Name: Yun Wen Chen
EID: dc27863
CS Login: dchen
Email: dianachen@utexas.edu

Lecture 17

1. If a computer system complies with the BLP model, does it necessarily comply with non-interference? Why or why not?

No. The BLP model is liable to leave a number of covert channels. These covert channels allow a low-level subject to see varying results depending on varying actions by a high-level subject, thus allowing a high-level subject to be able to indirectly communicate with a low-level subject. If the actions of a high-level subject is visible to a low-level subject, then the high-level subject interferes with the low-level subject. This means that the BLP model doesn't always comply with non-interference.

2. What would the NI policy be for a BLP system with subjects: A at (Secret: Crypto), B at (Secret: Nuclear)?

A and B should not be able to communicate with each other because neither dominates the other. (More specifically, neither need-to-know groups dominate the other.

3. Can covert channels exist in an NI policy? Why or why not?

In a absolutely perfect covert channel, no. H should not be able to do anything that affects L's view of the system. If you put all the attributes that L could possibly see into the system, then there would be no covert channels as H wouldn't be able to "signal" anything. However, if you miss subtleties like flags, clocks, etc., then H could utilize these attributes to create a covert channel.

4. If the NI policy A —> B, in a BLP system what combination of the levels "high" and "low" could A and B have?

A —> B if the level if B dominates A.

A= high, B = high
A = low, B = high
A = low, B = low

*This is assuming that the need-to-know groups of B is a superset of the need-to-know groups of A.

Lecture 18

1. Why do NI policies better resemble metapolicies than policies?

NI policies resemble metapolicies because they too are very abstract. In the BLP, the metapolicy states that information may flow from low to high, but not vice versa. This metapolicy does not state the rules or mechanisms that will uphold this goal. The NI policies, which state the direction communications may go between elements of a system, does not contain rules or mechanisms that will uphold these flows.

2. hat would be L's view of the following actions: h1, l1, h2, h3, … hj, l2, l3, …, lk?

l1, l2, l3, …, lk

3. What is difficult about proving NI for realistic systems?

In realistic systems, there are many interferences such that even if you did include everything regarding L's view, you wouldn't be able to prove that your system is non-interfering.

There are many low-level attributes in a system, and to be able to include them all, you would need an extensive model of these attributes and how they tie in with the rest of the system.

There are many benign interferences such that though parts of a system are interfering, the information they could possibly retrieve has no meaning.

Lecture 19

1. Explain the importance of integrity in various contexts.

Integrity is important when it comes to contexts involving the trustworthiness of information and the confidence in the ability of an entity to produce and handle information. We don't place high confidence in entities such as gossip and blogs to produce and handle trustworthy information. In return, we can't place high trustworthiness in the information that is produced and handled from these entities.

2. Why would a company or individual opt to purchase commercial software rather than download a similar, freely available version?

The company or individual would have higher confidence in a company that wrote the commercial software than in the individual or group who wrote the free version. While there are many intelligent people writing great free software, there are also people who write bad software or even malicious software. Even if the free software worked as intended, the commercial software (generating revenue) would have better outlets for support in case things go wrong, such as QA, better managed logs, company guarantees, legal guidance. As a result, the trustworthiness of the commercial software is placed higher than that of the freely available software, as chances are that it is produced by a legitimate company with trained professionals.

3. Explain the difference between separation of duty and separation of function.

Separation of duty states that several subjects must be involved to complete a critical function. Separation of function states that on subject can't perform two critical functions. Consider the example in the lecture. It takes two bank officers to validate a cashiers check. If it only took one, a corrupted bank officer would dispense money freely. Second, a person can't be a teller and an auditor, as they could steal money as a teller and destroy the evidence of the stolen transaction as an auditor.

4. What is the importance of auditing in integrity contexts?

Auditing is important such that a system should be able to assign responsibility to a subject if something goes wrong and be able to roll back the bad changes based on its records. In other words, a system should be able to pinpoint the entities or actions responsible for a fault, and be able to revert back to the "correct" state.

5. What are the underlying ideas that raise the integrity concerns of Lipner?

The integrity concerns of Lipner include the violation of separation of duty, separation of function, and auditing. Making sure that the people developing the software and the people using the software ensures separation of function. Having a special, controlled process of moving applications from development to production ensures separation of duty such that it probably takes more than one entity to approve a application for production. Having a log of this controlled process ensures auditing.

7. Name a common scenario where integrity would be more important than confidentiality.

Github is an example where integrity would be more important than confidentiality. Professor Downing has a public repository containing class examples, quiz solutions, and skeleton code for programming assignments that his students can clone into their own private repository. However, students can't push their version of the programming assignment to Professor Downing's repository. This is because Professor Downing's skeleton code to the programming assignment, though incomplete, is more trustworthy than a students version of the assignment. In turn, Professor Downing is the only one that can update the skeleton code for the programming assignments, as we have high enough confidence that he would produce a trustworthy skeleton code. If a student did push his assignment to Downing's repo, then that version of the programming assignment is not trustworthy.

Lecture 20

1. Give examples of information that is highly reliable with little sensitivity and information that is not so highly reliable but with greater sensitivity.

Ingredients found on food labels are not very sensitive, but are highly reliable for people who have food allergies.

The whereabouts of Kanye and Kim's honeymoon location are relatively more sensitive, but are not so reliable, as anyone who has an idea can divulge that information.

2. Explain the dominates relationships for each row in the table on slide 4.

(Expert: {Physics}) , (Student: {Physics}) — An expert in the field of physics dominates a mere student of physics.

(Novice: {Physics, Art}) , (Expert: {Physics}) — A novice of Physics does not dominate an expert at physics.

(Student: {Art}) , (Novice: {}) — A student in art dominates a novice (in life).

3. Construct the NI policy for the integrity metapolicy.

Low-integrity subjects should not be able to write bad, low-integrity information into a high integrity-object.

High-integrity object should not be able to read information for a low-integrity object.

This is to prevent information from flowing up in integrity.

4. What does it mean that confidentiality and integrity are "orthogonal issues?"

Integrity and confidentiality are not so much related to each other as you can have high integrity subjects with low confidentiality and vice versa.

Lecture 21

1. Why is Biba Integrity called the "dual" of the BLP model?

The Biba Integrity is called the "dual" of the BLP model because a subject can only read at its own integrity and above and write at its own integrity or below to stop the flow of information from low

integrity to high integrity. In the BLP model, a subject can only read at its own clearance or below and write at its own clearance or above to stop the flow of information from moving from high sensitivity to low sensitivity.

2. Why in the ACM on slide 5 is the entry for Subj3 - Obj3 empty?
Subj3 cannot read Obj3 because Obj3 does not dominate Subj3. Subj3 cannot write to Obj3 because Subj3 does not dominate Obj3.

3. If a subject satisfies confidentiality requirements but fails integrity requirements of an object, can the subject access the object?

No. If confidentiality and integrity are required, then a subject needs to fulfill both of these requirements with two sets of labels, one for confidentiality and one for integrity.

Lecture 22

1. What is the assumption about subjects in Biba's low water mark policy?

Biba's low water mark policy assumes that if you read an object with lower integrity, you become compromised as well.

2. Are the subjects considered trustworthy?

No

3. Does the Ring policy make some assumption about the subject that the LWM policy does not?

The Ring policy assumes that the subject has the common sense to filter out bad information.

4. Are the subjects considered trustworthy?

Yes

Lecture 23

1. Are the SD and ID categories in Lipner's model related to each other?

Yes. The SD is the label for the confidentiality aspect of programs under development whereas the ID is the label for the integrity aspect of programs under development.

2. Why is it necessary for system controllers to have the ability to downgrade?

Downgrade allows system controllers to move software/objects from development to production.

3. Can system controllers modify development code/test data?

Yes, because system controllers are allowed to downgrade. However, this cannot be done with the BLP and Biba model alone.

4. What form of tranquility underlies the downgrade ability?

Weak tranquility property.

Lecture 24

1. What is the purpose of the four fundamental concerns of Clark and Wilson?

The purpose of the four fundamental concerns of Clark and Wilson are aimed at consistency. Authentication allows the identity of all users to be verified somehow. Auditing allows for a log that keeps track of user actions in order to figure out what went wrong if something does goes wrong. Well-formed transactions only allow the manipulation of data in constrained ways to enforce legitimate accesses. Separation of duty keeps users from making unauthorized modifications on their own. Together, these concerns keep maintain a consistent system.

2. What are some possible examples of CDIs in a commercial setting?

Bank balances, checks.

3. What are some possible examples of UDIs in a commercial setting?

Food samples, empty forms.

4. What is the difference between certification and enforcement rules?

Certification rules pertain to keeping a consistent state, whether by monitoring TPs or checking CDIs. Enforcement rules determine which transactions can modify which CDIs, in which to preserve a consistent state.

5. Give an example of a permission in a commercial setting.

Consider an animal hospital:
{Veterinary technician, dispense, {heartworm medication})
{Veterinarian, dispense, {All pet medication})

A veterinary technician can dispense Heartworm Medication because most pet-owners use it every month. However, they cannot dispense any other pet medication.

A veterinarian can dispense all pet medication, even heartworm medication, because they have received the proper training to prescribe the appropriate medicine.

Lecture 25

1. Why would a consultant hired by American Airlines potentially have a breach of confidentiality if also hired by United Airlines?

Because American Airlines and United Airlines are in the same conflict class. In other words, a consultant may inadvertently pass information from American Airlines to United Airlines and vice versa.

2. In the example conflict classes, if you accessed a file from GM, then subsequently accessed a file from Microsoft, will you then be able to access another file from GM?

Yes because GM and Microsoft are in different conflict classes.

3. Following the previous question, what companies' files are available for access according to the simple security rule?

GM, Microsoft

Bank of America, Wells Fargo, Citicorp

4. What difference separate the Chinese Wall policy from the BLP model?

In the BLP model, subjects can access objects (given the correct clearance of the object and itself) in all its need-to-know groups. In the Chinese Wall policy, if any of these need-to-know groups have a conflict relation, then accessing one of these groups will cause the loss of access to the other group in its conflict class. In other words, a subject may have many need-to-know groups, but his maximum number of group access would be equal to the number of conflict classes that can arise from these groups.

Lecture 26

1. What benefits are there in associating permissions with roles, rather than subjects?

You don't need to associate permissions by examining every single subject. Rather, you can associate permissions by the roles that the subject will fulfilling. This makes assigning permissions easier and simpler to analyze and implement.

2. What is the difference between authorized roles and active roles?

Authorized roles are all the potential roles that a subject can take on. Active roles are the roles that they have right now.

3. What is the difference between role authorization and transaction authorization?

In role authorization, the subject's active roles must belong in the set of all its authorized roles. In transaction authorization, a subject can only execute transactions that belong to its active roles.

4. What disadvantages do standard access control policies have when compared to RBAC?

With standard access control, the system has to analyze every person in order to assign permissions whereas in RBAC, the system only has to assign permissions to a role, and every person with that role has those permissions. RBAC allows a subject to transition between roles without having to set up a new identity. In the standard access control, you typically don't want to transition between clearances. In summary, RBAC is more flexible, which is advantageous to a dynamic commercial setting.

Lecture 27

1. Why would one not want to build an explicit ACM for an access control system?

Because in realistic systems, most subjects do not have any access to other objects.

2. Name, in order, the ACM alternatives for storing permissions with objects, storing permissions with subjects and computing permissions on the fly.

Access control lists (i.e. inode), capabilities (sets), maintain a set of rules to compute access permissions "on the fly" based on attributes of subjects and objects.

Lecture 28

1. What must be true for the receiver to interpret the answer to a "yes" or "no" question?

The receiver must have a mechanism that maps the signal from the sender to a yes or no. In other words, if 1 means yes and 0 means no to the sender, then the receiver needs to have a way to tell that when it receives a 1, it means yes and when it receives a 0 it means no.

2. Why would one want to quantify the information content of a message?

Because information content may come in different sizes. In other words, someone receiving the information should know what the answer should "look" like. If you are expecting a information with a size 5 and you get one with size 6 or 4, then the information you got is nonsense.

3. Why must the sender and receiver have some shared knowledge and an agreed encoding scheme?

This allows the receiver and sender to communicate with each other. An agreed coding scheme is like two people being able to understand the same language.

4. Why wouldn't the sender want to transmit more data than the receiver needs to resolve uncertainty?

Because sending more data would cause the receiver to interpret the value incorrectly. If a "yes" in bits means 1 to both the sender and the receiver, sending 1 to the receiver would mean sending a yes. If instead, the sender sends a 10 (decimal 2) the receiver does not know what 2 means, as there is no mapping of 2 to the agreed encoding scheme between the sender and receiver.

5. If the receiver knows the answer to a question will be "yes," how many bits of data quantify the information content? Explain.

In the example, the agreed encoding scheme between the receiver and sender include a bit value of 1 for "yes" and a bit value of "0" for no. It only takes 1 bit of data to quantify "yes".

Lecture 29

1. How much information is contained in each of the first three messages from slide 2?

n-bit binary number: n bits
a single decimal digit: 4 bits
a two digit decimal number: 7 bits

2. Why does the amount of information contained in "The attack is at dawn" depend on the receiver's level of uncertainty?

It depends on how much information the receiver needs to resolve its level of uncertainty. For instance, if I were the general of an army awaiting an attack time, I don't need "The attack is at dawn", I only need "dawn". If I were the enemy of the attacking army, I would want "attack is at dawn" to know when to expect my invaders.

3. How many bits of information must be transmitted for a sender to send one of exactly 16 messages? Why?

4. The log base 2 of 16 is 4. In other words, if there are 16 difference messages, it takes 4 bits to represent the whole range of possible messages.

4. How much information content is contained in a message from a space of 256 messages?

8. The log base 2 of 256 is 8.

5. Explain why very few circumstances are ideal, in terms of sending information content.

In an ideal circumstance, you know the number of possible messages that could be send. As a result, every additional bit you receive cuts the number of possible messages by half, eventually reducing it to the actual message. However, few circumstances are ideal because you, the receiver, typically don't know how many possible messages there are to begin with, such as "The attack is at dawn" example. As a result, receiving a bit of information does reduce the number of possible messages that it could be, but you don't know by how much.

Lecture 30

1. Explain the difference between the connotations of the term "bit."

The first connotation of bit is the binary digit, with only discrete values 0 or 1.

The second connotation of the bit is a quantity of information, which is continuous value.

2. Construct the naive encoding for 8 possible messages.

Msg	code
M0	000
M1	001
M2	010
M3	011
M4	100
M5	101
M6	110
M7	111

3. Explain why the encoding on slide 5 takes 995 + (5 * 5) bits.

Given 1000 messages, 99.5% of the messages will be message 10. That means, 995/1000 messages will return only 1 bit of binary value 0. This results in 995 bits.

5/1000 times the message will be between M0 and M15 excluding M10. This means that 5 out of 100 messages will receive 5 bits. 5 * 5 = 25.

Thus, the encoding on takes 995 + (5 * 5) = 1020 bits, or 1.02 bits per message.

4. How can knowing the prior probabilities of messages lead to a more efficient encoding?

Knowing prior probabilities of messages can lead to more efficient encoding because it could reduce the number of bits needed to send a high-probability message. If a certain message has higher probabilities than other messages, then we can designate a low bit encoding to that message. This means that whenever this high-probability message is sent, it needs to transmit fewer number of bits, therefore increasing the bandwidth of the communication system.

5. Construct an encoding for 4 possible messages that is worse than the naive encoding.

4 messages, Message

Msg	code
M0	100
M1	0
M2	110
M3	111

Assume M1 has a 30% chance (higher than 25% even distribution).
Then the encoding becomes 300 + (700 * 3) = 2100

6. What are some implications if it is possible to find an optimal encoding?

Calculating the prior probabilities, determining how the prior probabilities should be handled in terms of bits.

Lecture 31

1. Name a string in the language consisting of positive, even numbers.

"2486222446826"

2. Construct a non-prefix-free encoding for the possible rolls of a 6-sided die.

1	11
2	1100
3	11001
4	110010
5	1100101
6	11001011

3. What is it necessary for an encoding to be uniquely decodable?

Because if a symbol's code is the union of two other symbols in the encoding, the receiver may interpret it as the two other symbols instead of the one symbol.

4. Why is a lossless encoding scheme desirable?

You want to be able to reproduce the original sequence in order because order of messages matters. If you send the word "hello" as "elolh" and the receiver is unable to recover the original sequence of the letters, then you have nonsense.

5. Why doesn't Morse code satisfy our criteria for encodings?

Morse code is not streaming (breaks in the transmission), allowing letters like S to be interpreted as EEEE (four E's).

Lecture 32

1. Calculate the entropy of an 8-sided fair die(all outcomes are equally likely).

h = - 8 * (1/8 * log(1/8)) = - 8 * (1/8 * -3) = 3
h = 3

2. If an unbalanced coin is 4 times more likely to yield a tail than a head, what is the entropy of the language?

h = - (4/5 * log(4/5) + 1/5 * log(1/5)) = .721

3. Why is knowing the entropy of a language important?

It is important to find an encoding that uses less than one bit per symbol, on average, as it is typically the optimal. However, knowing the entropy of a language is important because it is an ideal goal for when you try to set up an encoding.

Lecture 33

1. Explain the reasoning behind the expectations presented in slide 3.

The new probability of the results in slide 3 can be obtained by the probabilities of slide 2.
If the probability of heads is 3/4 and the probability of tails is 1/4. Then the probability of HH is 3/4 * 3/4 = 9/16. As a result, in 16 2-flips, we can expect 16 * 9/16 = 9 HH results. It is just a recalculation of the expected value, with updated probabilities for 2-flip.

2. What is the naive encoding for the language in slide 5?

Die	Code
1	000
2	001
3	010
4	011
5	100
6	101

3. What is the entropy of this language?

2.4

4. Find an encoding more efficient than the naive encoding for this language.

5. What is your encoding more efficient than the naive encoding.