Name: michael truong
EID: mkt532
CS Login: mtruong
Email: mtruong92@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; a computer system that complies with the blp model might have covert channels

2. What would the NI policy be for a BLP system with subjects: A at (Secret: Crypto), B at (Secret: Nuclear)?
there would be no ni policy; neither a nor b dominates or is equal to the other

3. Can covert channels exist in an NI policy? Why or why not?
no, there shouldn't be anything that sh can do that has effects visible to sl

4. If the NI policy is A− > B, in a BLP system what combinations of the levels “high”

and “low” could A and B have?
a: low; b: high

Lecture 18

1. Why do NI policies better resemble metapolicies than policies?
there're no rules about which subjects can read/write which objects. in fact, nothing about objects or actions at all

2. What 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?
it requires identifying within the view function all potential channels of information.
realistic systems have many such channels.
modeling must be at very low level to capture many such channels.
dealing with timing channels is possible, but difficult.
very few systems are completely deterministic.
some "interferences" are benign. e.g., encrypted files.

Lecture 19

1. Explain the importance of integrity in various contexts.
to protect data

2. Why would a company or individual opt to purchase commercial software rather than download a similar, freely available version?
more people have access to the similar, freely available version and can more easily discover its flaws

3. Explain the difference between separation of duty and separation of function.
separation of duty: several different subjects must be involved to complete a critical function;
separation of function: a single subject cannot complete complementary roles within a critical process

4. What is the importance of auditing in integrity contexts?
if something bad does happen, you can go back and assign responsibility and perhaps roll back or take care of whatever the problem was

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

6. Name a common scenario where integrity would be more important than confidentiality.
the commerical world

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.
my grades; information from tortured prisoners

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

expert >= student; {physics}⊇{physics};

novice < expert;

student >= novice; {art}⊇{}

3. Construct the NI policy for the integrity metapolicy.
there shouldn't be anything that sl can do that has effects visible to sh

4. What does it mean that confidentiality and integrity are “orthogonal issues?”
they are not really related to one another

Lecture 21

1. Why is Biba Integrity called the "dual" of the BLP model?
what biba said was why not use the mechanism that we already have in bell and lapadula and maybe mess it a little bit but come up with an analagous system

2. Why in the ACM on slide 5 is the entry for Subj3 - Obj3 empty?
neither subj3 nor obj3 dominates or is equal to the other

3. If a subject satisfies confidentiality requirements but fails integrity requirements of an object, can the subject access the object?
no

Lecture 22

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

2. Are the subjects considered trustworthy?
no

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

4. Are the subjects considered trustworthy?
yes

Lecture 23

1. Are the SD and ID categories in Lipner's model related to each other?
no

2. Why is it necessary for system controllers to have to ability to downgrade?
moving objects from the development to production world means changing their labels. there's no obvious way to do that in blp or biba

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

4. What form of tranquility underlies the downgrade ability?
weak tranquility

Lecture 24

1. What is the purpose of the four fundamental concerns of Clark and Wilson?
consistency among the various components of the system data

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

bank balances and checks

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

4. What is the difference between certification and enforcement rules?
certification rules: security policy restrictions on the behavior of integrity verification procedures (ivps) and transformation procedures (tps);
enforcement rules: built-in system security mechanisms that achieve the objectives of certification rules

5. Give an example of a permission in a commercial setting.
{user, tp, {cdi set}}; {customer, change password, {password}}

Lecture 25

1. Why would a consultant hired by American Airlines potentially have a breach of confidentiality if also hired by United Airlines?
he may carry some american airlines proprietary information that might disadvantage united airlines with respect to united airlines

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

3. Following the previous question, what companies' files are available for access according to the simple security rule?
gm, microsoft, and companies in any other conflict classes

4. What differences separate the Chinese Wall policy from the BLP model?
the chinese wall policy is designed to address a very specific concern: conflicts of interest by a consultant or contractor

Lecture 26

1. What benefits are there in associating permissions with roles, rather than subjects?
it makes managing an organization much more possible

2. What is the difference between authorized roles and active roles?
authorized roles: the roles a subject is allowed to fill at various times;
active roles: the roles a subject currently occupies

3. What is the difference between role authorization and transaction authorization?
role authorization: a subject's role must be an authorized role for that subject;
transaction authorization: a subject can execute a transaction only if the transaction is authorized for one of the subject's active roles

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

to RBAC?
hard to administer;
permissions are inappropriate to the organization;
does not recognize that a subject often has various functions within the organization;
does not allow a subject to transition between roles without having to change identities

Lecture 27

1. Why would one not want to build an explicit ACM for an access control system?
in realistic systems, most subjects don't have any access to most objects and the owner of a file can change the permissions at any time; storing hte matrix explicitly is expensive and usually unnecessary

2. Name, in order, the ACM alternatives for storing permissions with objects, storing permissions with subjects and computing permissions on the fly.
access control list (acl); capability-based system; 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 sender and receiver must have some shared knowledge and an agreed encoding scheme

2. Why would one want to quantify the information content of a message?
it is useful to know how much information can be transmitted over a specific covert channel. this is the "bandwidth" of the channel

3. Why must the sender and receiver have some shared knowledge and an agreed encoding scheme?
the receiver must know how to interpret the answer

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

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

Lecture 29

1. How much information is contained in each of the first three messages from slide 2?
n-bits; 4 bits; 7 bits; 168 bits

2. Why does the amound of information contained in “The attack is at dawn” depend on the receiver’s level of uncertainty?

if the only uncertainty were whether at dawn or dusk: one bit;
if the attack could have come anytime during the day: ? bits;
if the day was uncertain...: ? bits

3. How many bits of information must be transmitted for a sender to send one of exactly 16 messages? Why?
4; 2^4 = 16

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

5. Explain why very few circumstances are ideal, in terms of sending information content.
you don't know in advance exactly what messages could be sent

Lecture 30

1. Explain the difference between the two connotations of the term “bit.”
bit1: a binary digit (discrete);
bit2: a quantity of information (continuous)

2. Construct the naive encoding for 8 possible messages.
000, 001, 010, 011, 100, 101, 110, 111

3. Explain why the encoding on slide 5 takes 995 + (5 * 5) bits.
on average 99.5% will be message 10. the first bit represents whether the message is message 10 or not. the last four bits represent the 14 other messages. given 100 messages, on average 995 of them will be message 10, and 5 will be other messages. this encoding takes 995 + (5*5) bits

4. How can knowing the prior probabilities of messages lead to a more efficient encoding?
use fewer bits for the symbols that occur more frequently

5. Construct an encoding for 4 possible messages that is worse than the naive encoding.
0: message 1; 100: message 2; 101: message 3; 110: message 4

6. What are some implications if it is possible to find an optimal encoding?
messages take up less space, message passing is faster

Lecture 31

1. Name a string in the language consisting of positive, even numbers.
02468

2. Construct a non-prefix-free encoding for the possible rolls of a 6-sided die.
000: 1; 001: 2; 010: 3; 011: 4; 100: 5; 101: 6

3. Why is it necessary for an encoding to be uniquely decodable?
to prevent ambiguity

4. Why is a lossless encoding scheme desirable?
to prevent the loss of data

5. Why doesn’t Morse code satisfy our criteria for encodings?
not streaming

Lecture 32

1. Calculate the entropy of an 8-sided, fair die (all outcomes are equally likely).
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?
.721928

3. Why is knowing the entropy of a language important?
entropy sets a lower limit on encoding efficiency

Lecture 33

1. Explain the reasoning behind the expectations presented in slide 3.
it's the probability for the specific pairs of results

2. Explain why the total expected number of bits is 27 in the example presented in slide 4.
summation of (#count * bits in code) for each result

3. What is the naive encoding for the language in slide 5?
000: 1; 001: 2; 010: 3; 011: 4; 100: 5; 101: 6

4. What is the entropy of this language?
2.59092

5. Find an encoding more efficient than the naive encoding for this language.
00: 1; 01: 2; 100: 3; 101: 4; 110: 5; 111: 6

6. Why is your encoding more efficient than the naive encoding?
in my encoding, each number is represented in less than or equal to the number of bits as the numbers in the naive encoding