Brian Chow (brianj.chow@yahoo.com)
EID/CS login: bc23784
CS 361 (90155)
For 06/19/14

CS361 Questions: Week 2

Lecture 17

1) If a computer system complies with the BLP model, does it necessarily comply with non-interference? Why or why not?
    1. No, if the results of a failed write-down or successful read-up can be seen by S_L.
2) What would the NI policy be for a BLP system with subjects: A at (Secret: Crypto), B at (Secret: Nuclear)?
    1. They would not be allowed to interfere with each other.
3) Can covert channels exist in an NI policy? Why or why not?
    1. Yes, especially through shared system and/or inference. One user remotely sharing a computer with another user shouldn't be able to see what the other user is doing, but can make inferences as to what s/he's doing by looking at the CPU or disk utilisation. Another example would be if a lower-level user is working on a document that suddenly gets locked by a higher-level user. Another would be if a low-level shipping clerk notices in June 1944 that all ships have been requisitioned for some confidential purpose on June 6th.
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?
    1. *A* would be low and *B* would be high in order to establish a dominates relationship and for the information flow to be correct.

Lecture 18

1) Why do NI policies better resemble metapolicies than policies?
    1. They are abstract in nature, and fail to specify rules for (for example) "which subjects can read/write which objects".
2) What would be L's view of the following actions: h_1, l_1, h_2, h_3, . . . , h_j, l_2, l_3, . . . l_k ?
    1. l_1, l_2, l_3, l_k.
3) What is difficult about proving NI for realistic systems?
    1. Low-level system attributes must be analyzed, and many "intereferences" are benign (e.g., encrypted files).

Lecture 19

1) Explain the importance of integrity in various contexts.
    1. Integrity is a measure of who/what can write/modify information. The implications of faulty integrity range from "simply" blanking out a document to miscalculations resulting in incorrect calculations (e.g., Pentium FP bug) to taking over and redirecting resources to execute some other-than-intended program.
2) Why would a company or individual opt to purchase commercial software rather than

download a similar, freely-available version?
   1. Commercial software is more likely to be tested to a higher standard than freeware, and shouldn't contain any hidden procedures/malware that break integrity.
3) Explain the difference between separation of duty and separation of function.
   1. In the former, several different subjects must work together to complete a critical function; the latter is similar in nature, but states that a single subject cannot complete complementary roles while working towards completing a critical function.
4) What is the importance of auditing in integrity contexts?
   1. To determine who/what subject executed what function, to ensure correct results, and, if necessary, to be able to revert to a previous known-good state should a violation occur.
5) What are the underlying ideas that raise the integrity concerns of Lipner?
   1. Prevent a user from inserting some sort of backdoor into a program s/he writes, test programs on an “off-the-grid” system to prevent data breaches, log and record all actions during development and production for later analysis.
6) Name a common scenario where integrity would be more important than confidentiality.
   1. A calculator application producing incorrect results.

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.
   1. The former: a person with a graduate degree dispensing information related to his/her field of study, a journalist reporting from an on-site location, a textbook.
   2. The latter: someone eavesdropping on a private conversation, a rumour that *x*yz attack is going to occur against the US.
2) Explain the dominates relationships for each row in the table on slide 4.
   1. Row 1: an expert in physics is more trustworthy/reliable than a student learning physics.
   2. Row 2: a novice is not more reliable than an expert.
   3. Row 3: a student is more reliable than a novice.
3) Construct the NI policy for the integrity metapolicy.
   1. Don't allow information to “flow up” in integrity, so only allow a subject with higher integrity to interfere with a subject of lower integrity (and not vice versa).
4) What does it mean that confidentiality and integrity are orthogonal issues?
   1. They should be treated “at 90 degree angles”, that is, treated separately.

Lecture 21

1) Why is Biba Integrity called the “dual” of the BLP model?
   1. Its Simple Security (Integrity) and * Properties are the converse of those in the BLP model (i.e., no-write-up and no-read-down).
2) Why in the ACM on slide 5 is the entry for Subj3 - Obj3 empty?
   1. Neither dominates the other.
3) If a subject satisfies confidentiality requirements but fails integrity requirements of an object, can the subject access the object?
   1. No - it is satisfying BLP but failing Biba.

Lecture 22

1) What is the assumption about subjects in Biba's low watermark policy?
   1. Their integrity level can dynamically change.
2) Are the subjects considered trustworthy?
   1. Somewhat - their integrity levels can change after a read of low-integrity information.
3) Does the Ring Policy make some assumption about the subject that the LWM policy does not?
   1. It assumes that “a subject can properly filter the information it receives”.
4) Are the subjects considered trustworthy?
   1. Moreso than in the LWM policy.

Lecture 23

1) Are the SD and ID categories in Lipner's model related to each other?
   1. Only in that they are both assigned to subjects and objects.
2) Why is it necessary for system controllers to have the ability to downgrade?
   1. Somebody/something has to be able to change the labels of objects from development to production (this is not accounted for in either BLP or Biba).
3) Can system controllers modify development code/test data?
   1. No.
4) What form of tranquility underlies the downgrade ability?
   1. Weak Tranquility.

Lecture 24

1) What is the purpose of the four fundamental concerns of Clark and Wilson?
   1. To ensure “consistency among the various components of the system state”.
2) What are some possible examples of CDIs in a commercial setting?
   1. An order, check, invoice, or delivery form.
3) What are some possible examples of UDIs in a commercial setting?
   1. Information typed on a keyboard or a file uploaded by a user.
4) Give an example of a permission in a commercial setting.
   1. A user account in a system authorised to perform a transaction procedure(s) on a given set of constrained data items (e.g., read/execute a program, no write or installation abilities).

Lecture 25

1) Why would a consultant hired by American Airlines potentially have a breach of confidentiality if also hired by United Airlines?
   1. The consultant could, knowingly or unknowingly, pass on sensitive information not authorised to leave AA, or use that information to make biased decisions at UA, which could then be back-traced or extrapolated to glean more information on AA.
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?
   1. Yes. The two companies are in different conflict classes.
3) Following the previous question, what companies' files are available for access according to

the Simple Security Policy?

    1. Other files from GM, other files from Microsoft, Bank of America, Wells Fargo and Citicorp (with further access to the banking class defined by which banking company's files are accessed first).

4) What differences separate the Chinese Wall Policy from the BLP model?
    1. Write accesses are permitted only if access is permitted by the Simple Security Policy, and objects are subdivided into conflict classes.

Lecture 26

1) What benefits are there in associating permissions with roles, rather than subjects?
    1. There would be a reduced number of permissions sets, as there are usually multiple people with the same job position in a large company, reducing the potential for accidental unauthorized accesses or other mishaps occurring.
2) What is the difference between authorized roles and active roles?
    1. The former denotes all the roles for which an individual is authorized to fill at any given time; the latter denotes the roles for which an individual currently fills.
3) What is the difference between role authorization and transaction authorization?
    1. The former states that “a subject's active role must be an authorized role for that subject”; the latter builds upon that by only allowing a subject to “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?
    1. It allows multiple subjects with the same role to have different permissions and permissions are usually limited to being in terms of reading or writing a file

Lecture 27

1) Why would one not want to build an explicit ACM for an access control system?
    1. They would be massive in size, and there is no point when permissions can usually be computed on-the-fly.
2) Name, in order, the ACM alternatives for storing permissions with objects, storing permissions with subjects, and computing permissions on-the-fly.
    1. Access control list, capability-based system, maintaining a set of rules to compute access permissions 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?
    1. The receiver has to know that the sender can send a “yes” or “no” response as well as how to quantify any information received from the sender as such a response.
2) Why would one want to quantify the information content of a message?
    1. It would just be a meaningless stream of 0s and 1s otherwise.
3) Why must the sender and receiver have some shared knowledge and an agreed encoding scheme?
    1. Information is sent in bits with no apparent meaning attached to them - the receiver must know when the sender is sending a response as well as how to translate it into a meaningful response.

4) Why wouldn't the sender want to transmit more data than the receiver needs to resolve uncertainty?
    1. It could interfere with other operations of the receiver and/or open up a covert channel.
5) If the receiver knows the answer to a question will be “yes”, how many bits of data quantify the information content? Explain.
    1. 0 bits. If the answer is always yes, then there is no confusion from the receiver that needs to be resolved. (1 bit if a response is still always needed from the sender before the receiver can take action.)

Lecture 29

1) How much information is contained in each of the first three messages from slide 2?
    1. *n* bits, 1 to 4 bits, 4 to 7 bits.
2) Why does the amount of information contained in “The attack is at dawn” depend on the receiver's level of uncertainty?
    1. It depends on if the receiver needs to know the day of the attack, if the attack can occur at any other time if not at dawn, and/or when “dawn” actually is (not exclusive).
3) How many bits of information must be transmitted for a sender to send one of exactly 16 messages? Why?
    1. 4, not including the message itself, because 4 bits are required to represent up to 16 different numbers.
4) How much information content is contained in a message from a space of 256 messages?
    1. 8 bits of information content.
5) Explain why very few circumstances are ideal, in terms of sending information content.
    1. It is very difficult to encode a transmission such that each bit transmitted reduces the level of uncertainty by half.

Lecture 30

1) Explain the difference between the two connotations of the term “bit”.
    1. A bit can either refer to a single 0 or 1, or a continuous stream of 0s and 1s.
2) Construct the naïve encoding for 8 possible messages.
    1. For messages 0 through 7, in order: 0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000.
3) Explain why the encoding on slide 5 takes 995 + (5 * 5) bits.
    1. 99.5% of the time, the message will be 1 bit in length (message 10); the other 5 times, the message will be 5 bits in length.
4) How can knowing the prior probabilities of messages lead to a more efficient encoding?
    1. It could allow the number of bits needed for the encoding to be reduced. In the above example, if all messages were encoded with 5 bits each, then the encoding would take (1000 * 5) = 5000 bits or 5 bits per message, much more than 1020 bits or 1.02 b/m.
5) Construct an encoding for 4 possible messages that is worse than the naïve encoding.
    1. Padding each message using the naïve encoding (3 bits per message) with one or more leading 0s.
6) What are some implications if it is possible to find an optimal encoding?
    1. “Doing better” (using “fewer bits, on average, to transmit messages in the language”), and eliminating a possible covert channel.

Lecture 31

1) Name a string in the language consisting of positive, even numbers.
   1. “[4][16][28][2][146][996][1000002][8]” (brackets added for delineation).
2) Construct a non-prefix-free encoding for the possible rolls of a 6-sided die.

   1: 0
   2: 1
   3: 10
   4: 11
   5: 100
   6: 101
3) Why is it necessary for an encoding to be uniquely decodable?
   1. Multiple legal decodings could result in a worthless message being decoded at runtime.
4) Why is a lossless encoding scheme desirable?
   1. Lost symbols would result in a different decoding with a potentially different message.
5) Why doesn't Morse Code satisfy our criteria for encodings?
   1. There would be a large number of breaks in the transmission (streaming property).

Lecture 32

1) Calculate the entropy of an 8-sided, fair die (all outcomes are equally likely).
   1. h = - ([1/8 * log(1/8)] * 8) = 3 bits per symbol
2) If an unbalanced coin is 4 times more likely to yield a tail than a head, what is the entropy of the language?
   1. h = - ([4/5 * log(4/5)] + [1/5 * log(1/5)]) = - (-0.2575424 + -0.4643856) ~= 0.721928 b/s
3) Why is knowing the entropy of a language important?
   1. It allows us to determine the “information content of an average symbol in a language” and see how efficient it is at conveying information.

Lecture 33

1) Explain the reasoning behind the expectations presented in slide 3.
   1. Given P(H) = ¾ and P(T) = ¼, P(HH) = ¾ * ¾ = 9/16, P(HT) == P(TH) = ¾ * ¼ = 3/16, P(TT) = ¼ * ¼ = 1/16.
2) Explain why the total expected number of bits is 27 in the example presented in slide 4.
   1. HH, HT, TH, and TT are represented by 1, 2, 3, and 3 bits, respectively. Using the probabilities calculated above, the total number of bits expected is [(9 * 1) + (3 * 2) + (3 * 3) + (1 * 3)] = 27 bits.
3) What is the naïve encoding for the language in slide 5?
   1. For messages 0 through 4, in order: 000, 001, 010, 011, 100.
4) What is the entropy of this language?
   1. Since P(1) = P(2), P(3) = P(4), P(5) = P(6), P(1) = 2P(3) and P(3) = 2P(5), 4P(5) + 4P(5) + 2P(5) + 2P(5) + P(5) + P(5) = 1, and P(5) = 1/14.
   2. h = - ({2 * [2/7 * log(2/7)]} + {2 * [1/7 * log(1/7)]} + {2 * [1/14 * log(1/14)]})
      ~= 2.37878349349 bits per symbol

5) Find an encoding more efficient than the naïve encoding for this language.

    1: 0
    2: 10
    3: 1101
    4: 1111
    5: 1110
    6: 11000

6) Why is your encoding more efficient than the naïve encoding?

    1. Expected number of bits = 4 + (4 * 2) + (2 * (2 * 4)) + 4 + 5 = 37 bits
    2. Expected number of bits using naïve: (2 * (4 * 3)) + (2 * (2 * 3)) + (2 * (1 * 3)) = 42 bits
    3. (The non-prefix-free encoding in Lecture 31, #2 is expected to use 22 bits.)