PMSCS 694

Information Security

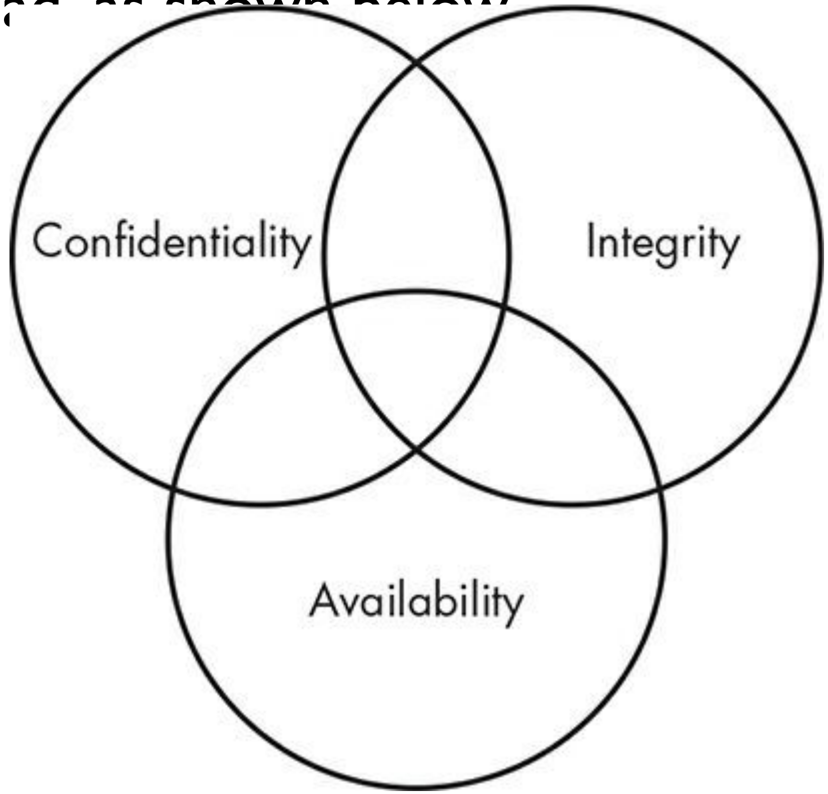
Lecture 2

Attacks

Md. Rafsan Jani
Associate Professor
Department of Computer Science and Engineering
Jahangirnagar University

Security Models

- ISO/IEC 27001, NIST
- The Confidentiality, Integrity, and Availability Triad
  - Three of the primary concepts in information security are confidentiality, integrity, and availability, commonly known as the (CIA) triad, as shown below.



Security Models

- The Confidentiality, Integrity, and Availability Triad
  - **Confidentiality**: refers to our ability to protect our data from those who are not authorized to view it. You could implement confidentiality at many levels of a process.
    - As an example, imagine a person is withdrawing money from an ATM.
    - The person in question will likely seek to maintain the confidentiality of the personal identification number (PIN) that allows him to draw funds from the ATM if he has his ATM card.
    - Additionally, the owner of the ATM will maintain the confidentiality of the account number, balance, and any other information needed to communicate to the bank from which the funds are being drawn.
    - The bank will also maintain the confidentiality of the transaction with the ATM and the balance change in the account after the funds have been withdrawn.

Security Models

- The Confidentiality, Integrity, and Availability Triad
  - Confidentiality can be compromised in a number of ways.
    - You could lose a laptop containing data.
    - A person could look over your shoulder while you enter a password.
    - You could send an email attachment to the wrong person, or an attacker could penetrate your systems etc.

Security Models

- The Confidentiality, Integrity, and Availability Triad
  - **Integrity:** is the ability to prevent people from changing your data in an unauthorized or undesirable manner.
  - To maintain integrity, not only you need to have the means to prevent unauthorized changes, but you need the ability to reverse unwanted authorized changes.
    - A good example of mechanisms that allow you to control integrity are in the file systems of many modern operating systems, such as Windows and Linux.
    - For the purposes of preventing unauthorized changes, such systems often implement permissions that restrict what actions an unauthorized user can perform on a given file.
      - For example, the owner of a file might have permission to read it and write to it, while others might have permission only to read, or no permission to access it at all.
    - Some such systems and many applications, such as databases, can allow you to undo or roll back changes that are undesirable

Security Models

- The Confidentiality, Integrity, and Availability Triad
  - Integrity is particularly important when it concerns data that provides the foundation for other decisions.
    - If an attacker were to alter the data that contained the results of medical tests, a doctor might prescribe the wrong treatment, which could kill the patient.

Security Models

- The Confidentiality, Integrity, and Availability Triad
  - **Availability:** refers to the ability to access our data when we need it.
  - You could lose availability due to a power loss, operating system or application problems, network attacks, or the compromising of a system, for example.
  - When an outside party, like an attacker, causes such issues, we typically call this a denial-of service (DoS) attack.

Security Models

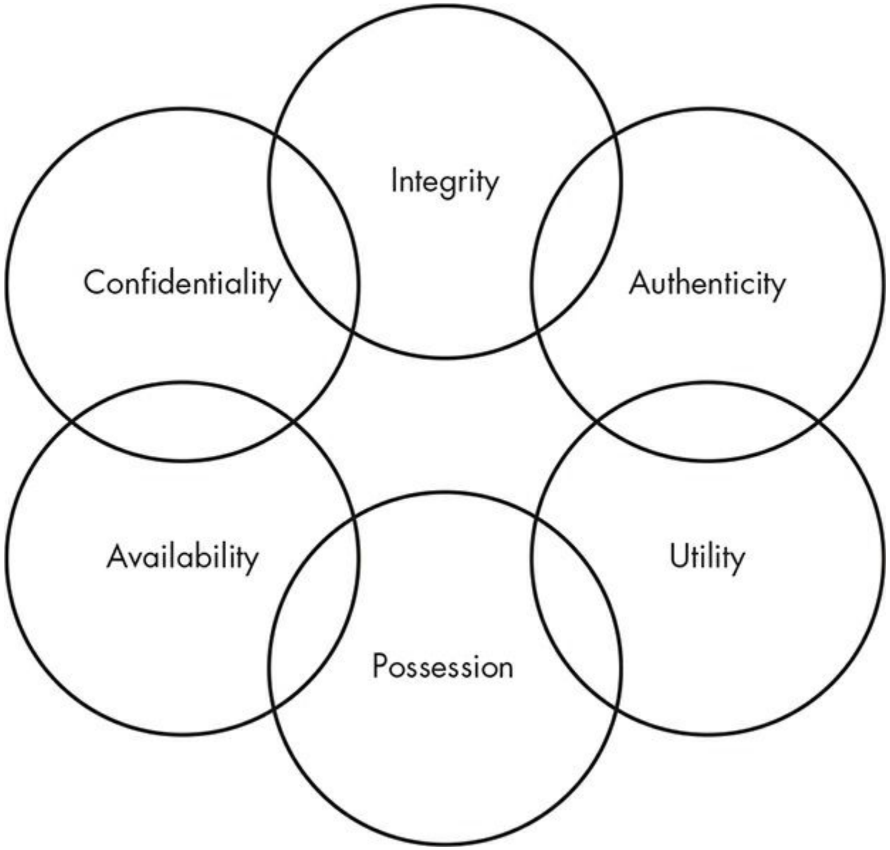
- How Does the CIA Triad Relate to Security?
  - Given the elements of the CIA triad, we can begin to discuss security issues with more detail than we otherwise could.
  - For example, let's consider a shipment of backup tapes on which you've stored the only existing, unencrypted copies of some sensitive data. If you were to lose the shipment in transit, you would have a security issue.
  - This is likely to include a breach of **confidentiality** since your files were not encrypted.
  - The lack of encryption could also cause **integrity** issues.
    - If you recover the tapes in the future, it may not be immediately obvious to you if an attacker had altered the unencrypted files, as you would have no good way to discern altered from unaltered data.

Security Models

- How Does the CIA Triad Relate to Security?
  - Given the elements of the CIA triad, we can begin to discuss security issues with more detail than we otherwise could.
  - For example, let’s consider a shipment of backup tapes on which you’ve stored the only existing, unencrypted copies of some sensitive data. If you were to lose the shipment in transit, you would have a security issue.
  - As for **availability**, you’ll have an issue unless the tapes are recovered since you don’t have backup copies of the files.
  - Although you can describe the situation in this example with relative accuracy using the CIA triad, you might find that the model is too restrictive to describe the entire situation. A more extensive model, the Parkerian hexad, exists for these cases.

Security Models

- The Parkerian Hexad
  - Parkerian hexad consists of these three principles as well as *possession or control*, *authenticity*, and *utility* for a total of six principles, as shown in Figure 2



Security Models

- The Parkerian Hexad
  - Parkerian hexad includes the three principles of the CIA triad, with the same definitions just discussed.
  - Parker describes integrity slightly differently; he doesn’t account for authorized, but incorrect, modification of data. For him, the data must be whole and completely unchanged from its previous state.

Security Models

- The Parkerian Hexad
  - **Possession or Control**: refers to the physical disposition of the media on which the data is stored.
  - This enables you to discuss your loss of the data in its physical medium without involving other factors such as availability.
  - Returning to the example of your lost shipment of backup tapes, let's say that some of them were encrypted and some of them were not.
  - The principle of possession would enable you to more accurately describe the scope of the incident;
  - the encrypted tapes in the lot cause a possession problem but not a confidentiality problem, while the unencrypted tapes cause both.

Security Models

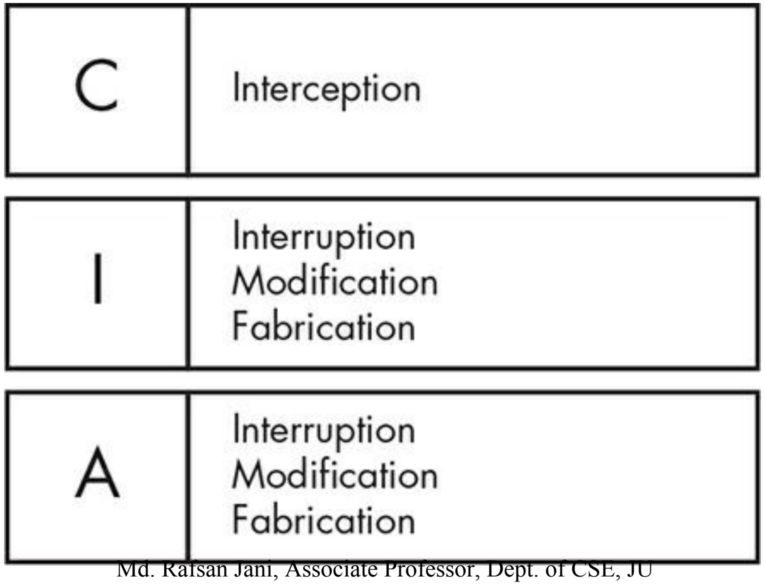
- The Parkerian Hexad
  - **Authenticity**: allows you to say whether you've accredited the data in question to the proper owner or creator.
  - For example, if you send an email message that is altered so that it appears to have come from a different email address than the one from which it was actually sent, you would be violating the authenticity of the email.
  - Authenticity can be enforced using digital signatures.
  - A similar, but reversed, concept to this is nonrepudiation, which prevents people from taking an action, such as sending an email and then later denying that they have done so.

Security Models

- The Parkerian Hexad
  - **Utility**: refers to how useful the data is to you.
  - Utility is also the only principle of the Parkerian hexad that is not necessarily binary in nature; you can have a variety of degrees of utility, depending on the data and its format.
  - For instance, in the shipment of backup tapes example, imagine that some of the tapes were encrypted and some were not.
  - For an attacker or other unauthorized person, the encrypted tapes would likely be of very little utility, as the data would not be readable. The unencrypted tapes would be of much greater utility, as the attacker or unauthorized person would be able to access the data.

Attacks

- Types of Attacks
  - You can generally place attacks into one of four categories:
    - interception,
    - interruption,
    - modification, and
    - fabrication.
  - Each of the categories can affect one or more of the principles of the CIA triad, as shown in Figure.



C	Interception
I	Interruption Modification Fabrication
A	Interruption Modification Fabrication

Attacks: Types of Attacks

- Interception
  - Interception attacks allow unauthorized users to access your data, applications, or environments, and they are primarily attacks against confidentiality.
  - Interception might take the form of unauthorized file viewing or copying, eavesdropping on phone conversations, or reading someone else’s email, and you can conduct it against data at rest or in motion
  - When they’re properly executed, interception attacks can be difficult to detect.

Attacks: Types of Attacks

- Interruption
  - Interruption attacks make your assets unusable or unavailable to you on a temporary or permanent basis.
  - These attacks often affect availability but can affect integrity, as well.
  - You would classify a DoS attack on a mail server as an availability attack.
  - On the other hand, if an attacker manipulated the processes on which a database runs to prevent access to the data it contains, you might consider this an integrity attack because of the possible loss or corruption of data, or you might consider it a combination of the two.
  - You might also consider such a database attack to be a modification attack rather than an interruption attack.

Attacks: Types of Attacks

- Modification
  - Modification attacks involve tampering with an asset.
  - Such attacks might primarily be considered attacks on integrity but could also represent attacks on availability.
  - If you access a file in an unauthorized manner and alter the data it contains, you've affected the **integrity** of the file's data.
  - However, if the file in question is a configuration file that manages how a service behaves—perhaps one that is acting as a web server—changing the contents of the file might affect the **availability** of that service.
  - If the configuration you altered in the file for your web server changes how the server deals with encrypted connections, you could even call this a **confidentiality** attack.

Attacks: Types of Attacks

- Fabrication
  - Fabrication attacks involve generating data, processes, communications, or other similar material with a system.
  - Like the last two attack types, fabrication attacks primarily affect integrity but could affect availability, as well.
  - Generating fake information in a database would be a kind of fabrication attack. You could also generate email, a common method for propagating malware.
  - If you generated enough additional processes, network traffic, email, web traffic, or nearly anything else that consumes resources, you might be conducting an availability attack by rendering the service that handles such traffic unavailable to legitimate users.

Attacks

- Threats
  - A threat is something that has the potential to cause harm.
  - Threats tend to be specific to certain environments, particularly in the world of information security.
  - For example, although a virus might be problematic on a Windows operating system, the same virus will be unlikely to have any effect on a Linux operating system
- Vulnerabilities
  - Vulnerabilities are weaknesses, or holes, that threats can exploit to cause you harm.
  - A vulnerability might involve a specific operating system or application that you're running, the physical location of your office building, a data center that is overpopulated with servers and producing more heat than its air-conditioning system can handle, a lack of backup generators, or other factors.

Attacks

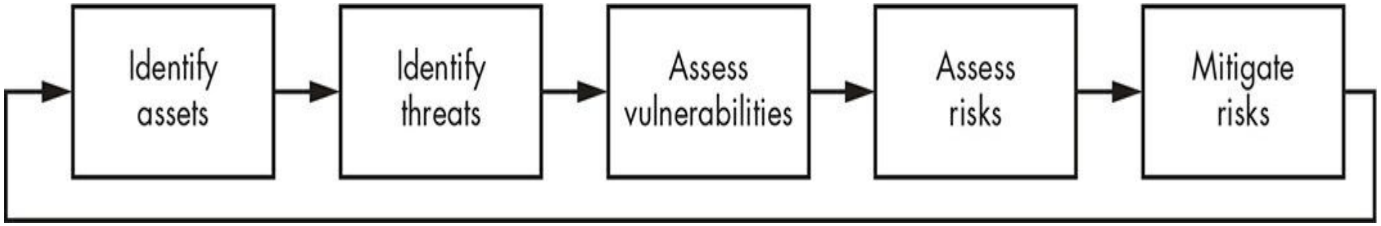
- Risk
  - Risk is the likelihood that something bad will happen.
  - For you to have a risk in an environment, you need to have both a threat and a vulnerability that the threat could exploit.
  - For example, if you have a structure that is made from wood and you light a fire nearby, you have both a threat (the fire) and a matching vulnerability (the wood structure).
    - In this case, you most definitely have a risk.
  - Likewise, if you have the same threat of fire but your structure is made of concrete, you no longer have a credible risk because your threat doesn't have a vulnerability to exploit.
    - You could argue that a sufficiently hot flame could damage the concrete, but this is a much less likely event.

Attacks

- Impact
  - Some organizations, such as the US National Security Agency (NSA), add a factor to the threat/vulnerability/risk equation called impact.
  - Impact takes into account the value of the asset being threatened and uses it to calculate risk.
  - In the backup tape example, if you consider that the unencrypted tapes contain only your collection of chocolate chip cookie recipes, you may not actually have a risk because the data exposed contains nothing sensitive and you can make additional backups from the source data.
  - In this case, you might safely say that you have no risk.

Attacks: Risk Management

- Risk management processes compensate for risks in your environment, Figure 4. *As you can see, you need to identify your important assets, figure out*
- *the potential threats against them, assess your vulnerabilities, and then*
- *take steps to mitigate these risks.*



- Identify Assets
  - One of the first and, arguably, most important parts of the risk management process is identifying the assets you’re protecting. If you can’t enumerate your assets and evaluate the importance of each, protecting them can become a difficult task indeed.

Attacks: Risk Management

- Identify Threats
  - It's often useful to have a framework for discussing the nature of a given threat. For instance, let's apply the Parkerian hexad to examine the threats credit card payments System.
  - **Confidentiality** If you expose data inappropriately, you could potentially have a breach.
  - **Integrity** If data becomes corrupt, you may incorrectly process payments.
  - **Availability** If the system or application goes down, you won't be able to process payments.
  - **Possession** If you lose backup media, you could potentially have a breach.
  - **Authenticity** If you don't have authentic customer information, you may process a fraudulent transaction.
  - **Utility** If you collect invalid or incorrect data, that data will have limited utility.

Attacks: Risk Management

- Assess Vulnerabilities
  - **Confidentiality** If you expose data inappropriately, you could potentially have a breach.
    - Your sensitive data is encrypted at rest and in motion. Your systems are regularly tested by an external penetration testing company. This is not a risk.
  - **Integrity** If data becomes corrupt, you may incorrectly process payments.
    - You carefully validate that payment data is correct as part of the processing workflow. Invalid data results in a rejected transaction. This is not a risk.
  - **Availability** If the system or application goes down, you won't be able to process payments.
    - You do not have redundancy for the database on the back end of the payment processing system. If the database goes down, you can't process payments. This is a risk.

Attacks: Risk Management

- Assess Vulnerabilities
  - **Possession** If you lose backup media, you could potentially have a breach.
    - Your backup media is encrypted and hand-carried by a courier. This is not a risk.
  - **Authenticity** If you don’t have authentic customer information, you may process a fraudulent transaction.
    - Ensuring that valid payment and customer information belongs to the individual conducting the transaction is difficult. You do not have a good way of doing this. This is a risk.
  - **Utility** If you collect invalid or incorrect data, that data will have limited utility.
    - To protect the utility of your data, you checksum credit card numbers, make sure that the billing address and email address are valid, and perform other measures to ensure that your data is correct. This is not a risk.

Attacks: Risk Management

- Assess Risks
  - Once you’ve identified the threats and vulnerabilities for a given asset, you can assess the overall risk.
  - Risk is the conjunction of a threat and a vulnerability.
  - A vulnerability with no matching threat or a threat with no matching vulnerability does not constitute a risk.
  - **Availability** If the system or application goes down, you won’t be able to process payments.
    - You do not have redundancy for the database on the back end of the payment processing system. If the database goes down, you can’t process payments.
  - In this case, you have both a threat and a corresponding vulnerability, meaning you risk losing ability to process credit card payments because of a single point of failure on your database back end. Once you’ve worked through your threats and vulnerabilities in this manner, you can mitigate these risks..

Attacks: Risk Management

- Mitigate Risks
  - To mitigate risks, you can put measures in place to account for each threat. These measures are called controls.
  - Controls are divided into three categories:
  - Physical,
  - Logical, and
  - Administrative.

Attacks: Risk Management

- Mitigate Risks
  - **Physical controls** protect the physical environment in which your systems sit, or where your data is stored. Such controls also control access in and out of such environments.
  - Physical controls include fences, gates, locks, bollards, guards, and cameras, but also systems that maintain the physical environment, such as heating and air-conditioning systems, fire suppression systems, and backup power generators.
  - Logical, and
  - Administrative.

Attacks: Risk Management

- Mitigate Risks
  - **Logical controls** sometimes called technical controls, protect the systems, networks, and environments that process, transmit, and store your data.
  - Logical controls can include items such as passwords, encryption, access controls, firewalls, and intrusion detection systems.
  - Logical controls enable you to prevent unauthorized activities; if your logical controls are implemented properly and are successful, an attacker or unauthorized user can’t access your applications and data without subverting the controls

Attacks: Risk Management

- Mitigate Risks
  - **Administrative controls** are based on rules, laws, policies, procedures, guidelines, and other items that are "paper" in nature. Administrative controls dictate how the users of your environment should behave.
  - Depending on the environment and control in question, administrative controls can represent differing levels of authority. You may have a simple rule such as "turn the coffee pot off at the end of the day," aimed at avoiding a physical security problem (burning your building down at night). You may also have a more stringent administrative control, such as one that requires you to change your password every 90 days.

Attacks: Risk Management

- Incident Response
  - The incident response process, at a high level, consists of the following
    - Preparation
    - Detection and analysis
    - Containment
    - Eradication
    - Recovery
    - Post-incident activity

Attacks: Risk Management

- Incident Response
  - Preparation
    - The preparation phase of incident response consists of all the activities you can perform ahead of time to better handle an incident.
    - This typically involves
      - creating policies and procedures that govern incident response and handling,
      - conducting training and education for both incident handlers and those who are expected to report incidents, and
      - developing and maintaining documentation.

Attacks: Risk Management

- Incident Response
  - Detection and Analysis
    - The detection and analysis phase is where the action begins.
    - In this phase, you detect an issue, decide whether it’s actually an incident, and respond to it appropriately.
    - Most often, you’ll detect the issue with a security tool or service, like
      - an intrusion detection system (IDS),
      - antivirus (AV) software,
      - firewall logs,
      - proxy logs, or alerts from a security information and
      - event monitoring (SIEM) tool or managed security service provider (MSSP).
    - Often requires human intervention.
    - When the incident handler evaluates the situation, that person will decide whether the issue constitutes an incident, evaluate the criticality of the incident, and contact any additional resources needed to proceed to the next phase.

Attacks: Risk Management

- Incident Response
  - Containment
    - Involves taking steps to ensure that the situation doesn't cause any more damage than it already has—or at least lessen any ongoing harm.
    - If the problem involves a malware-infected server actively being controlled by a remote attacker, this might mean disconnecting the server from the network, putting firewall rules in place to block the attacker, and updating signatures or rules on an intrusion prevention system (IPS) to halt the traffic from the malware.

Attacks: Risk Management

- Incident Response
  - Eradication
    - During eradication, you'll attempt to remove the effects of the issue from your environment.
    - In the case of your malware-infected server, you've already isolated the system and cut it off from its command-and control network.
    - Now you'll need to clean the malware from the server and ensure that it doesn't exist elsewhere in your environment.
    - This might involve additional scanning of other hosts in the environment to ensure that the malware is not present and perhaps examining logs on the server and network to determine what other systems the infected server has communicated with.
    - With malware, particularly very new malware or variants, this can be a tricky task. Whenever you're in doubt about whether you've truly evicted malware or attackers from your environment, you should err on the side of caution.

Attacks: Risk Management

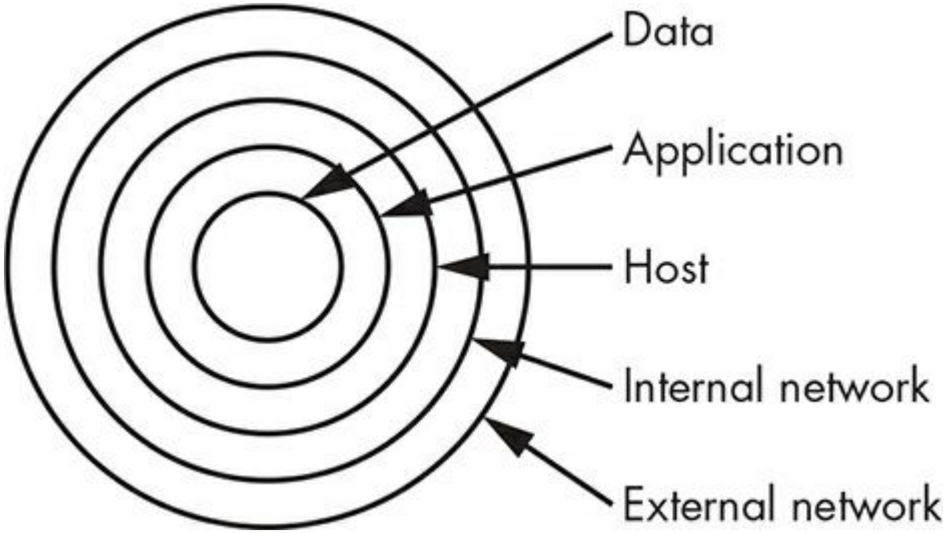
- Incident Response
  - Recovery
    - Recovery might involve restoring devices or data from backup media, rebuilding systems, or reloading applications. Again, this can be a more painful task than it initially seems because your knowledge of the situation might be incomplete or unclear.
    - You may find that you are unable to verify that backup media is clean and free or infection or that the backup media is entirely bad.
    - Application install bits may be missing, configuration files may not be available, or many other issues could occur.

Attacks: Risk Management

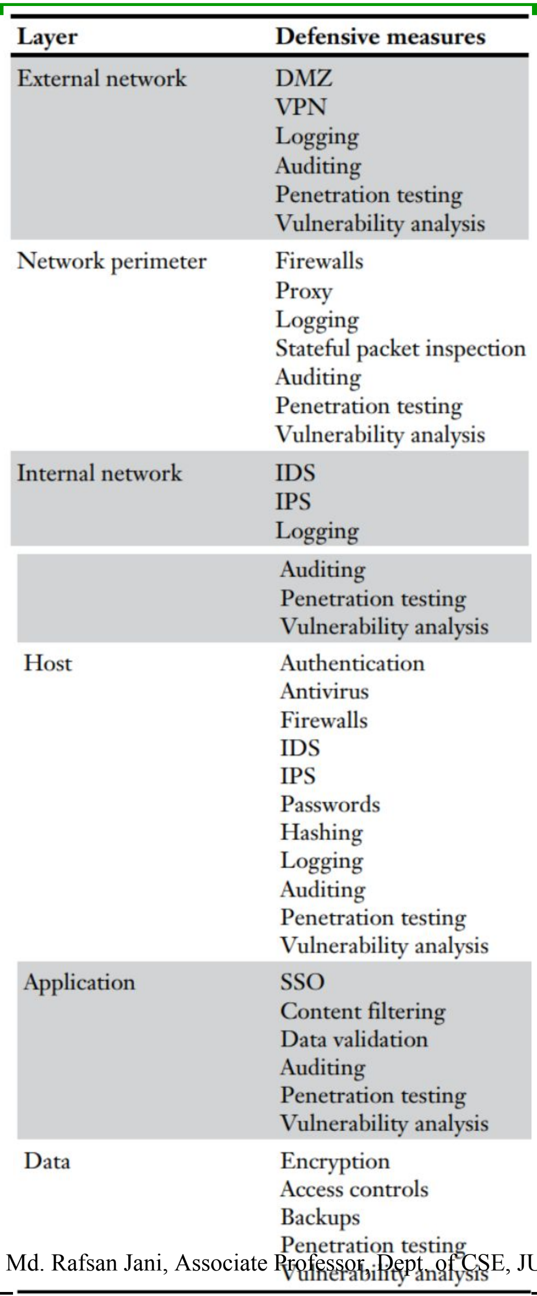
- Incident Response
  - Post-Incident Activity
    - Like preparation, post-incident activity is easy to overlook, but you should ensure that you don’t neglect it.
    - In the post-incident activity phase, often referred to as a post-mortem (Latin for “after death”), you attempt to determine specifically what happened, why it happened, and what you can do to keep it from happening again.
    - The purpose of this phase is not to point fingers or place blame (although this does sometimes happen) but to ultimately prevent or lessen the impact of future such incidents.

Defense in Depth

- **Defense in depth** is a strategy common to both military maneuvers and information security.
- The basic concept is to formulate a multilayered defense that will allow you to still mount a successful resistance should one or more of your defensive measures fail.
- In Figure 5, you can see an example of layers you might want to put in place to defend your assets.



Defense in Depth



Layer	Defensive measures
External network	DMZ VPN Logging Auditing Penetration testing Vulnerability analysis
Network perimeter	Firewalls Proxy Logging Stateful packet inspection Auditing Penetration testing Vulnerability analysis
Internal network	IDS IPS Logging Auditing Penetration testing Vulnerability analysis
Host	Authentication Antivirus Firewalls IDS IPS Passwords Hashing Logging Auditing Penetration testing Vulnerability analysis
Application	SSO Content filtering Data validation Auditing Penetration testing Vulnerability analysis
Data	Encryption Access controls Backups Penetration testing Vulnerability analysis