Name: Scott Stephens
EID: STS768
CS Login: scott483
Email: stevo4932@gmail.com

Lecture 1

3. Credit cards are often a source of lax security for me since my card information has been stolen twice in three years.
4. Pretty good chance since it's on and connected to the internet.
5. anti-virus/spyware and firewall. Also check cookies and saved passwords.
6. Yes for the most part but there only needs to be one flaw.
7. I do think it's slighly overstated but I also see how it's possible for someone to access the lauch codes for example.
8. To secure yoursel ad information from malicous attacks that can damage your info, hardware, credability and others connected to you.

Lecture 2
1. May be time consuming to get right especially when management wanted it out yesterday. May also affect performance and ease of use.
2. There is not really a systematic way to enumerate the “bad things” since they are not always easily known or the same across systems.
3. Defenders must securing there system from attackers. They must find all vulnerablities so that they may not be exploited. Attackers on the other hand are looking for vulnerablies in a system to potenitally exploit it and tamper with information.
4. To ensure one hundred percent security I do agree with morris and chang but I would say there are very effecive deinses. There will always be the possiblity of unforsean flaws no matter how well tested and searched over a program may be. Could be anything from internet hackers to mistakes in your own code causeing unwanted events.
5. It's similar to the classic liberty vs security debate. In order to gain more of one you must give up more of the other. In order to gain more security you must lose some of the freedom. Unclassified subjects can no longer access top secrete data. The key is to find the optimal amount of each.

Lecture 3
1. risk – possibility that a particular threat will adversely impact an info sstem by exploiting a particular vulnerabiltiy.
2. Software security is about managing risk since every piece of software lives on computers which always care risk. That risk must be managed to find a balance between security and risk.
3. I accept the risk of flying, avoid the risk of germs associated with the 5 second rule, and transfer the risk of high medical bills by purchasing medical insurance.
4. loss expectancy is essentially expected value. The problem with expected value is it does not tell the full story of how much can actually be lost. People looking for security are usually risk adverse meaning that this potential loss is more important to them then the average cost.
5. Technical, economic, and psychological factors are all relevant to rational risk assessment.

Lecture 4
1. Slide two describes the general major areas of a policy such as integrety and confidentiality. Slide three on the other hand is about the mechanisims that are used to support those areas of security.
2. Since I use my computer often for work and school avalibility is often most important. I must meet

deadlines for my professors and boss and can't do that if my data is not accessable when I need them.
3. Grouping and categrizing data means sorting the data into boxes based on security levels.
4. Authorizations may change if someone gets fired or promoted for example.
5. Part of security is knowing that your information will be there when you need it. In order for this to happen you must have a reliable system that is rarely down. If your system is unreliable people may not trust you to host there data as they may not be able to access when needed.
6. Online shopping seems to be an area where authentication and non repudiation would be important for both customers and sellers.

Lecture 5

1. To provide celular comunication from sender to the intended recipient whenever needed free from easvesdroping.
    1. To be able to provide requested information when needed to the appropriate individuals and the ability for certain individuals to modify or create necessary documents.
2. Metapolicy is a high level overview of the security goals that is often to general to act upon. Policy lays out the specific mechanisms for enforcing the metapolicy..
3. students and professors may not directly change grades.
    - Grades are to be sent for publishing to the registars
    - All grade inquires and issues are to be helded through the registars office.
4. Yes there may be conflicts in a policy from stakeholders' interests. A student may wish to change his or her grade directly (say from a B to an A) but a university would be opposed due to reputation, integrety, ect.
5. Protect students' SSN from unwanted eyes while still being avalible when absolutly nessasary.
6. Since the metapolicy is the general goal, the specific methods to complete that goal may not make since on their own. If someone does not know that they must disinfect the lab equipment to rid it of contaminates they may think that the activity is useless.

Lecture 6

1. The Military is in charge of lots of top secreate data that concerns the welbeing of the nation . We do not want our enemy's eyes on our top secrete war plans for example. This makes confidentiality extreamly inportant. We are also concerned with integrety as we want those plans to remain uncorupted by our enemies who may try to confuse us or set a trap by changing the plans. We also want to be able to access the plans when needed say for instructions or clarification.
2. Unauthored veiwing of information is the major threat in our MLS thought experiment.
3. The proviso is ther to isolate and properly establish confidentialies' mechanisms without having to worry about other security issues.
4. The labels we use have two parts. A linearly ordered set (top secrete down to unclassified) and a need-to-know unordered set of members that something can belong to.
5. We are not concerned with how the lables get there because we are only worried about enforcing the lables.
6. Facts ordering: 2,6,4,5,3,1
7. 2) top secreat, {invation} 6) top secreat{crypto} 4&5) confidential{payroll} 3&4)unclassified.
8. Suppose a mixed document mostly consists of secreat info but one line is top secreat info. If you mark it secreat then that level can now access top secreat information. That is wrong.

Lecture 7

1. labels are affixed to humans with clearnces and authentication levels with the same form as document lables.
2. Document lables indicate senstivity of information. Human lables indicate classes fo information authorized to access.
3. Documents are similar to directories or files in computer systems. Humans could be processes in computer terms.
4. The principle of least privilege makes sense since there is no need for nuclear people to see crypto information if they don't need it to complete their tasks. It's just extra information that is not really useful to their work so it's best to avoid the potential security risk.
5. secret is higher than confidential so yes they should be able to access the lower level. However the second subject is only secreate while the object is top secreate meaning the human would be reading. That's no good. The last one is obvious since any level may view an unclassified document.

Lecture 8

1. The terms are more general than the previous terms. The previous use of humans was two specific since we could also be talking about processes from other programs. So subject was a better fit. Same idea with folders. They could be directories or entire databases in the compute world.
2 &3. (top secreat, {crypto}) and (top Secreat, {Nuclear}) are neither greater than, less than or equal to each other. Therefor they are parial orders and not total.
4. (L1, S1) & (L2, S2), L1>=L2 & S2 must be in superset S1.
5. Simple security property says one may read objects at or below their level.
6. if and only if means that the condition is both necessary and sufficient but there may actually be other constraints that would prevent it from being sufficient. It therefore makes more since to say only if which implies that necessity but not always sufficiency.

Lecture 9

1. Simple security does not take into acount risk from writing down.
2. So that a higher level subject can't write top level data into lower level objects.
3. With computes we are now worried about the other programs that may use your clearence level to access higher level data then they should.
4. *-property says we can write at or above our level but not below.
5. Must essentially be equal meaning same ordered list level and at least a subset of the need-to-know catagories.
6. We could solve the general write down issue by having him long out of top secreate and into unclassified in order to send orders. This however leads us to worry about programs bring top level data down with them.
7. It is an issue that a corporal can overwrite a war plan but that is an integrity issue. Could be fixed wit restrictions on writing up.

Lecture 10

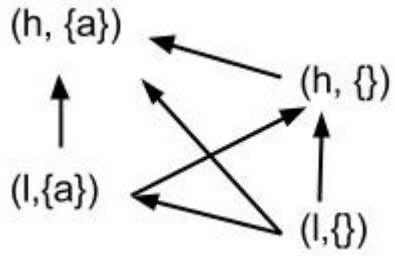
1. changing a subjects level down would lead to the possibility that they have residual high level information. Changing a subject upward may be ok since it would not necessarily affect the * or simple security properties.
2. Sometimes we may need to change levels daily like the general needing to send messages to his troops. Strong tranquility does not allow this,
3. Lower the level of an object is dangerous since subjects who should not be able to view the object

ccan now. It's similar to writing down which is not allowed.
4. Must be a stateless proram tha tdoes not retain highlevel information.

Lecture 11

1. Since we can read down and write up we would need subjects to be high and objects to be low.
2. Access control matrix for BLP systems can become huge. With thousands of objects and subjects it is often easier to calculate it without forming the matrix.

Lecture 12



Lecture 13

1. The BLP rules enforce the metapolicy by preventing information flow from high to low. The * property and simple security property of BLP insure that there is only read down and write up which enforces the metapolicy.
2.They both meet 8 and simple security properties of BLP
3. The create makes a new object at the same level as the create which means there is no information leak or different privileges from it's creater. The destroy command works like a write. Since it's perfectly acceptable to overwrite a higher level object it also offers no issues to destroy the object completely since no information is passed down to a lower level.
4. High must be able to transmit info down to lower for the covert channel on side 5 to work.
5.
6. The contents of the two paths are not different since they can both write but only the second can actually read the new information so that's why the transmitions are different.
7. SL is used as a kind of control but it does not have to do the same thing. It could vary the commands and only those that met the rules will execute as normal.
8. SH varies to show what happens when a high and low object interact and when they don't. Sh does not have to varie it could create an object everytime if necessary.
9. By SH sending information to SL it is breaking the simple security properties of BLP by allowing lower levels to view higher level data which violates the metapolicy.

Lecture 14

1. Two humans talking is not part of the system.
2. It is not a covert channel since they will both return 0 and no information is passed down.

3. The high level object stores the info in the state of the system.
4. For covert Channel #2 it stores the info in the ordering and duration of events on the system.
5.Channel #3 has aspects of both storage and timing since the last read is stored on the system while the order of the next read is based on the last storage.
6. Channel #4 is based on the control flow through the program which can give away information.
7. Termination Channel may have low bandwidth since it can only tell you wheather it terminated or not. Only two options.
8. To implement a power channel the low level would have to be able to since it while the high would have to modulate that power channel.