Savitribai Phule Pune University

Centre for Information and Network Security

Course: Introduction to Cyber Security / Information Security

Module 1: Pre-requisites in Information and Network Security

Chapter 3: Security Threats and Vulnerabilities

1. Basics of threat and vulnerability

In computer security a **threat** is a possible danger that might exploit a vulnerability to breach security and thus cause possible harm.

A **vulnerability** is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.

An example of a natural threat is the occurrence of a hurricane. Depending on the geographic location of the entity, the likelihood of that occurrence could be low, medium, or high, and one of the risks associated with the occurrence may be that the power could fail and the information systems could be unavailable. Based on the assessment conducted, the organization should develop a strategy to manage the risks associated with the potential of such a threat. So what is the vulnerability in the above example?

The vulnerability is us, humans. That we are fragile and cannot withstand strong winds. That we are dependent on natural as well as artificial resources to survive.

You can group threats into categories to help you formulate these kinds of pointed questions. One model you may find useful is STRIDE, derived from an acronym for the following six threat categories:

- **Spoofing identity**. An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password.

- **Tampering with data**. Data tampering involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet.

- **Repudiation**. Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise—for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. Nonrepudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package.

- **Information disclosure**. Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers.

- **Denial of service**. Denial of service (DoS) attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability.

- **Elevation of privilege**. In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defences and become part of the trusted system itself, a dangerous situation indeed

Let’s take a bank example to see how threats are categorized, here is a list of uncategorized threats for you, please put them in their respective categories:

1. If somebody is able to transfer money with my consent but I am not able to see who and how much he/she has transferred money from my account
2. If I transfer Rs.100 to another account every time more/less than Rs. 100 is deducted from my account
3. I as an user is not able to access a particular part of web application
4. A malicious user is able to change my account balance
5. Any other person is able to see how much balance I have in my account
6. A malicious user is able to change my email address and password

Answer:

Spoofing Identity: (6)

Tampering of data: (2)

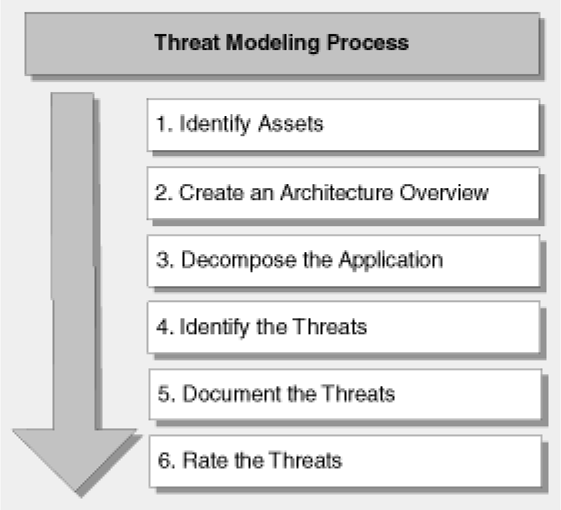
Repudiation: (1)

Information disclosure: (5)

Denial of Service: (3)

Elevation of privilege: (4)

2. How to do identify threats through threat modelling?



Source: https://msdn.microsoft.com/en-us/library/ff648644.aspx

An overview of the threat modeling process

1. **Identify assets**.

   Identify the valuable assets that your systems must protect. Example: Confidential data, such as customer databases

2. **Create an architecture overview**.

   Use simple diagrams and tables to document the architecture of your application, including subsystems, trust boundaries, and data flow.

3. **Decompose the application**.

   Decompose the architecture of your application, including the underlying network and host infrastructure design, to create a security profile for the application. The aim of the security profile is to uncover vulnerabilities in the design, implementation, or deployment configuration of your application.

4. **Identify the threats**.

   Keeping the goals of an attacker in mind, and with knowledge of the architecture and potential vulnerabilities of your application, identify the threats that could affect the application.

5. **Document the threats**.

   Document each threat using a common threat template that defines a core set of attributes to capture for each threat.

6. **Rate the threats**.

   Rate the threats to prioritize and address the most significant threats first. These threats present the biggest risk. The rating process weighs the probability of the threat against damage that could result should an attack occur. It might turn out that certain threats do not warrant any action when you compare the risk posed by the threat with the resulting mitigation costs

As said earlier threats arises due to presence of vulnerabilities, let’s take a look at few of the common security problems of IT and threats associated with them

3. Weak/Strong password and Password Cracking

Now-a-days passwords are the most important asset in any application. It is the key through which the application identifies the user and allows them to do their respective actions. If a malicious user is able to guess/retrieve your password then he is control of your data, information and in general existence.

So, what are the attributes of a strong password?

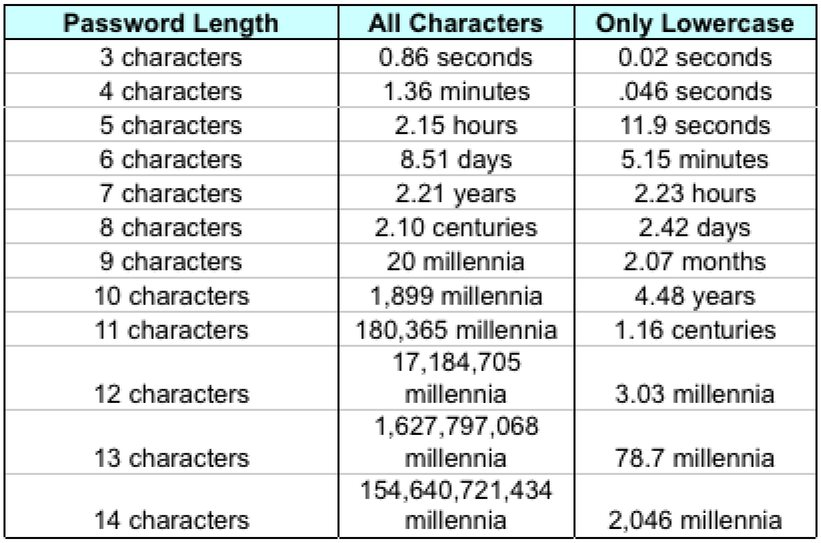
- Contains both upper and lower case characters
- Includes digits and punctuation characters as well as letters (!@#$%^&*()_+|~-=`{}[]:”;’<>?,./)
- Has at least eight characters
- Does not contain a word in any language, slang, dialect, jargon, etc.
- Is not based on personal information, names of family, etc.

And weak password?

- Contains less than eight characters
- Is a word found in a dictionary (English or foreign)
- Is a common usage word such as: Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software, sport team
- Birthdays and other personal information such as addresses, phone numbers, or license plates
- Word or number patterns like aaabbb, qwerty, 9876543
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (battleship52)

The user needs to create a strong password to avoid password cracking which is one of the foremost ways of hacking as it is very easy to do and provides complete control over the victim. So what is password cracking?

The time to crack a password is related to password strength, which is a measure of the password's information entropy, and the details of how the password is stored. Most methods of password cracking require the computer to produce many candidate passwords, each of which is checked. One example is brute-force cracking, in which a computer tries every possible key or password until it succeeds. More common methods of password cracking, such as dictionary attacks, pattern checking, word list substitution, etc. attempt to reduce the number of trials required and will usually be attempted before brute force.



Password Length	All Characters	Only Lowercase
3 characters	0.86 seconds	0.02 seconds
4 characters	1.36 minutes	.046 seconds
5 characters	2.15 hours	11.9 seconds
6 characters	8.51 days	5.15 minutes
7 characters	2.21 years	2.23 hours
8 characters	2.10 centuries	2.42 days
9 characters	20 millennia	2.07 months
10 characters	1,899 millennia	4.48 years
11 characters	180,365 millennia	1.16 centuries
12 characters	17,184,705 millennia	3.03 millennia
13 characters	1,627,797,068 millennia	78.7 millennia
14 characters	154,640,721,434 millennia	2,046 millennia

Source: http://lifehacker.com/5505400/how-id-hack-your-weak-passwords

4. Insecure Network connections

Through insecure network connection, the hacker will be able to get sensitive information over the network like username/password, browsing history, usage pattern etc.

The following are the characteristics of a non-secure network communication:

1. Non-Https communication where sensitive data is sent over the network with any kind of encryption
2. Unsecured firewalls where unnecessary ports are still opened and can be used to attack the system
3. Local digital certificates are used by websites which can be easily duplicated resulting in phishing attacks
4. Improper network connection where the host is connected to network which is not secured and created for a malicious intent. Example free wifi systems
5. Application Layer problems in which the application is built incorrectly and allows sensitive information to be leaked. Example of username and password in the url of a website

5. Malicious Code

Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors, and malicious active content.

Computer viruses are still the most common form of malicious code. A virus is a program that infects a computer by attaching itself to another program, and propagating itself when that program is executed.

Another frequently encountered malicious code is the worm, which is a computer program that can make copies of itself, spreading through connected systems and consuming resources on affected computers or causing other damage.

Some malicious codes, including most viruses, are fragments of programs that cannot exist alone and need to attach themselves to host programs. Other types of malicious code are able to spread and replicate by themselves (such as worms) and are able to propagate from computer to computer across a network.

6. Programming Bugs

Vulnerabilities also arises due to programming flaws, some of the common flaws are given below:

6.1 Improper Input Validation

Ensure that your input is valid. If you're expecting a number, it shouldn't contain letters. Nor should the price of a new car be allowed to be a dollar. Incorrect input validation can lead to vulnerabilities when attackers can modify their inputs in unexpected ways. Many of today's most common vulnerabilities can be eliminated, or at least reduced, with strict input validation.

6.2 Improper Encoding or Escaping of Output

Insufficient output encoding is at the root of most injection-based attacks. An attacker can modify the commands that you intend to send to other components, possibly leading to a complete compromise of your application - not to mention exposing the other components to exploits that the attacker would not be able to launch directly. When your program generates outputs to other components in the form of structured messages such as queries or requests, be sure to separate control information and metadata from the actual data.

6.3 Error Message Information Leak

Chatty error messages can disclose secrets to any attacker who misuses your software. The secrets could cover a wide range of valuable data, including personally identifiable information (PII), authentication credentials, and server configuration. They might seem like harmless secrets useful to your users and admins, such as the full installation path of your software -- but even these little secrets can greatly simplify a more concerted attack.

6.4 Failure to Constrain Operations within the Bounds of a Memory Buffer

The scourge of C applications for decades, buffer overflows have been remarkably resistant to elimination. Attack and detection techniques continue to improve, and today's buffer overflow variants aren't always obvious at first or even second glance.

6.5 Improper Access Control (Authorization)

If you don't ensure that your software's users are only doing what they're allowed to, then attackers will try to exploit your improper authorization and exercise that unauthorized functionality.

6.6 Hard-Coded Password

Hard-coding a secret account and password into your software is extremely convenient -- for skilled reverse engineers. If the password is the same across all your software, then every customer becomes vulnerable when that password inevitably becomes known. And because it's hard-coded, it's a huge pain to fix.

6.7 Execution with Unnecessary Privileges

Your software may need special privileges to perform certain operations; wielding those privileges longer than necessary is risky. When running with extra privileges, your application has access to resources that the application's user can't directly reach. Whenever you launch a separate program with elevated privileges, attackers can potentially exploit those privileges.

Cybercrime and cyber terrorism:

Cyber terrorism is the use of Internet based terror attacks, done deliberately in order to create disturbances or havoc in usual working of the internet. Since, many computers are connected through internet, the chances of high disruption in computer related services in personal as well commercial devices. Attacks through cyber terrorism can be in form of various illegal activities whose number is on a constant increase, a few are most lethal and common. These include attacks from viruses, attacks from Trojans, attacks from BOTS, attacks on databases, black hat hacking etc.

Example:

The MyDoom (or Novarg) virus is another worm that can create a backdoor in the victim computer's operating system. The original MyDoom virus -- there have been several variants -- had two triggers. One trigger caused the virus to begin a denial of service (DoS) attack starting Feb. 1, 2004. The second trigger commanded the virus to stop distributing itself on Feb. 12, 2004. Even after the virus stopped spreading, the backdoors created during the initial infections remained active [source: Symantec].

Later that year, a second outbreak of the MyDoom virus gave several search engine companies grief. Like other viruses, MyDoom searched victim computers for e-mail addresses as part of its replication process. But it would also send a search request to a search engine and use e-mail addresses found in the search results. Eventually, search engines like Google began to receive millions of search requests from corrupted computers. These attacks slowed down search engine services and even caused some to crash [source: Sullivan].

MyDoom spread through e-mail and peer-to-peer networks. According to the security firm MessageLabs, one in every 12 e-mail messages carried the virus at one time [source: BBC]. Like the Klez virus, MyDoom could spoof e-mails so that it became very difficult to track the source of the infection

Information warfare and Surveillance:

Surveillance is the monitoring of the behaviour, activities, or other changing information, usually of people for the purpose of influencing, managing, directing, or protecting them.

The vast majority of computer surveillance involves the monitoring of data and traffic on the Internet. In the United States for example, under the Communications Assistance For Law Enforcement Act, all phone calls and broadband Internet traffic (emails, web traffic, instant messaging, etc.) are required to be available for unimpeded real-time monitoring by Federal law enforcement agencies.

There is far too much data on the Internet for human investigators to manually search through all of it. So automated Internet surveillance computers sift through the vast amount of intercepted Internet traffic and identify and report to human investigators traffic considered interesting by using certain "trigger" words or phrases, visiting certain types of web sites, or communicating via email or chat with suspicious individuals or groups. Billions of dollars per year are spent, to intercept and analyse all of this data, and extract only the information which is useful to law enforcement and intelligence agencies.

Computers can be a surveillance target because of the personal data stored on them. If someone is able to install software, such as the FBI's Magic Lantern and CIPAV, on a computer system, they can easily gain unauthorized access to this data. Such software could be installed physically or remotely

References:

- https://en.wikipedia.org
- http://www.hhs.gov/
- https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx
- https://msdn.microsoft.com/en-us/library/ff648644.aspx
- https://en.wikipedia.org/wiki/Password_strength
- https://www.npdn.org/infosec_pw_strong
- http://www.infosec.gov.hk/english/virus/geninfo_what.html
- http://blog.codinghorror.com/top-25-most-dangerous-programming-mistakes/s
- http://readanddigest.com/what-is-cyber-terrorism/
- http://computer.howstuffworks.com/worst-computer-viruses.htm#page=7
- https://en.wikipedia.org/wiki/Surveillance