Final Study Guide

Tuesday, December 5, 2017 12:04 AM

CHAPTER 1 (Book Notes, Then Homework 1 Answers):

- James Anderson believes info sec in an enterprise is a "well informed sense of assurance that the info risks and controls are in balance".
- Computer security began as the idea that mainframe computers in WW2 needed to be physically secure, like the machine Alan Turing used to crack Enigma.
- The **Rand Report R609** was classified for 10 years, and describes the controls and mechanisms needed to keep a computerized data processing system safe. It is the paper that started the study of computer security.
- The **CIA Triangle** is based on confidentiality, integrity, and access. These describe the utility of information. An industry standard, it however is no longer viewed as being adequate enough in addressing the constantly changing environment of security.
- **Security** itself is protection. It is the state of being safe from danger or harm. It is also the actions taken to make sure something is secure.
- **Info Security** is the protection of info and its critical elements, including the systems and hardware that use, store, and transmit the info. This includes data, management, and network security.
- **Access** is defined as a subject or object's ability to use, manipulate, modify, or affect another subject or object.
- An **asset** is an org resource that is being protected.
- An **attack** is an intentional or unintentional act that can damage or otherwise compromise info and the systems that support it. A passive attack is someone unwittingly violating security policy. An intentional attack is a hack. A direct attack is using a PC to attack another PC. An indirect attack is a hacker using a system to attack other systems, not owning the original.
- **A control/safeguard/countermeasure** are mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and improve sec.
- An **exploit** is a technique used to compromise a system.
- **Exposure** happens when a system is in a state of being exposed, describing when a vulnerability is known to an attacker.
- **Loss** is when an asset sustains damage or destruction. Theft is considered loss.
- **A protection profile or security program** is the entire set of controls protocols and safeguards used to protect an asset.
- **Risk** is the probability of an unwanted occurrence, like a loss.
- A computer can be either a **subject** or **object of attack.** A subject attacks something, and object is attacked.
- **A threat** is a category of objects, people or other entities that are a danger to an asset.
- A **threat agent** is the specific instance or a component of a threat. Like a hacker or lightning bolt.
- A **vulnerability** is a weakness or fault in a system that opens it to attack or damage.

  availability An attribute of information that describes how data is accessible and correctly formatted for use without interference or obstruction.
  accuracy An attribute of information that describes how data is free of errors and has the value that the user expects.
  authenticity An attribute of information that describes how data is genuine or original rather than reproduced or fabricated.
  confidentiality An attribute of information that describes how data is protected from disclosure or exposure to unauthorized individuals or systems.
  integrity An attribute of information that describes how data is whole, complete, and uncorrupted.
  utility An attribute of information that describes how data has value or usefulness for an end purpose.
- The CNSS Security Model is the one the book uses to teach info security.
- The model uses the **McCumber Cube**, which contains things that must be addressed to remain secure.
-

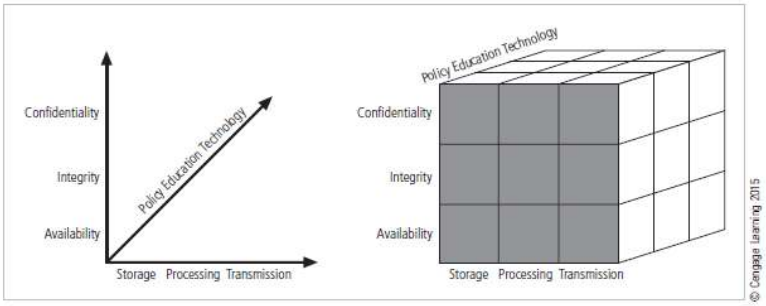


Figure 1-9 The McCumber Cube[13]

- The **McCumber Cube** uses nine properties. The first three are to do with the state of data, the second three are to do with the actions done on data, and the third are what is done to improve the other two:
  - Confidentiality
  - Integrity
  - Availability
  - Storage
  - Processing
  - Transmission
  - Policy
  - Education
  - Training
- The book defines an **info system** as much more than computer hardware, it is the entire set of people, procedures, and tech that enable business to use info. It has six critical components: hardware, software, networks, people, procedures, and data.
- **The bottom up approach** to the implementation of info security involves sysadmins attempting to improve the sec of their systems. The **top down** approach has upper level management issuing policies, procedures and processes. A bottom up has the advantage of technical knowledge from the start, but is weak due to the fact that no one wants

to listen to a goddamn sysadmin. The top down approach doesn't have the technical knowhow at first, but it brings funding, planning, and procedure.

- The **security systems development life cycle** is a methodology for the design and implementation of security systems. A methodology is a rigorous process with a clearly defined goal. It has steps:
    - Investigation, where upper management starts the project and outlines the process, outcomes and goals of that project. The budget is made, teams are made, the scope is defined, and other constraints are analyzed. A feasibility analysis is done to make sure the project will work.
    - Analysis, where existing security policy is analyzed along with current threats. Risk management is done, identifying, assessing, and evaluating the levels of risk in the org. Current legal issues are also examined.
    - Logical design, which develops the blueprints for info security. It also implements policies that influence later decisions. Incident response is also designed here, which tells how the business continues upon loss, what steps are taken during an attack, and what has to be done to recover systems after disaster.
    - Physical design, which evaluates the tech needed to be purchased in order to implement the logical design in real life.
    - Implementation, where everything is put together and tested multiple times. Personnel are trained, and upper management gets the results.
    - Maintenance and change, where the system is updated, kept afloat, and watched/monitored carefully for any new and changing threats working their way in.
- **Software assurance** is when security is built into the dev life cycle of software instead of after it is released.

- Modern computing has its roots in The Department Of Defense.
- The precursor to the internet was ARPANET.
- The paper that started the study of internet security was Rand Report R-609.
- The rapid proliferation of the internet increased security as it widened the attack surface of every organization that utilized it.
- The CIA triangle is a triangle combining confidentiality of data, integrity of data, and availability of data. Accessibility of data means you can get a hold of the data, but availability means it is in a format useful to you.
- **Access** is the ability to interact with a resource in any way.
- **An asset** is a specific organizational resource of value.
- **An attack** is an intentional or unintentional act that can damage an asset.
- A **countermeasure** is a specific security mechanism or policy which is intended to improve security.
- An **exploit** is a technique used to compromise an information system.
- **A loss** is an instance of an information asset suffering damage.
- A **threat** is an object, person, or other thing which represents a danger to assets.
- **A threat agent** is a person or system who uses exploits to instantiate threats.
- A **vulnerability** is a system weakness or fault which decreases security.
- Availability is a superset of accessibility.
- Something is **authentic** if the information it contains is genuine.
- **Confidentiality** means a piece of information is access restricted.
- Integrity measures the corruption of data.
- **Utility** determines the usefulness of data.
- **Possession** refers to who owns data or controls it.
- The six major components of an information system are:
    - Hardware
    - Software
    - Networks
    - People
    - Procedures
    - Data
- People are the most likely component to result in a security breach. This is because people ignore policy and protocol in the quest for personal convenience.
- Quality info security systems strike a balance between confidentiality and availability.
- Use TCSEC as a reference for evaluating your security plans.
- The five phases of the systems development cycle (different from the security systems dev cycle) are:
    - Evolution, where one determines if a project is feasible for an organization, and determines the goal of the project itself.
    - Requirements analysis, where the potential impact of legal issues are analyzed, and specific threat impacts are enumerated.
    - Design, where incident response plans are created, and project success criteria is established.
    - Implementation, where you build and buy selected components of the system, and educate the community who will be using this system.
    - Testing, where you simulate a business-affecting natural disaster among other threat scenarios, and measure your results vs success criteria.
- To keep people security related issues in check, make your requirements as transparent as possible, and be sensitive to the life situations of your employees.

CHAPTER 2 (Book Notes, Homework)

- Info security performs 4 important functions in an organization:
    - Protects the org's ability to function
    - Protects the data and info the org collects and uses
    - Enables the safe operation of apps running on the orgs IT systems
    - Safeguards the org's tech assets
- Implementing info security has more to do with management than technology.
- Data security is the protection of data that is in transmission, in processing, and at rest (in storage). Database security is the process of maintaining the confidentiality, integrity, and availability of a DBMS, and is done by applying a broad range of control approaches common to many areas of info security.
- A **threat** represents a potential risk to an info asset, whereas an **attack** represents an ongoing act against the **asset** that could result in a **loss**. **Threat agents** are people or entities that can cause loss by using **exploits** to take advantage of **vulnerabilities**.
- To protect an organization's information, you must be familiar with the info to be protected and the systems that store, transport, and process that info. You also have to know the threats you face.
- The CSI (Computer Security Institute) has a survey called the Computer Crime and Security Survey. It found in 2011 that 67.1 percent of responding orgs suffered malware infections, but only 11 were penetrated from the outside.
- The CAPEC (Common Attack Pattern Enumeration and Classification) tool is used by pros to understand attacks. It

uses characteristics of the attack to evaluate what kind of attack it is.

Category of threat	Attack examples
Compromises to intellectual property	Piracy, copyright infringement
Deviations in quality of service	Internet service provider (ISP), power, or WAN service problems
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, floods, earthquakes, lightning
Human error or failure	Accidents, employee mistakes
Information extortion	Blackmail, information disclosure
Sabotage or vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, denial of service
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

Table 2-2 The 12 Categories of Threats to Information Security[7]

- The 12 categories above represent a clear and present danger to everything contained within an org. You have to prioritize the threats in this list based on how you operate (your strategy).
- The first threat is compromises to your IP. This can include software piracy, the unlawful use or duplication of software based IPS. You can get around this by assigning licenses for software to individuals or orgs through a registration code and user compliance with an End User License Agreement.
- **IP losses** can occur through the exploitation of vulnerabilities in asset protection controls, like changing registry values for free FL Studio.
- **Deviations in QoS** are another threat. Availability disruption can occur when service providers fail to deliver expected services to your org. A Service Level Agreement is used with server hosting providers so that losses will be compensated upon a deviation in QoS from the hosting company. Public utility companies can also screw up, cutting off water systems, which cuts off AC for server rooms, destroying servers. Blackouts (long term outages in power), brownouts (long term decrease in power supplied) and faults (short interruptions in electrical power service) can all cause downtime for computer resources. Spikes and surges can fry equipment.
- **Espionage/trespass** is a large threat. While ethically researching your competitors information is merely considered competitive intelligence, industrial espionage occurs when your information collection crosses the line into unethical territory. When this is committed by a foreign agent, it is considered espionage and a threat to national security. Methods include shoulder surfing (hovering over someone and looking at their screen).
- Hackers commonly perform trespass, where info gatherers grab info from a system without permission. Hackers can be experts or novices, either writing their own code or using code written by others respectively. Hackers who work for money are considered professional. If that money is illicit, they are criminal, but if their work is paid and authorized by the company, they are usually a penetration tester. Pen testers allow an org to figure out where its holes are in its security practices.
- Hacks on a system usually follow a pattern. Hackers will first attempt to trespass into the server, by uploading some of their own code/information in malicious ways. This is usually done for the next step, privilege escalation, where vulnerabilities are exploited to give hackers root access to the filesystem and the system itself. At this point, they can do anything, obviously.
- **Crackers** are hackers who bypass software copyright protection and those who beat password encryption. **Phreakers** are hackers who mess with the phone system.
- There are a couple of ways to crack a password. The first is **brute force** password attacks, which try every possible password combination with a specific user account or multiple targeted ones. **Dictionary attacks** are variants of this, in which not every password is used, but a list of common or target passwords to a target.
- **Rainbow tables** takes the hashed passwords (usually from a database breach), and check the hashes against common password hashes in a table.
- Social engineering password attacks is phishing, basically.
- **Forces of nature** can blow the shit out of everything. Don't host servers in Florida.
- **Human error** can wreak havoc on an organization. People can make mistakes, or fail to follow established policy on purpose. Employees are one of the greatest threats to an orgs info security.
- **Social engineering** is used by attackers to gain system access or intel on how to access a system. People can impersonate the helpdesk, a sysadmin, a manager, or other positions of authority to exert pressure on employees to leak information in what they thought was a normal interaction. **Phishing** is a type of this where email is used to capture passwords through illicit exchanges. **Spear phishing** is when the email is targeted, regular phishing just blankets employees in an org hoping for one sucker.
- **Information extortion** is when someone steals info and demands a ransom for the deletion or return of it.
- **Sabotage or vandalism** occurs when a hacker isn't looking to gain anything out of the hack, but to cause as much harm to the org as possible. This can harm org image in the public eye.
- Software attacks can occur when malicious software is sent to the systems contained within an org. This software is known as **malware**. **Viruses** perform malicious actions through code, and propagate themselves to do the same across more computers in the org. **Macro viruses** are viruses embedded in code that automatically gets ran by existing legitimate software. **Boot viruses** infect the boot sector, making it damn near impossible to delete them.
- **Worm** attacks use software that replicate themselves that fill any resource it can on the computer.
- **Trojans** are viruses that have been disguised as helpful or wanted software. Polymorphic viruses can change its own code to evade antivirus detection.
- A **back door** is a hole left in system security that creates an easily exploitable vulnerability so that later hackers can access the system easily.
- A **Denial Of Service** attack attempts to stop service of a webserver or any other computer by flooding it with a large amount of information requests. A DDoS is the same thing, but using previously exploited computers, now called bots, the attacker uses each bot to send requests.
- Communication can be intercepted in many different ways, in **communication interception** attacks.
- **Packet sniffers** can monitor data travelling over a network. If data is not encrypted in a network, multiple packets can be used to recreate the info contained in them, like passwords.
- **IP spoofing** obtains IP addresses trusted by the org and modify packet headers to insert forged addresses.
- **Pharming** changes the IP returned by a DNS lookup so a user goes to a malicious website.
- A **man in the middle attack** sniffs packets, modifies them, and inserts them back into the network.
- Hardware failures/errors can occur when a manufacturer makes bad product.
- Software defects can be exploited easily, and are becoming more common as programming becomes a larger profession.
- **Buffer overflow** attacks allow target systems to execute instructions provided by the hacker themselves due to code

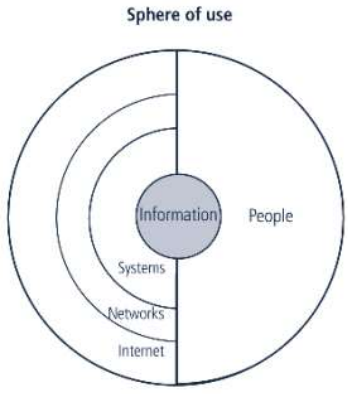
mismanaging memory.
- **Command injection** allows trusting code to be abused. Code takes user input and does not sanitize it, allowing for havoc to be wrought.
- **Cross site scripting** allows for info collection by injecting malicious code into a web page.
- Failure to handle errors or encrypt network traffic makes it way easier to intercept information.
- Tech can age and no longer be usable. If this happens to critical infrastructure, things can break easily.

H2 Babby

- The biggest gap in the knowledge of security professionals was their ability to understand the business.
- The four major business needs that establish the objectives of any security organization are:
    - Protecting the organization's ability to function
    - Protecting data and information assets
    - Enabling the safe guarding of the operation of applications
    - Safeguarding other technology assets
- All information security threat categories are listed in table 2-2.
- Attack types can increase and decrease. One that fell in frequency from 2000 to 2011, malware infection declined as users generally grew more savvy with internet safety.
- In 2013, PricewaterhouseCoopers reported hackers as the top source of attack/threat agents.
- A cost benefit analysis is used to monetize as many factors as possible in order to make decisions about implementation of designs.
- An **intangible** is an item in a business analysis which is difficult to monetize, but can affect other important areas of interest for the company like their reputation or morale.
- A datacenter operating at **five nines** or 99.999% uptime has less than 3 minutes of down time a year.
- **Intellectual property** is undocumented creations or knowledge of high value that is stored in the mind.
- Lack of training is a cause of human error.
- A potential risk of using pirated software within a business is litigation.
- An act of corporate espionage is the theft of IP from an outside corporate organization.
- Extortion occurs when an offer to return property to its rightful owner in exchange for something of value occurs.
- A polymorphic attack is a type of malware that can change itself to evade antivirus software.
- You know what a trojan is damnit.
- An example of an intangible asset it company reputation.
- Litigation is a loss to an org from pirated software use.
- If you hire out an outside firm to manage your servers, you can transfer risk onto them, but you are risking them causing downtimes to your application without your permission or involvement.
- We are about magnetic disk drive failures as large data centers operate thousands from different years of manufacture, and those are a lot of work to keep running and backed up.
- A threat is just the potential for attack, an attack is something that involves the attempted cause of loss to an asset.
- The deadly sins of software development:
    - Buffer Overflows
    - Command/SQL Injections
    - Failure to handle errors
    - Failure to protect/encrypt network traffic
    - Using pseudo-random numbers
    - Using an untrusted source in a formatted string
- Obsolescence threatens technology due to the potential to render data unavailable that you really need.

CHAPTER 3 (Homework and A Couple of Lecture Notes)

- **Laws** are formally enforced rules that mandate or prohibit certain societal behavior
- **Ethics** define socially acceptable behavior, both formally and informally. Ethics will differ between separate nationalities and ethnic groups. Setting proper expectations for ethical behavior can be done through education and training. Professional societies are the driving force behind ethics within info security.
- **Fair use** is an exception to copyright law which allows use of protected material under certain limited circumstances
- Doing your **due diligence** means informing yourself of laws that apply to you so as to make the best decisions you can**.** **Due care** means doing the right thing and abiding by them.
- **Policies** are a body of formalized expectations created by an organization. Enforceable policies are distributed, readily available to learn, easily understood and formally acknowledged. If you act in accordance with an illegal policy, you are still doing an illegal act. Effective policies are constantly evolving.
- **Standards** are built on top of policy, and instruct on how to comply with policy in specific detail.
- **Practices, procedures and guidelines** are detailed steps used to promote increased adherence to established standards.
- The **sphere of use** illustrates how people interact with information using a lot of mechanisms:
- The **sphere of protection** illustrates the wide variety of controls available to protect information at all interfaces within the sphere of use.

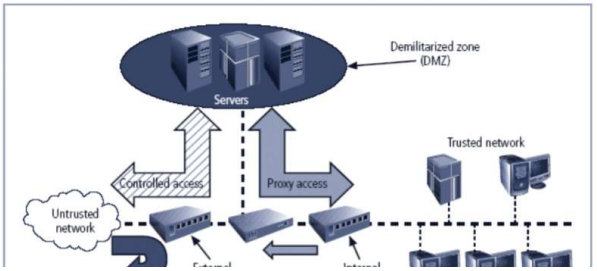


CHAPTER 4 (Homework and Lecture Notes)

- **Risk management** is a comprehensive process that can be split into:
  - Risk Identification
  - Risk Assessment
  - Risk Control
- "If you know your enemy, and you know yourself, you need not fear the result of a thousand battles" - Sun Tzu, Famed Book Guy Who Did War And Shit. In Risk Management, knowing yourself is risk identification, and risk assessment is knowing your enemy.
- **Risk identification** identifies, inventories, and categorizes your assets. These can be people, procedures, data, software, and other things. It specifies from those broad categories into specific assets. It then classifies, values, and prioritizes them. This action is done with a **weighted factor analysis**, which scores each asset based on the way it affects the business (financially, morally, legally). After this, it identifies and prioritizes the threats to those assets. This is done the same way as your asset identification. Then it finally specifies asset vulnerabilities. It does this using the **threat/vulnerability/asset matrix**. This matches the threats that apply to assets with the assets themselves, creating a vulnerability.
- **Risk assessment** determines the frequency of loss, as well as the magnitude of losses, and calculates risk, finally assessing risk acceptability. This step in the risk management process basically estimates the risk of each vulnerability taken from your TVA matrix. The **estimated risk** is calculated as the likelihood of attack * likelihood of successful attack * estimated magnitude of the loss caused by the attack. Based off of these estimates, the **ranked risk vulnerability worksheet** is created. This lists every vulnerability, the impact it has, the estimate risk, and the **risk rating factor**, which is the impact times the estimated risk.
- **Risk control** selects control strategies to deal with risk, justifies those controls, and implements, monitors, and assesses those controls. There are five separate control strategies:
  - Defense/Avoidance, where you attempt to prevent exploitation of the vulnerability through policy, education, tech, or a combo of all of these things.
  - Risk Transfer, which transfers non expert internal services to external expert organizations
  - Mitigation, which attempts to reduce the impact of an attack through planning and preparations. This involves an incident response plan, a business continuity plan, and a disaster recovery plan, which describe immediate actions, the continuation of basic operations, and recovery from a total loss respectively.
  - Acceptance, which does nothing to protect vulnerabilities. This is done when the cost of the loss is less than the cost of control.
  - Termination, where the possibility of risk causes a loss greater than the actual benefit to the business it is generating.
- To select a risk control strategy, you can run a **cost benefit analysis**, which evaluates the value of assets to be protected compared with the expense of the protection. You could also run **benchmarking**, which seeks out and studies practices in other organizations and tries to duplicated them. This allows to show due care, because you are doing as good as anybody else, and due diligence, as you are trying your best to remain informed of current practices. Finally, you could subscribe to **best practices**, which are security practices that provide a superior level of protection. To do this, you have to meld them to how your organization operates.
- California Polytechnic State Uni Best Practices:
- 1. **Install anti-virus software**
  2. **Update (patch) operating systems, applications, and antivirus software regularly**
  3. **Use strong passwords**
  4. **Log off public computers**
  5. **Back up important information ... and verify that you can restore it**
  6. **Keep personal information safe**
     - **Be wary of suspicious e-mails**
     - **Pay attention to browser warnings and shop smart online**
     - **Use secure Wi-Fi connections at home and away**
  7. **Limit social network information**
     - **Stay off of facebook**
  8. **Download files legally**
  9. **Lock your computer when you walk away from it**
  10. **Secure your laptop, smart phone or other mobile devices**

CHAPTER 5 Firewalls (Just Lecture)

- **Firewalls** prevent specific types of information from moving between the outside world and the inside world. It can be a separate computer system, a software program running on an existing router or server, or a separate network containing supporting devices.
- There are five types of firewalls, and they are categorized by their place in the TCP/IP Stack:
  - Application gateways are stored in the application layer
  - Circuit gateways lie in the transport layer
  - Packet Filtering lies in the network layer
  - MAC layer firewalls lay in the link layer
- **Packet Filtering** examines the headers of data packets, based on a combination of the IP source/destination, direction (into the server, out of the server), and the TCP/UDP source/destination ports. Simple firewalls can enforce rules based on certain addresses and ports. **Static filtering** has the rules that define what packets get through be developed by a human. **Dynamic filtering** allows firewalls to react to emergent events, and create/update rules based on those events. **Stateful inspection firewalls** keep track of each network connection between internal and external systems using a state table. Think UFW on Ubuntu.
- **Application gateways** are installed on a dedicated computer known as a **proxy server**. These are usually placed in the **DMZ**, an unprotected layer of the network, which means it has a higher level of risk of attacks from untrusted networks. You can add more filtering behind the proxy for more protection.
- **Screened Host Firewalls** combine packet filtering with a separate dedicated firewall like a proxy. Allows a router to prescreen packets, which are then sent to the proxy in an effort to minimize proxy load. This proxy is called the **bastion host**, and is a rich target for attacks from the externet.
- A **dual homed host firewall** has a bastion host with two NICS, one connected to the internal network and one connected to the externet. This allows for the internal card to have routing on completely separate IP addresses using a technology called **NAT**.
- **Screened subnet firewalls** place two bastion hosts behind packet filtering routers between the BH's, the external network, and the internal network. The bastion hosts act as the DMZ.
- **IP Packets** include a source and destination IP address, as well as a checksum for error checking, protocol version, flags, as well as the data in the packet.



called **NAT**.
- **Screened subnet firewalls** place two bastion hosts behind packet filtering routers between the BH's, the external network, and the internal network. The bastion hosts act as the DMZ.
- **IP Packets** include a source and destination IP address, as well as a checksum for error checking, protocol version, flags, as well as the data in the packet.
- You can use 0 as a wildcard character to select anything within the x.x.x.0 address range. To prevent IP spoofing from the external network, block any traffic coming from your internal network. Keep this as the first entry. Then, block any external address to your external firewall and DMZ, as well as any traffic from the firewall to prevent spoofing. Next, allow the services needed over specific ports from specific IPS in your internal network. Finally, deny all other traffic.

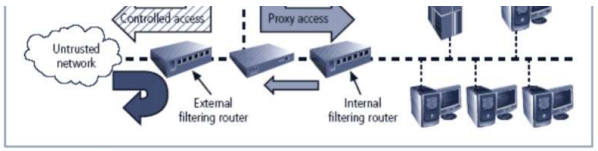


FIGURE 6-13 Screened Subnet (DMZ)

Intrusion Detection
- The function of an IDS is to:
  - Detect malicious activities and attacks
  - Raise alarms
  - Log Events
  - React to attacks
- A **false negative** is the failure of an IDS to react to an actual attack, and a **false positive** is when an alarm goes off indicating an attack when no attack exists.
- A **confidence value** is the certainty with which an IDS detect attacks and intrusions.
- There are a couple of types of IDS detection methods and operational methods.
- Signature based detection type IDS examine data traffic in search of patterns that match known signatures. This means that we have to constantly update IDS databases with signatures of new attack types, and if we do not have those, we cannot detect an attack. It has low false positives, but low detection for zero days.
- Statistical Anomaly Based detection type IDS compare current traffic activity to a control traffic activity sample. If there is a significant difference between the two samples, an alarm is raised. This can detect zero days and other new attacks without a database, but takes more processing power and generates a lot of false positives.
- A NIDS, or Network IDS resides on a PC or appliance in an org's network and looks for signs of attacks within packets. It watches all network traffic going into and out of the network segment it monitors. A few of these can monitor a large network, are passive and do not disrupt normal traffic, and are not susceptible to direct attack. However, they cannot work with encrypted traffic, can be overwhelmed by network traffic, and needs access to all traffic. Tricks can be used to get around these, like fragmented packets.
- Host Based IDS, or HIDS, reside on computers and monitor activity on that system only. It monitors the status of key system files, and can detect when these are changed. Most detections are done when something is changed on the system. It can usually detect things that elude network based IDS, can access encrypted traffic, and can protect specific hosts much more effectively. Managing them is a pain in the ass, can wear down system performance, and can be directly attacked by malware.
- Application IDS monitor applications ONLY for attacks.
- To evaluate the effectiveness of an IDS, we use two metrics. We evaluate the number of attacks detected in a known sample of admin generated attacks. Then, we evaluate the level of use (network traffic, processing power) that IDS fail at, meaning at what point of strain do they stop detecting attacks.
- A honey pot is a decoy system designed to lure potential attackers away from critical systems, and to attack the pot itself. A honey net is a subnet of honeypots. A padded cell is a protected honeypot. The legal use of these is not well defined. And they can piss off attackers, which will probably attack the organization more in some kind of egotistic personal redemption.
- The act of footprinting is the research of internet addresses owned and controlled by a target organization. Fingerprinting is the research and survey of all of these addresses, where operational nature of the network is revealed. To do things like this, we use port scanners and firewall analysis tools to find IP addresses with leaky ports, and exploitable holes in organization firewalls. Packet sniffers are used to intercept useful data on a network as well.

Cryptography
- Cryptology encompasses both cryptography and cryptanalysis.
- Cipher methods include:
  - Encrypted plaintext through bitstream methods, where each bit is transformed into a cipher bit one bit at a time. An example of this is a XOR cipher, where each bit of each character is XOR'd with a key.
  - Block cipher methods, where the message is divided into blocks and each is transformed into encrypted blocks of cipher bits using an algorithm and a key. An example of this is the block substitution method, where a simple substitution is used to encrypt cipher text, using ASCII 8 bit character blocks.
- XOR cipher weaknesses include repeating keys which can be used to map out original plaintext, and few different encodings existing for identical plaintext. Many XOR ciphers can be run on one piece of text and compared with known cipher text to figure out the XOR cipher used.
- For block ciphers, Known plaintext attacks also exist, where we know what some mappings between plaintext and ciphertext. There are also repeated letter attacks, where you feed the algorithm the same characters to see what weaknesses exist, or what patterns emerge. Frequency attacks can be used to determine specific plaintext characters based on patterns in the English language.
- Symmetric key crypto involves using one key used to encrypt and decrypt, with a key that must be kept secret. Asymmetric key crypto involves a private and public key. You can encrypt with the public key, and decrypt with the private key, so that anyone can send a message to only the person belonging to that public key.. This allows multiple people to encrypt something only for you.
- RSA uses large prime numbers to encrypt things as computing these is considered NP Hard. RSA is a famous asymmetric key algorithm that was cracked using electronic noise from computers running the algorithm.
- DES is one of the most popular symmetric encryption standards. It has a 64bit block size, with a 56 bit key. There are 16 rounds of XOR transposition operations. It got cracked.
- AES was standardized in 128 bit. It was cracked using acoustic monitoring, when the computer made different noises for each character encrypted.
- You can combine symmetric and asymmetric encryption in a hybrid. For example:
  - Encrypting a message with your private symmetric key
  - Encrypting your private symmetric key with recipients public key
  - Recipient gets package of key and message
  - Decrypts with public key
  - Decrypts with decrypted symmetric key
- A one-time pad is a robust symmetric key that is only used once, usually used as the symmetric key in a hybrid system. It is the most secure encryption known today.
- Digital signatures involve someone "signing" a document. They encrypt a message using their private key, and then add plaintext signature onto the document. This is then encrypted using the "authorizer's" public key. The auth then

decrypts using their private key, see the signature, and use the sender's public key to decrypt the message to ensure it came from them.

- Digital Certificates are electronic documents containing key values and identifying info about entities that control keys. A signature attached to certificate's container file to certify file is from entity it claims to be from
- A Julian Cipher is a Caesar cipher