UTEID: dpk326
FIRSTNAME: David;
LASTNAME: Ko;
CSACCOUNT: davidko;
EMAIL: davidpeterko@gmail.com;

CS361 Questions: Week 1
These questions relate to Module(s) 1. Type your answers and submit them via
email to the TA by 5pm on Thursday, June 11.

Lecture 1
1. What uses of the term “security” are relevant to your everyday life?
Security can refer to physical security, like home protection, or it can be related to informational security
at your job where you must protect valuable information that the company gives you. Financial security is also
relevant to our everyday lives; we must protect our investments from thieves and our cash/bank account.
2. What do these have in common?
They are require a type of authentication or a means of access. For example, for home security, to bypass the
alarm, you would require a 4 digit pass code to turn it off before the police is notified. For credit card/bank
account it is similiar, you have a pin code you must enter before transactions can occur; bank accounts have account
numbers and passwords for online access and etc.
3. Have you been a victim of lax security?
Yes, everyone has. Not every security measure is 100% adamant, and there will be instances of lax security.
4. What is the likelihood that your laptop is infected? How did you decide?
There is probably a 65% my laptop is infected. You can run several spyware or virus scanners on your computer
to be definitely sure. Or you can just use an eye ball test`and see if your computer is doing very slow things or
acting slow and not processing the right programs in the intended way.
5. What security measures do you employ on your laptop?
Always use a secure shell when doing access, enable anonymity in your browser and avoid clicking on random links
that you do not know the destination of where they lead to. Having a very good firewall also is a very good way to
prevent intrusions.
6. Do you think they are probably effective?
They are good enough to eliminate small-medium threats (such as using McAfee or something similiar), but for lagre
scale attacks or worms/scripts you would just need to be able to

avoid places on the internet or just not be connected
to the internet to avoid these.
7. Consider the quote from the FBI official on slide 10. Do you think it overstates
the case? Justify your answer.
No, I do not think it overstates the case. The cyber security and cyber attack issues right now are mos definitely
serious. Countries such as China are producing more and more attacks on the US everyday and I have no doubt in my mind
that if they wanted to, they could hi-jack any computer system/ network in the US and do whatever they please.
8. What is the importance in learning about computer security?
Learning about computer security allows you to protect yourself from the dangers of the internet and cyberattacks
and help aware others of the problem. Also you can help prevent people around you from becoming attacked by providing
your own knowledge. As well as chasing a career in helping cover up and prevent the exploitation of these holes in net
works of the US.

Lecture 2
1. Consider the five reasons given why security is hard. Can you think of other
factors?
Other factors would include human nature. Some people are born talented with bright minds and sometimes that mind
is just biologically programmed to do bad things. You can't stop someone from doing something if it is all they know
The problem with the security issue is that there are numerous factors that could be in play at any given time. Technology
is constantly evolving and changing daily and eventually someone/ something will surpass its previous version and beat it or
destroy it.
2. Is there a systematic way to enumerate the “bad things” that might happen
to a program? Why or why not?
Debugging, test (specifically pen-testing) and finding all security holes starting from the compilation of the program
are as close as you can get. With so many components of a program, is it really hard to enumerate EVERY problem correctly
or entirely.
3. Explain the asymmetry between the defender and attacker in security.
The defender must keep its private or public key or information from being decrypted or stolen whereas the attacker
must work to take that information or find a way to break the encryption. The attacker will try to break the defenders
defense, the defender just has to be able to not be broken with negligible advantage.

4. Examine the quotes from Morris and Chang. Do you agree? Why or why not?

I do agree. As long as your computer is connected to an internet network, there will always be threats of a cyber attack. But that solution is not realistic, therefore we have people working daily to ensure a better future in the cyber world where cyber attacks will diminish or do minimal or negligible damage.

5. Explain the statement on slide 8 that a tradeoff is typically required.

By putting so much time and effort into security, it could also hinder or lessen the effectiveness of another area of the program/system that ordinarily wouldnt be affected. For example, if you put all the resources and energy into security, the time to market of the system will be enlongated and the launch will be delayed.

Lecture 3

1. Define “risk”?

Risk is the possibility that a particular threat will adversely impact and information system by exploiting a particular vulnerability.

2. Do you agree that software security is about managing risk?

Yes, by reducing the amount of risks, you are directly reducing the amount of threats/damage to be done in the future. Managing risk is a surefire way to prevent future problems in your software.

3. Name and explain a risk you accept, one you avoid, one you mitigate, and one you transfer?

1. insurance - sometimes the cost of insurance is greater than the potential loss. 2. disallowed remote log in 3. placing a hazard sign before the hazardous area to prevent people from entering that area. 4. home security systems.

4. Evaluate annualized loss expectancy as a risk management tool.

Using annualized loss expectancy to gather information on total loss to evaluate whether or not the risk is worthy of the fix is a very important fool for lots of companies. If the risk cost ot fix is way greater than the loss itself, then the assessment is that the risk can be ignored (in some instances). It also calculates the expected value of any security expenditure.

5. List some factors relevant to rational risk assessment

Technical, psychological, economical, financial.

Lecture 4

1. Explain the key distinction between the lists on slides 2 and 3.

The List on slide 3 are measures and tools that are used to apply to the list on slide 2 to help them.

2. Consider your use of computing in your personal life. Which is most important:
confidentiality, integrity, availability? Justify your answer.
Confidentiality is the most important to me. I want to be able to keep my information safe and to myself only
unless i want it to be shared. The would be no reason for security if Confidentiality didn't exist, everyone would
know everyones information.
3. What does it mean “to group and categorize data”?
To categorize the data into understable sections or groups to help differentiate the data from other data to be able
to see what to do with each data group.
4. Why might authorizations change over time?
Authorizations change over time due to just to never have the same passwords or access codes for too long of a time.
By changing them periodically it keeps the data protected. If an ex-emplyee has the passwords for something important,
if the password is not changed from tiem to time, the ex-employee still has access to delicate and important information that
he can access whenever he wants. By keeping the passwords and authentications fresh, it eliminates these risks.
5. Some of the availability questions seem to relate more to reliability than to
security. How are the two related?
Availability and relibility go hand in hand because data that is available 24/7, is also reliable. If a company goes down
and the data they someone needs cannot be reached or accessed, the reliability rating goes down. That company is not reliable
enough to keep its servers or information up for its customers/ business partners.
6. In what contexts would authentication and non-repudiation be considered
important?
If you pay amazon.com for an item with YOUR account, it is assigned to you, this prevents amazon.com from saying they
never recieved payment (non-repudiation) from YOUR accont for a specific service or item.

Lecture 5
1. Describe a possible metapolicy for a cell phone network? A military database?
For a cellphone company, the user must pay the company for usage on their cell phone network. For a military database, the users must be authorized employees that
are allowed access and must have their own unique log in to differentiate between
other users.
2. Why do you need a policy if you have a metapolicy?
The metapolicy just describes the security measures of the

overall service or situation. Where as a separate policy is system-specific of the metapolicy to proovide guidance to developers and users
of the system.

3. Give three possible rules within a policy concerning students' academic
records.

A student may only access his or her own academic records. Faculty or staff may not change a students academic record if they are not authorized to do so. Documentation containg the students academic record can only be accessed by specific faculty trained ot handle it and the student themselves.

4. Could stakeholders' interest conflict in a policy? Give an example.

Yes, thes stakeholder could have different ideas of the policy or company that conflicts with the policy set in place for the company. FOr example, the stakeholder wants a specific method of access for something, but the policy in place does not allow that.

5. For the example given involving student SSNs, state the likely metapolicy.

The metapolicy most likely states that no one other than the student can use the students SSN.

6. Explain the statement: "If you don't understand the metapolicy, it becomes
difficult to justify and evaluate the policy."

The metapolicy sets in stone the security measures of the system. If the person doesnt understand the overall impact of the metapolicy it will be harder to understand the reasoning for having the policy in place.

Lecture 6

1. Why is military security mainly about confidentiality? Are there also aspects
of integrity and availability?

There are different security levels to allow different levels of access to different personnel. Yes at different levels of access, there should be a higher level of integrity and availability based on how important that person is trying to access the information.

2. Describe the major threat in our MLS thought experiment.

Trying to differentiate and make confidential the difference between the sensitivity levels and the individuals permitted to acess the selected pieces of information.

3. Why do you think the proviso is there?

The proviso on confidentiality is there to allow the information to be secure and only available to the people authorized to access such information. Being confidential allows the information to be secure and unknown to outside forces that are not allowed to know about it.

4. Explain the form of the labels we're using.

Each part of the label (iunclassified, confidential, secret, top

secret) are there to provide different levels of access and confidentiality. Each piece of information is categorized into one of these labels to help separate the informations sensitivity level.
5. Why do you suppose we're not concerned with how the labels get there?

The labeling decisions are out of the scope of our concern. our only concern is being able to differentiate betwene these levels. Each comapny/person that creates these labels are different in their thinking to provide these labels.

6. Rank the facts listed on slide 6 by sensitivity.

From highest sensitivity level to lowest: 6, 2, 4, 5, 1, 3.

7. Invent labels for documents containing each of those facts.

Govt Secret for 6,2. Company Level for 4, 5. Community Level for 1, 3.

8. Justify the rules for "mixed" documents.

The mixed docuemnts are used to separate documents that both contain sensitive and non-sensitive information. You use the appropriate level and the category to separate the documents.

Lecture 7

1. Document labels are stamped on the outside. How are "labels" affixed to humans?

Labels affixed to humans are related to the individuals permitted to access to selected pieces of information.

2. Explain the difference in semantics of labels for documents and labels for humans.

Document labels are to differentiate important of the document on the information is contains (for example, for nation secrets allt he way down to common information). And the human labels dictate which personnel is allowed to access which level of information.

3. In the context of computers what do you think are the analogues of documents? Of humans?

The analogues of documents are whatever pieces of information that are stored on the computers database or hard drives. For humans, it is what ever information they possess in their being.

4. Explain why the Principle of Least Privilege makes sense.

For the bare minimum access levle, the Principle of Least Privilege allows the worker to do their assigned job without having too much access to what is not needed to complete the task.

5. For each of the pairs of labels on slide 6, explain why the answers in the third column do or do not make sense.

1. makes sense, the clearance is secret so they are allowed to access almost anything from the sensitvity levels. 2. The clearance is for crypto and nuclear, but only at a secret level, and the sensitivity is at top secret which is not in their access. 3. The

third one can be either or, the clearance level is secret with respect to nuclear, but the sensitivity is unclassified, so in this case the person should be able to access it but the information could be something very sensitive depending on what it is.

Lecture 8:

1. Why do you think we introduced the vocabulary terms: objects, subjects,
actions?
    They help us understand the type of security policy for our construction.
2. Prove that dominates is a partial order (reflexive, transitive, antisymmetric).
    We can see that (L1, S1) dominates (L2, S2) iff L1 >= L2 in the ordering on levels and that S2 is a subset of S1.
3. Show that dominates is not a total order.
    There is a partial order such that security labels A and B such that neither A >= B nor B >= A.
4. What would have to be true for two labels to dominate each other?
    They would have to be of the same level or they are equal to each other.
5. State informally what the the Simple Security property says.
    The subject S with a certain clearance may be granted READ access to object O with classification as long as tthe subject S's clearance levl is greater than the objects O's classification.
6. Explain why it's "only if" and not "if and only if."
    If it is "iff" there can be a contrapositive of the statement but that cannot be true, this statement is only one way so it can only be "only if."

Lecture 9

1. Why isn't Simple Security enough to ensure confidentiality?
    The simple security property isnt enough because it only allows read access but it doesnt correctly define the write access on for exmaple Top Secret documents.
2. Why do we need constraints on write access?
    We need contrains on the write access to disallow unauthorized parties the ability to change or pollute very sensitive information.
3. What is it about computers, as opposed to human beings, that makes that
particularly important?
    Some programs or computers may contain malicious logic such as a trojan horse that causes it to "leak" information without the users knowledge.
4. State informally what the $*$-Property says.
    The $*$ property is a rule for write access. The subject S with a certain level of clerance may be grnated write access to an object O with classification level if the subject's clerance is lower or equal

to the objects Os classification level.
5. What must be true for a subject to have both read and write access to an
object?
The subject must have equal level of clerance for the object O in order to be able to write and read an objects information.
6. How could we deal with the problem that the General (top secret) can’t send
orders to the private (Unclassified)?
We could give the General certain access privileges that are only unique to him since his clearance level is of the highest in the ranks.
7. Isn’t it a problem that a corporal can overwrite the war plan? Suggest how
we might deal with that.
We give certain objects a restriction that they cannot be writen without another party's consent that is of equal of higher clearance compared to the object.

Lecture 10:
1. Evaluate changing a subject’s level (up or down) in light of weak tranquility.
By moving a subjects level up or down should not violate the "spirit" of the security policy. This is a good impelemenation since it does not change the policy but allows fleixbility with the levels of labels.
2. Why not just use strong tranquility all the time?
Because sometimes soubject and objects may increase in rank or importance and that requires a change of label so that the information stays sensitive when it needs to be on a different level.
3. Explain why lowering the level of an object may be dangerous.
By lower an objects level is dangerous because it allows more access to people of lower clearance and in that case the object must be properly reviewed for a demotion to be sure that allowing lower clerance personnel access to it does not put the system in jeopardy.
4. Explain what conditions must hold for a downgrade (lowering object level)
to be secure.
The simple security property, the $*$ property and the traquility property must all hold for the idea of the mutli level security (military security).

Lecture 11:
1. Suppose you wanted to build a (library) system in which all subjects had
read access to all files, but write access to none of them. What levels could
you give to subjects and objects?

Subject would all have a higher level of clerance than the object, but not equal or lesser to prevent any write accesses.

2. Why wouldn't you usually build an access control matrix for a BLP system?

As with any access control policy, you could define an ACM for a large BLP system. However, the amtrix would be huge for most realistic systems.

Lecture 12

1. Suppose you had hierarchical levels L, H with L < H, but only had one category A. Draw the lattice. (Use your keyboard and editor to draw it; it doesn't have to be fancy.)

2. Given any two labels in a BLP system, what is the algorithm for finding their LUB and GLB?

You could the cycles from one point the next point and how many different ways there are of reaching a certain level in the hierarchy.

3. Explain why upward flow in the lattice really is the metapolicy for BLP.

For any BLP system, we only want information to flow upward in the lattice of security levels. Equivalently, information may flow from L1 to L2 only if L2 >= L1. You only want levesl to be able to access their own level and below.

Lecture 13

1. Explain how the BLP rules are supposed to enforce the metapolicy in the example on slide 1.

By allowing only an upward flow, the information flow is permitted from L to H if L ---> H but no vice versa. This captures th metapolicy of this sytem. If it is possible to instantiate this system such that BLP is satisfied, but information flows in violation of the metapolicy, something is wrong.

2. Argue that the READ and WRITE operations given satisfy BLP.

They satisify the BLP because is allows upward flow. READ ensures that the subject level is higher than the object. WRITE ensures that Ls >= Lo to be bale to change the value.

3. Argue that the CREATE and DESTROY operations given satisfy BLP.

They satisify the BLP because it creates an object at the subjects level if there is no object there at all in the system. The destroy works because the subjects level must be equal or lower.

4. What has to be true for the covert channel on slide 5 to work?

In order for them to work, the subjet and object levels must be in agreement for each of the function to be performed to transmit either a 0 or 1.

5. Why is the DESTROY statement there?

The destroy statement is there to ensure that the subject and obejct levels are what they are supposed to be.

6. Are the contents of any files different in the two paths?

No they are not, the path both contain the same contents.

7. Why does SL do the same thing in both cases? Must it?

Yes because it must differentiate between either seeing a value of 0 or 1.

8. Why does SH do different things? Must it?

Yes, if Sl and Sh can corordinate their acitivites, SH can transfer arbitrary amounts of information to SL given enough time.

9. Justify the statement on slide 7 that begins: “If SL ever sees...”

If SL sees something different depending ont he actions of SH you could send the bit of information regardless even if it violates the metapolicy because it is still in agreement with the policy and is still secure. (covert channel)T

Lecture 14

1. Explain why “two human users talking over coffee is not a covert channel.”

Because the flow is between subjects with the system, not two humans.

2. Is the following a covert channel? Why or why not?

Send 0	Send 1
Write (SH, F0, 0)	Write (SH, F0, 1)
Read (SL, F0)	Read (SL, F0)

Yes because the flow of information between Sh and Sl are different.

3. Where does the bit of information transmitted “reside” in Covert Channel #1?

This is called covert storage because SH is recording information within the system state.

4. In Covert Channel #2?

This is a covert timing channel because the information is recorded in the ordering or duration of events on the sytem.

5. In Covert Channel #3?

Process p and q are not allowed to communicate, but they share access to a disk drive. The scanning algorithm services requests in the order of which cylinder is currently closest to the read head.

Process p either access cylinder 140 or 160. Process q requests accesses on cylinders 139 and 161. Thus, q recieves values from 139 and then 161 or from 161 and then 139 depending o p's most recent read.

6. In Covert Channel #4?

An implicit channel is one that uses the control flow of aprogram. The resulting values dpends on another value. There are sophisiticated language based information flow tools that check for these kinds of dependies in programming languages.

7. Why might a termination channel have low bandwidth?

The termination channel only does one thing: destroy, so the bandwidth needed shouldnt be that high. Does not need much bandwidth to see if a computation terminates.

8. What would have to be true to implement a power channel?

The power consumed must be a certain amount that the system can handle.

9. For what sort of devices might power channels arise?

Long distance communications or high powered communications that might use power channels.

Lecture 15

1. Explain why covert channels, while appearing to have such a low bandwidth,
can potentially be very serious threats.

Having low bandwidth means that information transfer rate will be very low this can cause very serious threats because it gives the attack or threat time to infiltrate or do whatever they ar doing on that low bandwidth channel with having a small time contraint. Becuase of such a large time given, you could transfer alot of data still.

2. Why would it be infeasible to eliminate every potential covert channel?

They are pretty much in every system and it is impractical ot remove every single one of them.

3. If detected, how could one respond appropriately to a covert channel?

Close the channel or observe it and try and increase the noise on the channel.

4. Describe a scenario in which a covert storage channel exists.

BY using the internet and visiting different websites, you leave packets there. these packets can be accessed by attackers attempting to steal information.

5. Describe how this covert storage channel can be utilized by the sender and
receiver.

As long as the sender and receiver still have access to the covert storage channel the sender and write and the reciever can do a write/read/destroy. The resulting output will either be a 0 or 1 depending on what the sender sends.

Lecture 16

1. Why wouldn’t the “create” operation have an R in the SRMM for the “file existence” attribute?

the create operation is a modification

2. Why does an R and M in the same row of an SRMM table indicate a potential channel?

if someone can check for the R and M of the SRMM then its a binary flow

3. If an R and M are in the same column of an SRMM table, does this also indicate a potential covert channel? Why or why not?

No because they should never be in the same column.

4. Why would anyone want to go through the trouble to create an SRMM table?

Control the standard information flow, identify convert channels, and deal with covert channels by closing them, restricting them, or monitoring them.