**CS 361 Week 1 Questions**

**Lecture 1**

1. Personal Security, Network Security and System Security.
2. These relate to one another because there is private information about myself on my computer system and if someone were to infiltrate my system through another network I was connected to, my personal security is at risk.
3. When I was a young kid, my computer received a virus from an email I opened in my spam folder. At the time, I did not know what a spam folder was and my computer became infected.
4. I do not think my computer is infected, but it could be infected without my knowledge.
5. My computer has a minimal amount of security at the time. I try the risk avoidance approach mostly.
6. The security measures I take are not very effective.
7. I believe the quote is spot on. Reason being, our world is be connected through the network at the click of a button. Once someone becomes inspired to take down the whole system, they will find the one little loophole that can tear our country along with others. All the disasters in the world's history happened because there was a conspiracy that nobody was prepared for, and it can happen without a moments notice.
8. Learning computer security allows an individual to take more cautious measures when on the computer. Most security breaches on an individual happen because they did not know they were at risk. Educating yourself on computer security will be beneficial for everyone now and in the future.

**Lecture 2**

1. Being careful around the people you work with or are close to through friends and family. No one truly knows the intentions of another person, and those people could take advantage of your little knowledge about security to steal right in front of your eyes without you noticing.
2. There are steps to be cautious about the "bad things" that could happen to your program, but there is not a full proof system to figure out everything because perfect security does not exist.
3. The difference is simple between the defender and the attacker. Defending takes in account for all things to not come through the line of defense. There are multiple factors on how to handle many situations. While on the other hand, the attacker has to find one single break in the defender’s line to corrupt the whole system. The job of a defender has to always be one step ahead of an attacker.
4. The only way to ensure perfect security is to not have any risk at stake. It is like playing poker at the casino. Your best chance at making sure you do not lose any money is by not gambling at all.
5. Tradeoffs are typically required because sometimes the cost and struggle of protecting a part of the system is too much to handle. Therefore, sacrificing a part of the program will help avoid the attacks.

**Lecture 3**

1. Risk is the possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability.
2. We manage risk on a daily basis whether it is what we eat, where we commute, when we sleep, etc. The same goes with computer security and managing the risk in a logical way can help prevent the system be efficient in the best way possible.
3. A risk I accept would be not taking the precautions to my computer system when it says I am at risk of security when accessing a webpage that I believe is secure. A risk I avoid would be entering my social security to websites that “require” it for a sign-up or application. A risk I mitigate would be bringing my other laptop on vacation because if I lose that laptop, I won’t be as upset if I lost my good one. A risk I transfer would be using a friend’s login to watch movies, and if his parent’s get kicked off from too many users on the account, he will get blamed and not me.
4. Annualized Loss Expectancy can help hash out the numbers when managing the security risk on a system. Knowing what cost would be cheapest but most beneficial to a system through either accepting, avoiding, mitigating, or transferring a risk can give a company or person a number on how their system/program stands.
5. Assess assets, threats, vulnerabilities, risk, prioritize countermeasure options, and make risk management decisions.

**Lecture 4**

1. The key distinctions between the two slides is that the first slide explains the big security measures someone should look out for in protecting, and the second slide uses examples of tools that help defend the system from those kind of security breaches from the first slide.
2. As a student, availability would mean a little more than the others because I tend to go to the Internet for help or guidance in the right direction for everything. If most websites are down due to security reasons, it hinders my ability to find a solution to my temporary problem and causes my time to be used in a non-efficient way.
3. Grouping and categorizing data allows someone to group similar data with an associated security risk and categorize which data is most important compared to the group.
4. Authorization may change over the years to prevent hackers from breaching the systems integrity. Measures will become more secure to prevent anyone from accessing content they should not get their hands on.
5. Security and reliability relate because if a website does not take the proper measures to ensure their availability security, their reliability as a website will take a huge shot and could cripple the whole website if the security process is not taken seriously.
6. Authentication and non-repudiation are considered when buying things off the Internet. Considering if this site can be trusted and authentic can help consumers from being ripped off for their credit card information. If the website decides not to give you what you ordered and just steal your information, this ties both authentication and non-repudiation together.

**Lecture 5**

1. A metapolicy for a cellphone network could be protect the identities and phone numbers of customers from being accessed by fake telemarketers, random numbers, etc. A metapolicy for the military database is making sure no one gains access to the database that does not have the appropriate credentials.
2. The policy is needed because it provides specific and enforceable guidelines to the system user/developer.
3. The policy can have the three policies: Only the appropriate staff can change and access the student’s records, The student can access his/her’s records but cannot change them, and make sure no one outside of the student and the appropriate staff members have access to viewing the student’s records.
4. A stakeholder could have conflict with the policy if they believe the student’s parents, in the example above, should have access to the student’s records.
5. The example’s metapolicy would likely be protecting the confidentiality of a student’s SSN.
6. Not understanding the metapolicy would make it difficult to implement the policy because the policy would seem arbitrary.

**Lecture 6**

1. The military is mainly about confidentiality because they do not want anyone that is not authorized to access the information they have available for the appropriate people. The military is not worried about the integrity or availability.
2. The major threat is making sure no one that is not authorized to view the documents gains access to them.
3. The proviso is only concerned with the confidentiality of the information and nothing else.
4. The labels contain the hierarchical component and the set of “need-to-know” categories. Ex: ([hierarchical component]: {“need-to-know categories”})
5. We are not worried about how the labels got there because they were made for the appropriate people to access.
6. Level of sensitivity going from most sensitive to least: 1) The Normandy Invasion is scheduled for June 6. 2) The British have broken the German enigma codes. 3) Col. Jones just got a raise. 4) Col. Smith didn’t get a raise. 5) The base softball team has a game tomorrow at 3 pm. 6) The cafeteria is serving chopped beef on toast today.
7. 1) (Top Secret: {Personnel}) 2) (Secret: {Crypto}) 3) (Confidential: {Personnel}) 4) (Confidential: {Personnel}) 5) (Unclassified: {Personnel}) 6) (Confidential: {Personnel, Janitorial})
8. For mixed documents, use the highest confidentiality with all the appropriate categories.

**Lecture 7**

1. The “labels” on humans indicate the classes of information a human is authorized to access.
2. For a document, it only has one label and can only be seen if accessed by authorized personnel. Documents differs from Human labels because the label for humans allows them to access anything at or below their hierarchical component and within their categorie(s).
3. In computers the documents are stored in folders within the system and the people can gain access to these documents if they have the password to the system.
4. The Principle of Least Privilege works because when someone has access to material that does not pertain to their job or assignment could possibly be leaked through them.
5. The first row could make sense because at the higher level they may need something from a lower level to finish their assignment. The second row makes sense because the individual is not qualified to access top-secret information. The third row makes sense because it seems to be public information for the military base that anyone can have access to.

**Lecture 8**

1. The vocabulary terms listed are essential to the process of authorizing an individual’s access to certain documents.
2. (L1, S1) dominates (L2, S2) iff (1) L1 ≥ L2 and, (2) S2 C S1 --> (L1, S1) ≥ (L2, S2)
3. It is not a total order because neither label (L1, S1) ≥ (L2, S2) nor (L2, S2) ≥ (L1, S1)
4. An individual requesting access to view a document must dominate the sensitivity of the label in order to gain access.
5. The reason it is “only if” instead of “if and only if” is because an individual could dominate the sensitivity of the label but there could be a person who was recently banned from accessing any documents. This would require the person to be flagged when trying to access the label and then be denied.

**Lecture 9**

1. A person with clearance to a Top Secret document can access the document, write down the information, and then stick it into a folder labeled Unclassified. This would violate the military’s confidentiality.
2. There needs to be constraints on write access because loose restrictions can compromise the military’s confidentiality.
3. Computers do not have a face opposed to a person. There is no way to trust another computer even if you know the person that has access to it.
4. The subject S can only gain write access to the subject O only if O dominates S. Which means you can not write down to a lower level.
5. The subject can only “read down” and “write up” at their associated level.
6. The Private does not take orders from the General over the computer to prevent any leaks in the system security.
7. That is a problem of integrity, but to solve this problem there could be an approval from authorized personnel to write the plan.

**Lecture 10**

1. The Weak Tranquility Property would allow the upping of an object level but would deny lowering the object level. Also, prohibits moving the subject up levels to gain access to information they are not authorized to view. Lastly, moving a subject down could be detrimental to the confidentiality because the subject could bring information previously accessed down with them.
2. Strong Tranquility wouldn’t allow for any changes for the whole lifetime of the system, and this would make it impossible for anyone in the system to level up or add subjects throughout their military career.
3. Lowering the level can be dangerous because of the information previously accessed can be pulled down with them to the lower levels and breach the confidentiality.
4. A person with a stateless subject would possibly be able to level down.

**Lecture 11**

1. All the subjects would be at a high security level and all the objects would be at a low security level.
2. The matrix would be too big to realistically utilize for a large BLP system.

**Lecture 12**

1. (L,{A}) ----------> (H,{A})
2. LUB = (Lx, {y}) --------> (Lx+1, {y}) only if (Lx, {y}) ≤ (Lx+1, {y}) GLB = (Lx, {}) --------> (Lx, {y,…,z}) only if (Lx, {}) ≤ (Lx, {y}) ≤ (Lx, {y,…,z})
3. The upward flow is the metapolicy because the lattice system if following the policies of the metapolicy to ensure the BLP system works.

**Lecture 13**

1. The BLP rules will allow L to flow information to H and H can view the flow but not flow information to L. This would satisfy the BLP conditions.
2. READ satisfies the BLP rules because the only way to READ an object is if the object exist and the LS ≥ LO which ensures the subject dominates the object. WRITE satisfies the BLP rules due to the vice versa of the READ rules which is LS ≥ LO satisfying that the object dominates the subject.
3. CREATE satisfies BLP through creating a new object if it does not exist and the level of the subject ≤ object. DESTROY satisfies through the vice versa of the CREATE statement.
4. The way for the slide to be true is if the high level subject and object is not created. This allows the covert channel to succeed and violating the BLP conditions of transferring info from high to low.
5. The DESTROY statement allows the lower level to view the bit sent.
6. Yes, the example in slide 5 shows that the low level saw 0 bit when the high level subject and object were created, but when they were not, the low level saw bit 1.
7. Yes, because using the covert channel mechanism will allow them to transfer information form high to low through single bits at a time and the low level just doesn’t have to change to view the information differently.
8. The high has to change so the bit can be manipulated each time through creating and not creating the high-level subject and object.
9. If SL were to be able to see bits at a time, using a loop would allow SH and SL to transfer information from high to low and that would violate the BLP conditions.

**Lecture 14**

1. It is not a covert channel because it was a human-to-human interaction and that would not qualify as a covert channel. This was just an example of someone not keeping their mouth shut on private information.
2. No, because SL would read 0 in both instances.
3. The bit resides in the Resource not found or the Access denied attempt from SL.
4. The bit resides in the system clock based of the time.
5. The bit resides in the cylinder closest to the read head.
6. The bit resides in the control flow of the system.
7. A termination with low-bandwidth can tell the lower level which bit based on the appearance of a “slow” transfer.
8. The low level process can sense the power usage and the high level can modulate the power usage that provides a path to distribute information.
9. Power channels could be utilized through phone information.

**Lecture 15**

1. Though the bandwidth is low and slow, the system operates at thousands of bits per second and can transfer a lot of information despite the low-bandwidth.
2. It is infeasible because the system cannot sacrifice too much to where the system has been rendered to nearly inoperable.
3. They can modify the system implementation, lower the bandwidth, or monitor through intrusion detection.
4. A sender and receiver must share an object. The sender must be able to modify the attribute while the receiver can view that attribute like a system clock. Lastly, the sender and receiver must have a process that allows them access the shared resource.
5. The sender and receiver can utilize the process by modifying and monitoring the system clock to pass information.

**Lecture 16**

1. The R wouldn’t exist because the resource does not exist, yet. This would be a new resource being introduced to the matrix.
2. The R & M in the same row shows that someone can potentially modify it and another can view. It is just a potential instance for a covert channel to exist.
3. No because the new row would eliminate someone from viewing something from the above row if they are not authorized.
4. Creating the SRMM table would allow someone to view possible covert channels and this can make it easy to close these holes and prevent security breaches.