Foundations of Information Security

1. Why can you not fully trust and code that you haven’t written yourself?

You can’t fully trust code that you haven’t written yourself because you don’t have a full understanding of what the code does when it’s written by someone else, so you could be overlooking built-in exploits or weaknesses in the code.

1. Schell defined threat in terms of four levels of computer misuse, three of which are: Theft of computational resources, Disruption of computational services, Unauthorized information modification and one more. What is the fourth level of computer misuse?

The fourth level is Unauthorized disclosure of information in a computer.

As a list the levels are:

* Theft of computational resources
* Disruption of computational services
* Unauthorized information modification
* Unauthorized disclosure of information

1. Schell and Schneier both address the notion of threat. They come at the question very differently. How do each describe their vision of threat.?

Schell views threat as the possibility of someone helping exploit a vulnerability by disclosing or modifying information without authorization. So they view it through more of a technical, information oriented, lens.

Schneider views threat more literally, saying that threats in the cyber world are very similar to threats in the physical world, in that they all disrupt someone’s life, and could both even cause physical harm.

1. What are the four parts of a threat?

NA

1. What is the difference between privacy and anonymity?

Privacy is the idea that the system knows an identity but doesn’t tell anyone about it.

Anonymity is where the system doesn’t know and can’t possibly tell anyone about it.

So the key difference lies in the fact that in privacy the system knows, but in anonymity the system doesn’t.

1. What are some of the hazards to information assets?

Some of the hazards to information assets are:

* The unauthorized disclosure of information (Confidentiality Loss)
* The unauthorized modification of information (Integrity Loss)
* The disruption of authorized access to information (Availability loss)

1. What are three factors that affect the ability to prosecute cyber-crime?

Three factors are:

* The lack of actual physical evidence which is typically needed to prosecute someone for a crime.
* The lack of understanding of how a crime was committed, it’s hard to prosecute someone when the extent or details of the crime are hard to describe or understand.
* The age of the defendant, since it’s pretty typical to find someone very young committing cyber crimes.

1. What legal purpose is served by following “best practices” in computer security?

The purpose served by following ‘best practices’ is that of assuring that your system won’t be exploited by an attack/exploit you’re already aware of. Basically so that nothing malicious that is already known gets the better of you.

1. What are the four main components that constitute THREAT?

NA

1. What is the formula for risk we are using in this class?

The formula we are using is:

* Risk = Threat X Consequences

1. What are the specific descriptions of the three elements of the CIA triad?

* Confidentiality means the data is only accessible to specific parties.
* Integrity is the certainty that the data has not been tampered with or degraded.
* Availability means that the information is available to authorized users when it is needed.

1. What is the singular differentiator that distinguishes cyber security engineering from all other engineering disciplines?

The singular differentiator that distinguishes cyber security engineering is the fact that cyber security engineering involves working against the efforts of an *actual adversary*, one who is persistent and malicious.

1. Considering the answer to question10, What is it about the digital/computer/cyber context that makes determining a meaningful quantitate value for Risk so difficult?

The thing about the cyber context that makes capturing a value for Risk so difficult is the fact that the elements that define Risk aren’t very knowable, and so it’s hard to defend any basis you make for quantifying Risk.

1. We have looked very closely to the use of the word "secure" in the cyber security context. What have we concluded is wrong with the conventional use of the word and how do we recommend changing the use of the term?

What we have concluded was wrong about the conventional use of the word is that it doesn’t really explain what is being protected, or what the goal is.

We recommend changing the use of the term to reflect the reality that security to us means Information Assurance.

1. According to "Secrets and Lies" Schneier asserts that physical threats mirror those in cyber space, but the attack characteristics are different. He further asserts that cyber space has three distinct attack characteristics not shared with the physical threats. One of which is: Automation. What are the other two characteristics? In a few words please explain what Schneier has in mind.

The other two characteristics are:

* Action at a Distance
* Technique Propagation

1. As this is a course on the foundations of information security, naturally our focus is centered on information. The concept of information has existed since the beginning of civilization, and in fact, it’s not farfetched to say that modern civilizations today have being built on a foundation of deep-rooted and categorically distinct information sets that have contributed to the growth and development of cultures, science and technology. Yet, the one thing that still stands ambiguous is the proper definition of information. What is the definition of information given by Shannon that we use and is considered to be the closest proper definition?

The definition given by Shannon that we used is that information is ‘That which reduces uncertainty or chaos’.

1. Within preliterate communities, how was sacred confidential information, protected? What is one big problem with this traditional solution?

Sacred, confidential information was protected by keeping the information with the Shaman of the tribe, who’s role was to remember all of this sacred important information. One big problem of this solution was that when the Shaman died (especially if he died unexpectedly) all the sacred information would be suddenly lost.

1. The intention of the bag guy has no practical limitations. However, the whole broad spectrum of the bad guy intentions can be more of less rolled up into one short phrase. What is that phrase?

NA

1. This course advances the idea of an Information Domain. Define and describe an Information Domain and explain why it is so important.

An information domain can be defined as the collection of:

* Information objects
* Users
* Policy

Information objects are self explanatory, they’re literal information.

The Users are those who would possibly use the info.

Policy would be defined as the expectations of what the user can do with regards to the information

This domain is incredibly important do define as it gives you an explanation of what you need to protect when you’re building anything that has to do with information, it helps provide the starting grounds of talks over information assurance.

1. What is the fundamental task of the cyber security engineer?

The fundamental task of the cyber security engineer is to attenuate the threat to an acceptable level of risk.

1. What is the notion of attack surface and how can you quantify an attack surface?

The notion of attack surface is that of all the entry points for someone to attack your system. You can quantify an attack surface by locating every possible point of entry, which would be every location (or part of your system) where a vulnerability can arise.

1. Can you make that case that DEEPFAKES are a violation of one or more of the three principles of information security

I could make a case that DEEPFAKES violates integrity, as it gives an ‘inauthentic’ image of something.

It’s somewhat difficult to make the case that DeepFakes violate a principle as they are technically ‘Authentic’ images in how they’re good enough to paint a very ‘correct’ image of reality.

1. A widely held belief is that cyber criminals need more skill than their traditional counterparts. However, another school of thought believes that exactly the opposite is true. Comment.

I believe that cyber criminals DO NOT need more skill than their counterparts simply because their counterparts need to account for an insane amount of factors to ensure that cyber criminals can’t exploit their system. A cyber criminal, on the other hand, needs only to find one vulnerability to accomplish what they’re after, but their counterpart needs to search endlessly, patching multiple vulnerabilities continuously.

1. Why do laws, in particular cyber laws always seem to be so behind the technology?

Cyber laws always seem to be so behind the technology because laws relating to technology are only ever really written to resolve particular events, so they’re not really forward looking, they’re just patched in to fix things that have already gone wrong, instead of setting standards and goals to keep up with the technology.