In reference to the CIA triad slide from 8/22

These 3 concepts (Confidentiality, Integrity, Availability) can be connected. A disruption/breach of one objective, such as confidentiality can lead to an availability concern which can then lead to another confidentiality concern. Cycles can occur.

Security Objectives

- Prevention is more fundamental than detection
  - It is not however 100% obtainable due to the fact we don’t always know how a breach will occur. And in some cases, even if we do know, we still can’t always prevent it. This leads to Detection playing a large role.
  - The system used to detect (Intrusion Detection System) a compromise in the base security system, must itself be protected (by prevention) from compromise which illustrates why prevention is more fundamental that detection
  - If detection is compromised, then the underlying security system can also be compromised

- In addition to Confidentiality, Integrity, and Availability, system security must also have the following traits:
  - **Authenticity** – similar to integrity, but pertaining to a representation of a person (e.g. e-mail address) as opposed to data.
    - An example would be that an email someone receives from a friend was actually sent by that friend, and not from an attacker who forged the friends address.
  - **Accountability** – helps deter attackers by holding them responsible and creating a means to prosecute them. Ensure people answer for their actions.
    - Helps investigators understand the situation and what happened. Aids forensics
    - It is gained importance because more and more attacks are being performed from within the system by someone with intimate knowledge. This is known as Insider Attacks. An example of an insider is when Stuxnet, a virus used to cripple Iran’s Nukes, was delivered via a thumb drive.
    - An example would be that computers are identified with IP addresses, a way to connect a suspected attacker to a particular attack
  - **Non-repudiation**—is related to accountability by the scope of denyability
    - In order to have proper accountability, an attacker must not be able to deny being involved.
    - It is hard to be 100% certain of a person’s involvement
      - One reason for this is because IP addresses can be manipulated/forged
      - Question: Who holds attackers accountable?
        - Answer: since there are no national boundaries on the net, it is often a collaboration between nations to enforce accountability

Levels of Impact
● It is important to note that system security is a relatively new science, and as such has no quantifiable models by which to create standards of comparison. In other words you can’t say we have achieved a 92% on our security rating.
● Instead the models used are qualitative, and things like impact are judged subjectively
  o i.e. low, moderate, high

**Computer Security Challenges**

● Cross-cuts all levels of IT and therefore complex
● Must account for users who are not able to recognize threats (e.g. dangerous links) as readily as security personnel.
● Security by Obscurity, or making a system increasingly complex as a means of making it more secure can be good or bad
  o Argument against: Doesn’t work since people are becoming more skilled
  o Argument for: Could work because a decoy could be built into the system. Deceives attacker.
● Approaches such as cryptography, involve keeping secret info a secret. This means we trying to keep a secret safe with a secret.
● Should tools be deployed at all weak spots?
  o Becomes a matter of weighing the cost of implementation against the cost of security breach at each weak spot.
  o Can also make a system too complex for regular users which can also be thought of as a “cost”.
● An attacker just needs to exploit one weak spot, whereas admin must account for every one of them with finite resources.
● It is difficult to show a return on the investment in security, until after it is needed and therefore difficult to obtain resources from CEO.
● Can be regarded as an annoyance to a regular user who doesn’t consider the need for a system.
● Requires continuous monitoring of the system as well as the monitoring of all attacks that are happening in the world in order to understand what you might be going up against it.
  o Side note: on average a new machine connected to the world is probed in 2 mins.

**Computer Security Terminology**

● Be familiar with the definitions of the following terms located in the book:
  o Adversary (threat agent)
  o Attack
  o Countermeasure
  o Risk
  o Security Policy
  o System Resource (Asset)
  o Threat
  o Vulnerability

**Systems Security Components**

● Components are connected to each other (see UML diagram from 8/24 slides)
  o A cycle can be found between countermeasures and vulnerabilities, for instance
A patch to fix one issue can often cause problems in other software and may even make that software vulnerable
  - This is because patches are tested in isolation and cannot be tested on every user's workspace

**Vulnerabilities, Threats, and Attacks**

- Attacks can be passive: such as eavesdropping
- Or active: where an attacker is interacting with the system

**Achieving Security**

- Security is made up of Policy, Mechanisms, Evaluation, and Assurance
  - This class will focus on policy and mechanisms
- Security Policy – what needs to be secured
- Security Mechanisms (Countermeasures) – how can security be implemented?
  - This class will focus on the prevention and detection aspects because they don't involve legality, as deterrence does
  - Will also touch on response and recovery

**Questions:**

**In-Class Questions:**

1) how do we really hold somebody accountable, if entity is not under jurisdiction?
   - It’s where international law steps in. However, there’s still a scope of deniability that comes with an attack. You can’t normally de facto prove someone’s accountable. For example, IP addresses are completely forgeable.

2) You may not be able to defend all fault, when you had unknown attack? what will be your action, when you have all tools to defend? OR what will you do as system administrator?
   - No, we may not be able to do so.
   - I thought the answer is we are not able to do so due to the cost...?
   - He said it depends. There’s tradeoffs and it’s situational. We can't ever foolproof a system so it can be costly preventing things and sometimes if a system is hit it may not be worth the resources to defend.

3) Can humans be considered a weak spot?
   - Yes, humans are the weak spot.

4) How do attackers discover weak points and learn about the systems that they're attacking?
   - Probe the defense until find the weak point.
- The attacker uses an attack vector, sees if certain information is available, attempts different probe missions, attempts to go through different ports, phishing emails, et cetera. There’s a plethora of things they can do.

5) How do people hack the cloud?
   - Scope too large for class. Many different techniques, for instance, phishing.

6) What does the cryptocurrency security field look like?
   - I believe it was along the lines of “It is theoretically secure but the devil is in the details. It is practical and usable. Sometimes misused due to lack of understanding”.

7) Is the use of COBOL by some financial systems an example of security by obscurity?
   - I would not say so. COBOL is still being used because there are too many legacy systems design using COBOL and it will be too costly to upgrade them.

8) How are security risks prioritized?
   - Cost of protection vs cost of recovery of attack.

9) Can you provide an example of a low level impact intrusion?
   - Low impact is subjective to the business/entity. Changing the headline of a NYT web article to a joke might be low impact.

10) Would it be worthwhile to leave a specific weakness at risk as bait, assuming it can be isolated from the system?
    - He didn’t really cover much other than saying that they do do this. He said something about “honey pot” and “honey net.”

11) Is it possible to design a system that can detect it is being attacked and thus the system attacks the attacker?
    - Yes this is possible. There is a whole branch of security work that dwells on offensive warfare.

12) Why do ads become compromised by malware?
    - Question was not very clear. In general ads are pieces of software scripts. So they compromised the same way that other software gets compromised.

13) How do attackers forge a public IP assigned to a different area without being tracked?
    - This wasn’t a question he answered. He said that people can forge IP addresses as an example of scope of deniability. (See question 1)

14) Can you use a VM to mask your identity when launching an attack?
    - You can, but the IP address is still physical. However, utilize VM is a great way to practice defense from hacker.
    - He said that you can have a cluster of VM’s with the same IP address so it could be useful...
15) Why are USB’s so insecure?
   - They’re very portable. It has a plug and play feature, where the machine recognizes the drive and just launches it. Like with floppy drives. They’re read/write devices. Because of all of this a lot of US Government machines won’t allow jump drives.

16) Is it more difficult to design a secure system or attack one?
   - It’s certainly harder to design a secure system. Generally, with more code and larger applications, they have more vulnerabilities.

17) So older tech is generally more secure?
   - Yes, cutting edge technology has more unknown vulnerabilities. We’ve dealt with corner cases of older designs more so they’ve become more secure.

Note: I changed some of the questions to red because they either weren't actually answered or the answer was brushed off. They're not really helpful to keep in the document. Also, where did a lot of these questions come from? Were they just from the list that he never actually got to?