Neil Jones
nj2977

Week 1 Questions

Lecture 1

1. The term “Security” is relevant to almost every aspect of my daily existence. It covers my electronic activities (banking, shopping, etc.) as well as physical activities (keeping the door locked, not leaving any of my possessions unattended, etc.).

2. They all have to do with the protection of assets (identity, money, possessions, well being).

3. Yes, I have had to rid my computer of many malicious programs over the years.

4. It is probably very likely. There are many malicious programs which cannot yet be detected by anti-virus programs.

5. I use an anti-virus program as a last resort. Mostly I rely on common sense to keep the most harmful infections off of my computer.

6. They may be. If my computer is infected, the malicious programs on it don't seem to be targeted at anything I “own.” They may collect data or they may be using my computer as a vector to reach their intended targets.

7. It probably isn't overstating the case anymore. Every aspect of modern life is controlled by computer systems. Many of these systems are vital to the health and safety of the populace (food supply shipping routes, financial exchanges, etc.). If these systems were to fail irreparably, the amount of time it would take to restore them could completely transform how people live.

8. Computer security is important to learn about because every aspect of our lives depends on computer systems that function as intended. It is in the best interest of everybody for these systems to be secure. Beyond that, it is important for users to know best practice when dealing with these systems.

Lecture 2

1. We have to decide which threats have more weight than others. We have to balance security against functionality.

2. No, There is no way to ensure that any given security mechanism will completely protect a system from attack. We can use a list of common vulnerabilities or think of possible vulnerabilities but it isn't very likely that all of the possible weak points will be covered.

3. A defender can only prevent attacks that they can think of and respond to attacks in progress. An attacker has the advantage of coming up with new methods of attack and they

don't have as much to lose if they fail.

4. Yes, it seems impossible to completely protect a system from being successfully attacked because there are so many methods of attack. It would be an act in futility to attempt to protect against everything and doing so may compromise the usability or functionality of the system. We have to accept some level of risk.

5. When building security measures for a given system, there is only so much we can add without compromising its usability or functionality. There has to be a balance between the two. If a system becomes too difficult to use, nobody will use it.

Lecture 3

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

2. I think that the application of software security is about managing risk. Resources are limited so we need to allocate them as effectively as possible.

3. Accept: Loss of data through physical theft.
   Avoid: Password theft through social means.
   Mitigate: Virus infection.
   Transfer: Account theft. I leave the security to the managing entity.

4. ALE could be a useful tool for portioning out resources. However, some risks, while having a low probability of occurrence, could be catastrophic for the system if they do occur. So while ALE is a useful tool, it isn't the only thing that should be considered when portioning out resources.

5. How much will you lose if a security measure fails? How likely is a particular occurrence of a security breach? Can the system afford to pay the cost of a breach?

Lecture 4

1. The list on slide 2 describes the aspects of meta-policies in security while the list on slide 3 describes specific means for implementing these meta-policies.

2. Availability closely followed by confidentiality and integrity. I want my personal computing devices to be easy to use and available to use because I use them often. At the same time, I want my data to be mine alone and I want that data to change only at my command.

3. Grouping and categorizing data is the act of separating data into equivalence classes based on their security level.

4. It is possible for users to be recategorized. For instance, if a person gets a promotion then their access to company secrets may be elevated. Data can also be recategorized if it is no longer considered sensitive.

5. If a system isn't reliable, it may become difficult to ensure its security due to the fact that we can't check for coherency if the system is unavailable.

6. Authentication is important for online banking systems. Are you who you say you are? Non-repudiation is important for online sales. Did a particular transaction take place for a specific amouunt of money?

Lecture 5

1. The data transferring between users should be protected from outside access. Confidential information should not be viewable by unauthorized users.

2. A policy describes a specific implementation in order to realize a metapolicy.

3. Student records should only be viewable by authorized personnel. Student records should be protected from unauthorized amendments. Student records must only be available to the students which they respectively concern by request.

4. Yes, free access to a category of data may be advantageous for one class of users but not another.

5. Student SSN's must be protected from being viewed by unauthorized personnel.

6. If you don't understand the overall goal of the security system then you can't tell if it is operating as intended.

Lecture 6

1. Military documents could contain highly secret information such as war plans which should never fall into the hands of the enemy. Integrity is important because sensitive information ought to be reliable. Availability is important because secret information may be needed at any moment and it ought to be available.

2. Secret information falling into the hands of the enemy.

3. Integrity may not be important because lower level personnel may need to use blind writes to communicate with higher level officials. Availability may not be important because it could possibly used as a covert channel of communication.

4. The labels each represent a level in our security hierarchy. We also have sub-components which can be used to compartmentalize within our primary security levels.

5. We are only concerned with confidentiality.

6/7. The cafeteria is serving chopped beef on toast today. Unclassified
The base softball team has a game tomorrow at 3pm. Unclassified

Col. Smith didn't get a raise. Confidential | Personnel
Col. Jones just got a raise. Confidential | Personnel
The British have broken the German Enigma codes. Top Secret | Crypto
The Normandy invasion is scheduled for June 6. Top Secret | Executive

8. The least secure document must inherit the security level of the most secure document so that the most secure document does not fall into unauthorized hands.

Lecture 7

1. Labels are affixed to humans through various methods of authentication: cryptography, photo ID's, finger prints, etc.

2. Labels on documents explain the level of sensitivity of the contained documents. Labels on human beings explain the highest level of information that they are allowed to view.

3. Files, network ports, maybe particular areas in memory. User privilege level: user, group etc.

4. If they don't need access to information then they have no need to ever access it. Letting an individual who doesn't need to view information have access to that information opens the system up to a possible breach.

5. 1) true, the individual has clearance to view secret (> confidential) and they have clearance to view crypto related info.
2) true, the individual only has clearance to view secret (< top secret).
3) true, the document is unclassified so it may be viewed by anybody.

Lecture 8

1. They are more abstract terms which is important because each could represent different entities depending on the system being secured.

2. Reflexive:
(L1, S1) dominates itself. L1 = L1, S1 = S1
Transitive:
(L1, S1) dominates (L2, S2)
(L2, S2) dominates (L3, S3)
L1 >= L2 >= L3, so L1 >= L3
S3 ⊆ S2 ⊆ S1, so S3 ⊆ S1
Antisymmetric:
(L1, S1) dominates (L2, S2)
(L2, S2) dominates (L1, S1)
L1 >= L2, L2 >= L1, so L1 = L2
S2 ⊆ S1, S1 ⊆ S2, so S1 = S2

3. (L1, S1) not dominate (L2, S2)

(L2, S2) not dominate (L1, S1)
L1 >= L2, but S1 ⊆ S2

4. The level would have to be the same and the set of conditional labels would have to be the same.

5. A subject may access an object only if their label has a higher level than the document's and the set of the user's conditional labels contain all of the conditional labels of the document.

6. “if and only if” means that access implies dominance and dominance implies access.
“only if” means that access implies dominance but not necessarily the other way around.

Lecture 9

1. It doesn't govern write access.

2. If we don't place constraints on writing, covert communication channels may be used or high ranking subjects may be able to write down and pass information to unqualified subjects.

3. The activity of people is easily monitored. This isn't so easy for computers.

4. Write access to an object may only be granted to a subject if the object dominates the subject.

5. The subject and object must dominate each other.

6. The general could log in as an unclassified user so that any secret info from his classified account will not be transferred.

7. We could allow confidential subjects to place write locks on selected files.

Lecture 10

1. Moving a subject down will pose no threat because they will not have access to anything that they didn't before. Moving them up may pose a problem because they will be able to access information that was previously restricted, thereby violating weak tranquility.

2. It may be necessary to upgrade or downgrade subjects or objects.

3. It may make sensitive information available to the wrong subjects.

4. Information that is sensitive must not be lowered to a level where unauthorized subjects may freely view it. This requires an examination of the information in the object.

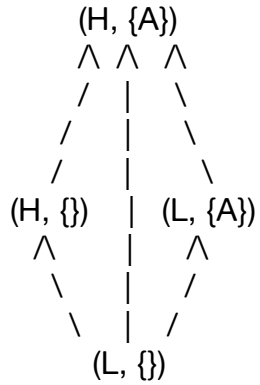
Lecture 11

1. Subjects would be labeled as “Subject” and objects would be labeled as “Object.” Subjects would only be able to read objects.

2. It can be easily computed on the fly. BLP systems can have thousands of subjects and objects so the resulting matrix would be huge and sparse.

Lecture 12

1.



2. The node with no incoming edges is the GLB and the node with no outgoing edges is the LUB.

3. BLP preserves confidentiality of information. In order to achieve this information may only flow from low to high (governed by the dominates relation). This flow is completely mapped by the directed edges of the lattice.

Lecture 13

1. BLP governs the flow of information by means of the dominates relation. This can be guaranteed by blind writing.

2. Read is only used by higher level subjects so information only moves up from lower levels. Write is blind so information cannot flow down.

3. Create guarantees existence without passing information back. Destroy guarantees destruction (with write access) without passing anything back. So information is not transferred by these operations.

4. Read must return a value based on existence.

5. Destroy guarantees that the slate is wiped clean before each exchange.

6. No, the contents are always the same, it is the level of existence that changes.

7. SL is checking for access each time. It is receiving information.

8. SH is the one sending information so it must take different actions depending on what it

wants to send.

9. This covert channel allows information to pass from a higher level to a lower one. This violates the metapolicy.

Lecture 14

1. People are explicitly exchanging information which violates the metapolicy.

2. No, this is explicitly exchanging information through an object.

3. The information transferred exists in the existence of either 0bit or 1bit.

4. The amount of time elapsed.

5. The order of cylinder access.

6. The value of the low order variable l which depends on the value of h.

7. It takes a long time to transfer each bit because process termination takes a lot of time.

8. Smartcards, external devices which receive power from the host computer.

Lecture 15

1. A lot of the time even a small amount of information can be dangerous. Even though they are slow relative to normal computer operations, they are still very fast.

2. It isn't possible to systematically enumerate resource access because what constitutes useful interaction between levels may not be rigidly defined. Systems are extremely complex, so it would take a lot of time.

3. Modify the system implementation, introduce noise, or monitor it.

4. One process could create a particular file to initiate an exchange. This process could then create different files for either 1 or 0. The receiving process then checks for the existence of these files at a predetermined interval.

5. The sending process sends a 0 or 1 through file existence and the receiving process receives the values through existence checks.

Lecture 16

1. Create guarantees existence without returning any values to the creator.

2. If a subject has the power to read then it is higher level so it shouldn't be able to modify. This is how information is passed down.

3. No, because this doesn't imply that a subject can send information through a single object.

4. It could be important if the information in the system is particularly sensitive. Detecting covert channels is difficult, so any method we can use to weed them out is useful.