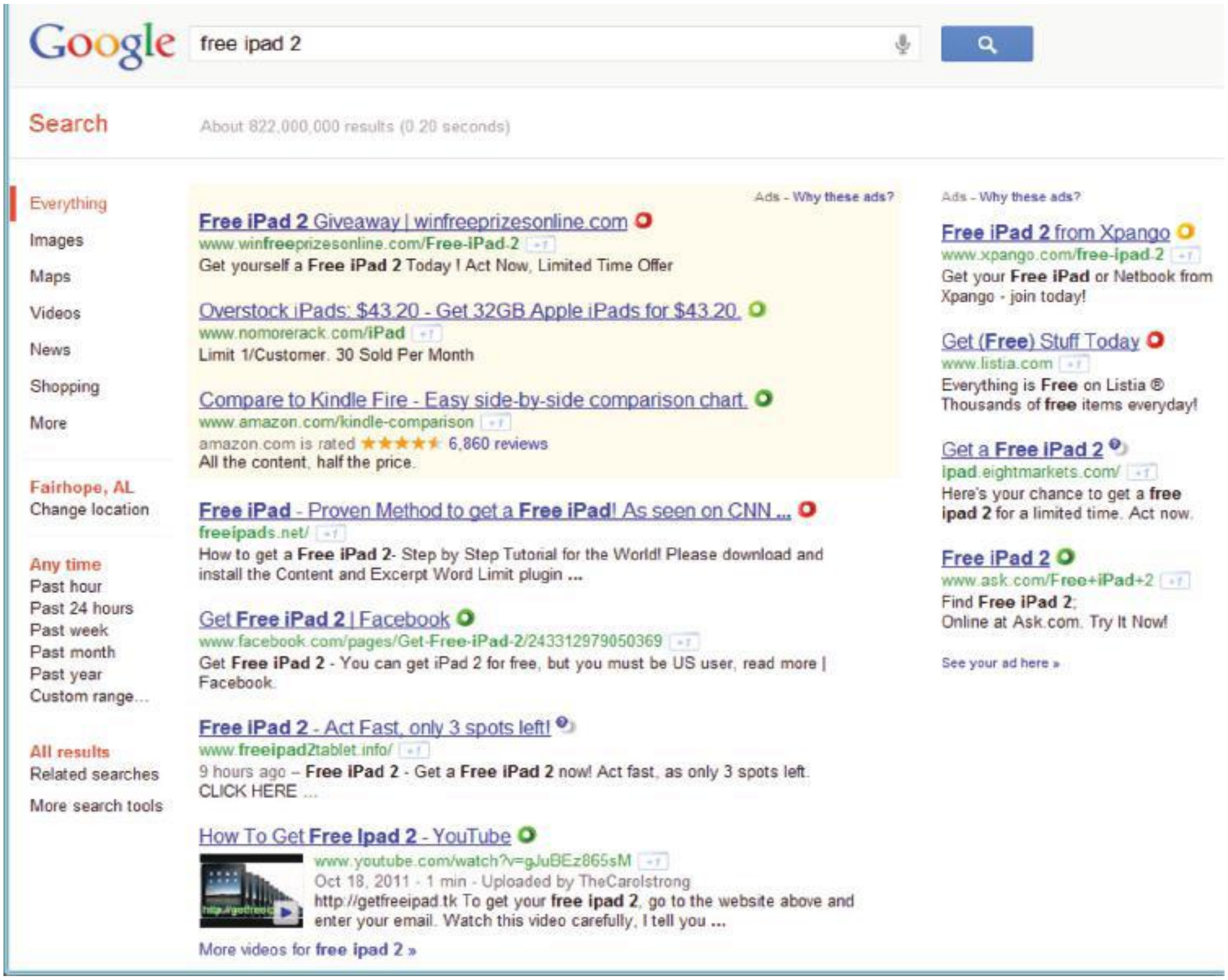
1)safe browsing tool

Since the web is the most frequently used attack vector, it is important to have protection for browsers, especially when a search is used

Example :The Web of Trust (WOT) Plugin for Safe Browsing

The WOT is a community-based collection of websites, based on a reputation achieved through the ratings of millions of users. It is a free safe surfing plugin for major browsers and provides website ratings and reviews to help web users as they search, surf and shop online. WOT uses color-coded symbols to show the reputation of a site: Green indicates the site is trusted by the community, yellow warns a user to be cautious and red indicates potential danger. A gray symbol with a question mark means that there is no rating due to a lack of sufficient data.

When a “hot” keyword like free ipad is used in the search, Figure 26.14 illustrates theratings for the websites found



About 822,000,000 results (0.20 seconds)

Ads - Why these ads?

Free iPad 2 Giveaway | winfreeprizesonline.com
www.winfreeprizesonline.com/**Free-iPad-2**
Get yourself a **Free iPad 2** Today ! Act Now, Limited Time Offer

Overstock iPads: $43.20 - Get 32GB Apple iPads for $43.20.
www.nomorerack.com/**iPad**
Limit 1/Customer. 30 Sold Per Month

Compare to Kindle Fire - Easy side-by-side comparison chart.
www.amazon.com/kindle-comparison
amazon.com is rated ★★★★★ 6,860 reviews
All the content, half the price.

Free iPad - Proven Method to get a **Free iPad**! As seen on CNN ...
freeipads.net/
How to get a **Free iPad 2**- Step by Step Tutorial for the World! Please download and install the Content and Excerpt Word Limit plugin ...

Get **Free iPad 2** | Facebook
www.facebook.com/pages/Get-**Free-iPad-2**/243312979050369
Get **Free iPad 2** - You can get iPad 2 for free, but you must be US user, read more | Facebook.

Free iPad 2 - Act Fast, only 3 spots left!
www.**freeipad2**tablet.info/
9 hours ago – **Free iPad 2** - Get a **Free iPad 2** now! Act fast, as only 3 spots left. CLICK HERE ...

How To Get **Free Ipad 2** - YouTube
www.youtube.com/watch?v=gJuBEz865sM
Oct 18, 2011 - 1 min - Uploaded by TheCarolstrong
http://getfreeipad.tk To get your **free ipad 2**, go to the website above and enter your email. Watch this video carefully, I tell you ...
More videos for **free ipad 2** »

Ads - Why these ads?

Free iPad 2 from Xpango
www.xpango.com/**free-ipad-2**
Get your **Free iPad** or Netbook from Xpango - join today!

Get (**Free**) Stuff Today
www.listia.com
Everything is **Free** on Listia ®
Thousands of **free** items everyday!

Get a **Free iPad 2**
ipad.eightmarkets.com/
Here's your chance to get a **free ipad 2** for a limited time. Act now.

Free iPad 2
www.ask.com/**Free+iPad+2**
Find **Free iPad 2**;
Online at Ask.com. Try It Now!

See your ad here »

Figure 26.14

2)uniform resource locator (url) filtering

Both Internet Explorer (IE), Chrome, and Firefox provide phishing filters. Phishing and malware protection is accomplished by checking the site that is being visited against lists of reported phishing and malware sites. These lists are automatically downloaded and updated by browsers.

Example: The Location of a List of Phishing Sites

PhishTank (http://www.phishtank.com/) is a collaborative clearing house for data and information about phishing on the Internet

3)**the obfuscated url and the redirection technique**

Two of the most common techniques employed in phishing are the confusing/obfuscated URL and the redirection technique. For example, the following URLs appear to be an ebay site since ebay is prominently displayed in the listing.

http://ebay.hut2.ru

4) education and awareness

5)anti –phishing software

WEB-BASED ATTACKS

The vulnerabilities in web-based attacks are manifested in a variety of ways. For example, the inadequate validation of user input may occur in one of the following attacks: Cross-Site Scripting (XSS or CSS) HTTP Response Splitting or SQL Injection

1) web service protection

Web services based on the eXtensible Markup Language (XML), Simple Object Access Protocol (SOAP), and related open standards that are deployed in Service Oriented Architectures (SOAs) allow data and applications to interact without human intervention through dynamic and ad hoc connections.

2)attack kits

Unfortunately, there are a number of attack kits that although illegal, can be purchased on the black market.

A short description of several of these attack kits will provide an indication of their capabilities as shown in Table

Black Market Attack Kits

Attack kit type	**Average price**	**Price range**
Botnet	$225	$150–$300
Autorooter	$70	$40–$100
SQL injection tools	$63	$15–$150

3)http response splitting attacks

HTTP response splitting attacks may happen where the server script embeds user data in HTTP response headers without appropriate sanitation

4)cross-site request forgery (csrf or xsrf)

A Cross-Site Request Forgery attack [28] tricks the victim’s browser into issuing a command to a vulnerable web application. Vulnerability is caused by browsers

5)clickjacking

The technique works by hiding malicious link/scripts under the cover of the content of a legitimate site. Buttons on a website actually contain invisible links, placed there by the attacker. So, an individual who clicks on an object they can visually see, is actually being duped into visiting a malicious page or executing a malicious script. When mouseover is used together with clickjaking, the outcome is devastating. Facebook users have been hit by a clickjacking attack, which tricks people into "liking" a particular Facebook page, thus enabling the attack to spread .

STRUCTURED QUERY LANGUAGE (SQL) INJECTION ATTACKS

SQL injection is a technique where malicious users can inject SQL commands into an SQL statement, via web page input.

SQL injection is the top vulnerability of websites. It exploits improper input validation in database queries. A successful exploit will allow attackers to access, modify, or delete information in the database. It permits attackers to steal sensitive information stored within the backend databases of affected websites, which may include such things as user credentials, email addresses, personal information, and credit card numbers

Example 26.39: The Manner in Which to Execute a SQL Injection Attack

As an example of a SQL injection attack, consider the normal user login request shown in Figure 26.38. A user supplies their username and password, and this SQL query checks to see if the user/password combination is in the database. The query is of the form

$query = "SELECT username,password FROM login WHERE username ='$username' AND password = '$password'";

The attacker wants to take over the administrative privilege of the database and therefore uses the user name: administrator'#, as indicated in Figure 26.39. The # sign indicatesthe start of a line comment, which although generally useful can typically be ignored. The password can be anything, since the server will ignore anything that follows the # sign. The form of the query and the ignored comment, indicated by the strikethrough, are then

$query = "SELECT username,password FROM login WHERE username ='administrator'# AND password = '$password'";

Through the use of this approach, the attacker gains administrator privilege by dropping the password verification, as indicated in Figure 26.40.

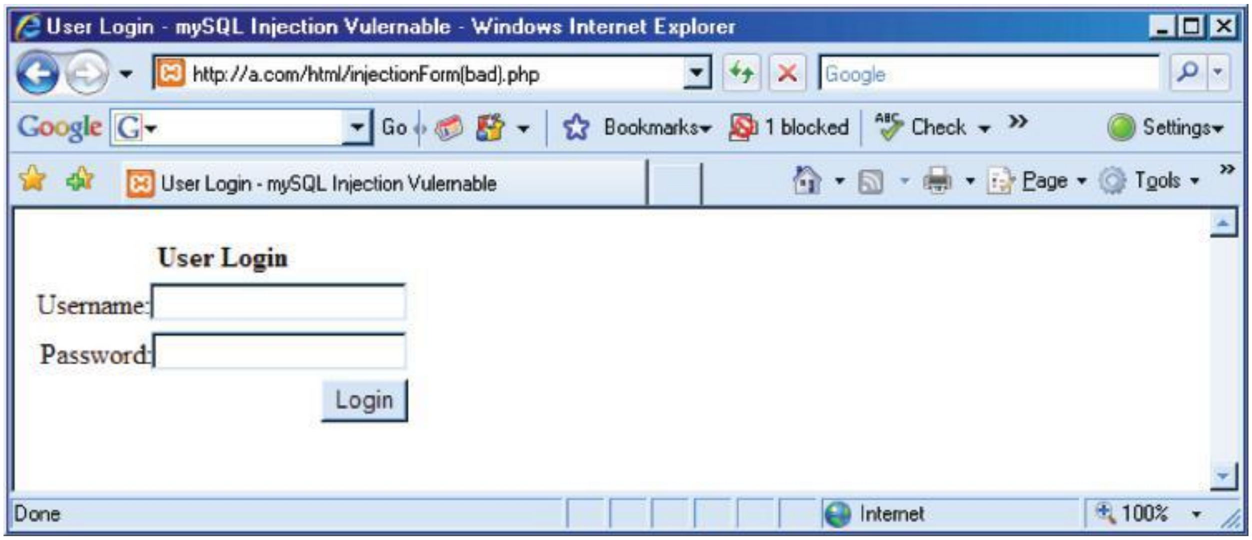
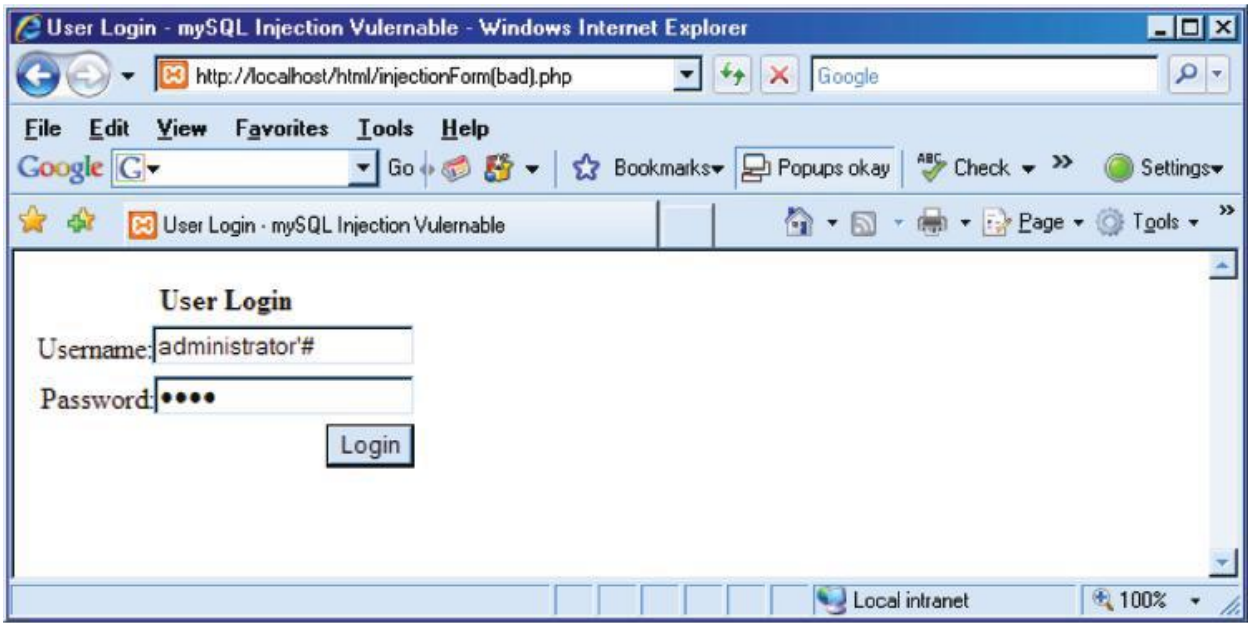

User Login - mySQL Injection Vulernable - Windows Internet Explorer
http://a.com/html/injectionForm(bad).php
Google
Go
Bookmarks
1 blocked
Check
Settings
User Login - mySQL Injection Vulernable
Page
Tools
User Login
Username:
Password:
Login
Done
Internet
100%

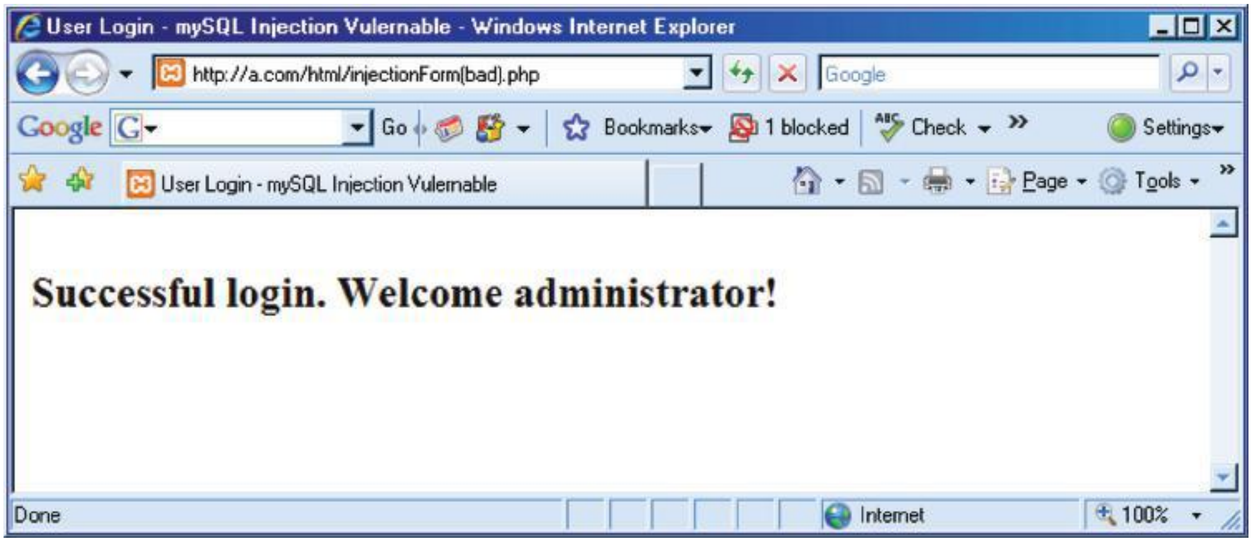
FIGURE 26.38 A SQL injection attack


User Login - mySQL Injection Vulernable - Windows Internet Explorer
http://localhost/html/injectionForm(bad).php
Google
File
Edit
View
Favorites
Tools
Help
Go
Bookmarks
Popups okay
Check
Settings
User Login - mySQL Injection Vulernable
Page
Tools
User Login
Login
Local intranet
100%

Username: administrator'#

Password: ••••

FIGURE 26.39 The attacker employs the user name: administrator' #.


User Login - mySQL Injection Vulernable - Windows Internet Explorer
http://a.com/html/injectionForm(bad).php
Google
Go
Bookmarks
1 blocked
Check
Settings
User Login - mySQL Injection Vulernable
Page
Tools
Done
Internet
100%

Successful login. Welcome administrator!

FIGURE 26.40 A SQL injection success.

Example2

SQL Injection Based on 1=1 is Always True

Look at the example below .Let's say that the original purpose of the code was to create an SQL statement to select a user with a given user id.

If there is nothing to prevent a user from entering "wrong" input, the user can enter some "smart" input like this:

UserId:

105 or 1=1

Server Result

```
SELECT * FROM Users WHERE UserId = 105 or 1=1
```

The SQL above is valid. It will return all rows from the table Users, since **WHERE 1=1** is always true.

SQL INJECTION DEFENSE TECHNIQUES

SQL injection can be protected by filtering the query to eliminate malicious syntax, which involves the employment of some tools in order to

(a) scan the source code using, e.g., Microsoft SQL Source Code Analysis Tool,

(b) scan the URL using e.g., Microsoft UrlScan,

(c) scan the whole site using e.g., HP Scrawlr, and (d) sanitize user input forms through secure programming.

(d) In addition, the input fields should be restricted to the absolute minimum, typically anywhere from 7-12 characters, and validate any data, e.g., if a user inputs an age make sure the input is an integer with a maximum of 3 digits.