Colin Murray

UTEID: Cdm2697

UTCS-username: Tashar

Email: murray.colin43@gmail.com

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?

   If the actions of a high level subject have some noticeable effect from a low level subject's perspective, these actions in and of themselves complying with BLP security policies, than the high level subject might abuse this to send information to the low level subject through the covert channel.
2. What would the NI policy be for a BLP system with subjects: A at (Secret: Crypto), B at (secret: Nuclear)?

   A -> A, B -> B

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

   No, the goal of a NI policy is such that nothing a high level subject does can "interfere" with a lower level subject, meaning that the lower level subject can see no consequences of the higher level subject's actions.
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}, {A = high, B = high}, {A = low, B = Low}

Lecture 18

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

   NI simply suggests that information can only flow from low to high and doesn't specify rules on which subjects can read/write which objects. This is essentially the metapolicy of BLP.
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?

   NI is more abstract compared to BLP and given the high levels of complexity in real world systems it can be very difficult to address all the possible actions a high level subject can make in

order to prevent interference with a low level subject. L's view must be heavily restricted in real world systems to a possibly impractical level to fully achieve non-interference.

Lecture 19

1. Explain the importance of integrity in various contexts.

   The integrity of information can be just as important as its confidentiality. Say for instance a news organization will hire anyone who can make up an amusing story, true or not, like *The National Enquirer* for example organization and its publications will have a low integrity compared to organizations like *The New York Times* which hold the trust of their readers by hiring qualified and honest individuals. Since those who can modify data (or write news stories in this case) are held to a lower standard with the *National Enquirer* than *The New York Times* it is no surprise that the integrity of *National Enquirer* is much lower. Another context in which this is relevant might be how an operating system determines which processes may modify certain critical directories (such as win32). A process installed owned by some random organization may be assumed to have lower "trustworthiness" than an OS process or one run as an administrator by the user and thus be declined any write privileges.
2. Why would a company or individual opt to purchase commercial software rather than download a similar, freely available version?

   The company has to maintain a degree of trust with their customer in order to stay in business, otherwise their integrity would suffer and future buyers may be dissuaded. Free software on the other hand does not have to worry about future buyers and may even benefit from violating the trust of the user and stealing assets.
3. Explain the difference between separation of duty and separation of function.

   To increase the likelihood that a function is done with higher integrity, separation of duty would require that several different subjects must participate in order to complete that function. If there is a chance that one subject is less trustworthy than the trustworthy subjects might prevent the untrustworthy subject from performing any malicious actions. Separation of function conversely would prohibit one subject from performing multiple functions. The possible damage that can be done by one malicious subject is mitigated if it can only perform one task.
4. What is the importance of auditing in integrity contexts?

   If a breach of integrity does occur, careful auditing may allow the system to recover completely or hold whichever subject responsible accountable, allowing steps to be taken in order to prevent this subject from doing any more damage.
5. What are the underlying ideas that raise the integrity concerns of Lipner?

   Lipner found that integrity was often more important than confidentiality in commercial settings. In order to offer trustworthy, consistent and reliable commercial software Lipner lists the following concerns to consider:
   a. Users will not write their own programs, but instead use existing production software.

   b. Programmers develop and test applications on a nonproduction system, possibly using contrived data.
   c. Moving applications from development to production requires a special process.
   d. This process must be controlled and audited
   e. Managers and auditors must have access to system state and system logs.
6. Name a common scenario where integrity would be more important than confidentiality.

   News organizations often present information (news stories) publically with little concern over confidentiality, but must take great measures if they are to remain reputable and trusted to control the integrity of information presented in these stories. Other examples include pages like Wikipedia that allow anyone to edit unprotected pages but mandate more rigorous requirements when editing "protected" pages in order to maintain some degree of integrity with the information presented on their website. Since their goal is give unrestricted access to all the information on their website and provide as honest and reliable information as possible, integrity is a much higher concern.

Lecture 20

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

   The value of UTC time is not sensitive at all but must be extremely reliable as many important, time sensitive systems rely on it. On the other hand, some testimonials or anonymous tips in criminal investigations may be treated with a high degree of sensitivity but a low degree of integrity (as the information may be misleading or untrustworthy depending on the source).
2. Explain the dominates relationship for each row in the table on slide 4.
   a. Row1: Label 1 dominates Label 2 since {Expert : (Physics)} should be more reliable and have a higher integrity than {Student : (Physics)}
   b. Row2: Neither dominates the other since Label 2 {Expert : (Physics)} cannot comment on information that is (Physics, Art) given he lacks any trustworthiness when art is concerned. Label 1 does not dominate Label 2 since as a Novice in (Physics, Art) he cannot be deemed trustworthy to comment on {Expert : (Physics)}, even though Physics is included in his domains of interest.
   c. Row3: Label 1 dominates label 2 since Student is more trustworthy than Novice and Label 2's domain of {} is a subset of Label 1's domain of {Art}.
3. Construct the NI policy for the integrity metapolicy.

   A subject with low integrity shouldn't be able to interfere with a subject with high integrity. (i.e. H -> L)
4. What does it mean that confidentiality and integrity are "orthogonal issues?"
   In BLP's confidentially model, confidential information must only be allowed to flow upward. In integrity systems information cannot flow upward and instead must only flow downward. They are orthogonal since their metapolicies' view on information flow are polar opposites.

Lecture 21

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

   Biba Integrity has analogous policies to BLP. In this case the Simple *Integrity* Property which is the inverse of BLP's Simple Security Property and the *Integrity* *-property which is the inverse of BLP's *-property. Thus it is essentially the "dual" or inverse of the BLP model.
2. Why in the ACM on slide 6 is the entry for Subj3-Obj3 empty?

   Subj3 does not dominate Obj3 nor does Obj3 dominate Subj3. This is because Subj3's {A, B} is not a subset of Obj3's {B, C} or vice versa.
3. If a subject satisfies confidentiality requirements but fails integrity requirements of an object, can the subject access the object?

   No, access is only allowed if *both* BLP's and Biba's policies are satisfied.

Lecture 22

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

   Subjects still follow the integrity *-policy as with Biba Integrity, however they are allowed to read any information but their trustworthiness can change depending on what they read. Thus if a subject ever taints itself be reading an object at an integrity level lower than itself, its own label will be demoted to match the object's.

2. Are the subjects considered trustworthy?

   No, they are only as trustworthy as the lowest integrity object they choose to read.
3. Does the Ring policy make some assumption about the subject that the LWM policy does not?

   It assumes that subjects are sensible enough to filter out information they choose to write such that the integrity of a system is not compromised by what they have read.
4. Are the subjects considered trustworthy?

   Yes, Subjects are trusted to make sensible decisions on what information they should write and are not demoted based on if they read down.

Lecture 23

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

   They are related in that both deal with the development of software. An ordinary user would never possess SD or ID categories.
2. Why is it necessary for system controllers to have the ability to downgrade?

   In order to keep the software development process going there must be some subject that has the ability to downgrade an object (piece of software) such that it may be released from development to production (otherwise the developers could never release the software they're working on).

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

   No, they fail the confidentiality *-property for writing (they must be dominated by the object to write, their label of (SL, {SP, SD}) dominates the development code/test data's confidentiality label of (SL, {SD}). Despite the fact that they pass integrity *-property requirements for writing that mandate the subject (system controllers) {ISP, {IP, ID) must dominate the object (development code/test data) {ISL, {ID}), they must fulfill both confidentiality and integrity requirements to modify the development code/test data.
4. What form of tranquility underlies the downgrade ability?

   Weak tranquility since downgrade is given in a way that doesn't violate the spirit of the integrity and confidentiality requirements in the system.

Lecture 24

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

   They are meant to address integrity in such a way that it can be applied to yield a workable commercial policy, ideally achieving consistency among the various components of the system state.
2. What are some possible examples of CDIs in a commercial setting?

   Bank balances, audit reports, employee payroll information
3. What are some possible examples of UDIs in a commercial setting?

   Somewhat subjective but possibly the # of free samples taken by customers, # of times the entranceway door was opened, anything of trivial concern with regard to integrity.
4. What is the difference between certification and enforcement rules?

   Certification rules specify in a more abstract manner how the basic concepts of Clark and Wilson (CDIs, UDIs, IPVs and TPs) cooperate and what requirements each must meet. Enforcement rules detail less-abstract mechanisms by which the certification rules are met in real world usage.
5. Give an example of a permission in a commercial setting.

   {*user* = bank customer, *TP* = withdrawal, *CDI set* = (bank account balance, withdrawal history,…)}

Lecture 25

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

   In moving from American Airlines to United Airlines this consultant may carry with him some proprietary information along with him that may disadvantage American 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, since Microsoft and GM exist in separate conflict classes there is no risk of a Chinese Wall security violation.
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?

   The Chinese Wall policy attempts to stop information from flowing between conflict classes, none of which have a higher or lower security label than the other (no hierarchal structure). BLP focuses on the flow of information in a hierarchal and categorical security system and has no notion of conflict classes.

Lecture 26

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

   In large organizations it might be impossible to adequately assess, assign and maintain custom tailored access control labels to each individual in the organization, especially as roles and circumstances change. It is much easier and more practical to associate permissions with functions/jobs/roles within the organization and allow subjects to possess these rolls in order to do their jobs properly with sufficient access.
2. What is the difference between authorized roles and active roles?

   An authorized roll is a role that an individual is allowed to fill at various times, an active role is one that the subject currently occupies.
3. What is the difference between role authorization and transaction authorization?

   Role authorization makes sure the subject is actually authorized to have a particular active role in a given moment. Transaction authorization goes further to specify that some transactions are authorized to specific roles and thus for a subject to execute a transaction the subject must possess a role which is authorized to make the transaction.
4. What disadvantages do standard access control policies have when compared to RBAC?

   Standard access control policies require assignment of permissions to each individual subject which is much harder to administer than the roles in RBAC. Permissions in standard access control are somewhat abstract (like "read/write") where they can be much more custom tailored to an organization in RBAC (like "open an account"). Standard access control prohibits a subject from possessing multiple labels for confidentiality and multiple for integrity whereas it's easy to have a subject possess multiple roles in RBAC (which is good since subjects often have multiple functions within an organization), each role having sufficient permissions to perform

the role effectively. Finally RBAC allows a subject to transition between roles where in standard access control policies a subject would be forced to change identities.

Lecture 27

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

   Generally there are a very large number of different subjects and objects in a system and in most cases subjects will only have access to a small percentage of objects, making a lot of empty subject-object pairings in the matrix.
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, capability based system, Implicit rules

Lecture 28

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

   The receiver must know that the sender plans on sending either a yes or a no and each sender and receiver must have agreed in advance how to interpret the sender's message into one of the two categories {"yes", "no"}
2. Why would one want to quantify the information content of a message?

   Understanding how to quantify the information content of a message can lead to efficient encoding schemes that pass more information through equivalent bandwidths. This is very important to optimize any sort of information transfer.
3. Why must the sender and receiver have some shared knowledge and an agreed encoding scheme?

   If the sender starts transmitting information to the receiver using an encoding scheme unknown to the receiver, the receiver has no way to interpret the content of the message.
4. Why wouldn't the sender want to transmit more data than the receiver needs to resolve uncertainty?

   In a world of limited bandwidth and increasing demands for speed it is important to find efficient encoding schemes that send only the minimum amount of data possible to reconstruct the message. This is especially important when bandwidth could be severely limited like in 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.

   Since the answer is already known, no information transfer is necessary to confirm the already known value ("yes"). In this case 0bits quantify the information content.

Lecture 29

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

   - N bits
   - 4 bits
   - 7 bits
2. Why does the amount of information contained in “The attack is at dawn” depend on the receiver’s level of uncertainty?

   If the receiver knows the sender will send a message that is contained within a set of known possibilities (“The attack is at dawn” being one of these possibilities) than the sender must only send n bits where 2^n >= #possibilities. If the receiver knows it will be at dawn or at dusk than only 1 bit of information is necessary. However if more possibilities emerge due to uncertainty in other factors like multiple days, more times in the day it could happen, ect the number of bits necessary to transmit this message increases. In the worst case the receiver has no certainty and the entire message in ascii is sent (assuming the receiver at least knows how to decode ascii).
3. How many bits of information must be transmitted for a sender to send one of exactly 16 messages? Why?

   4 bits. Since there are 16 possibilities and $\log_2(16) = 4$, there are exactly 16 different combinations of 4 bits possible, each which can be paired to a particular message.
4. How much information content is contained in a message from a space of 256 messages?

   $\text{Log}_2(256) = 8$
5. Explain why very few circumstances are ideal, in terms of sending information content.

   Uncertainty in the information content of a messages in real life can be fairly large. Many systems could be optimized if there were a ridged, known set of possibilities but this is rarely the case.

Lecture 30

1. Explain the difference between the two connotations of the term “bit.”

   One connotation is of the literal computer bit with a value 0 or 1 whereas a continuous bit or stream of bits is more a measure of quantity of information (like bits per second).
2. Construct the naïve encoding for 8 possible messages.

   M1 = 000 ; M2 = 001 ; M3 = 010 ; M4 = 011 ; M5 = 100 ; M6 = 101 ; M7 = 110; M8 = 111
3. Explain why the encoding on slide 5 takes 995 + (5 * 5) bits.

   In the example it is assumed that 99.5% of messages sent are M10. Since M10 is indicated by a single 0 and all other messages are distinguished be a leading 1 (making the number of bits required to transmit one of the 16 possible error messages 5 rather than 4) we get:

(# messages) * (0.995) * (1 bit for transmitting a 0 for M10) + (# messages) * (0.005% chance for an error message) * (# bits needed to encode error messages).

The example also specifies 1000 messages are transmitted in this encoding so by plugging that into the equation we get (1000 * 0.995 * 1) + (1000 * 0.005 * 5) = 995 + (5 * 5)

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

   Sacrifices can be made if probabilities are known to reduce the number of bits necessary to transmit the most common message/s at the cost of increasing the number of bits necessary to transmit the less common messages. In the example above, on average only 1.02 bits are sent per message vs. 4 bits per message in the naïve approach because the most common message sent (M10) was transmitted by only sending a single bit (0) rather than 4 in the naïve approach.
5. Construct an encoding for 4 possible messages that is worse than the naïve encoding.

   m1 = 1000; m2 = 0100; m3 = 0010 ; m4 = 0001
6. What are some implications if it is possible to find an optimal encoding?

   Is there a known set of possibilities for the message being sent? Out of these possibilities, are some messages sent with a higher probability than others? What is the most efficient assignment of bit codes to messages according the probabilities of each message that still yields an encoding scheme where each encoded message is still uniquely decodable?

Lecture 31

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

   2462846286644
2. Construct a non-prefix-free encoding for the possible rolls of a 6-sided die.
   1 = 1
   2 = 10
   3 = 100
   4 = 1000
   5 = 10000
   6 = 100000

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

   The receiver must be able to recover unambiguously what message the sender is trying to send, otherwise the receiver may misinterpret the message and react incorrectly.
4. Why is a lossless encoding scheme desirable?

   A lossless encoding scheme means that no information is lost from the receiver's end when trying to reconstruct the message. Generally losing information in a transmitted message is undesirable, especially if any lost information can make the receiver's interpretation unclear (transmitting text that becomes garbled as characters are lost for example).

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

   Morse code is not streaming, in this case because it requires a break in between each message since it's not prefix-free and uniquely decodable without these spaces.

Lecture 32

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

   $h = -\sum_{1\text{-}8}(1/8\text{Log}_2(1/8)) = 8(1/8\text{Log}_2(1/8)) = \text{Log}_2(1/8)$
   $h = 3$
2. If an unbalanced coin is 4 times more likely to yield a tail than a head, what is the entropy of the language?

   $h = -(1/5\text{Log}_2(1/5)+4/5\text{Log}_2(4/5)) \approx 0.72$

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

   Knowing the entropy of a language allows you to determine what the lower limit for the amount of bits are required to encode a message in that language efficiently. This gives us a good way to measure the efficiency of any existing encoding and gives a known lower limit that cannot be surpassed.

Lecture 33

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

   Since you cannot reduce the encoding scheme for the 2 possibilities of {heads, tails} any lower than 1 bit, even though the entropy states the minimum as being 0.811 bits, it is desirable to wait for more results before transmitting to in effect expand the number of possible messages that can be transmitted. On slide 3 the language is expanded from all combinations of a single flip into all combinations of 2 consecutive flips which yields 4 possibilities in the transmitted message rather than just 2. This allows the transmission of the most common event (heads, heads) with just a single bit rather than the 2 bits that would be needed to transmit the event when there was only 2 possible messages. This is done at the acceptable cost of increasing the number of bits to transmit other less likely combinations (HT, TH, TT).
2. Explain why the total expected number of bits is 27 in the example presented in slide 4.

   Since all the probabilities of the events (HH, HT, TH, TT) share the common denominator of 16, out of 16 occurrences of these events (32 flips) it the most likely breakdown of results is HH = 9, HT = 3, TH = 3, TT = 1. The encoding for this scheme favors sending only 1 bit (0) to indicate the HH event occurred since it is most common, meaning of 32 flips it's expected the sender will send 9 bits. HT and TH have the same probability but one is arbitrarily chosen (HT) to be paired with the 2 bit code (10) and the other (TH) is paired with the 3 bit code (110). HT (10) will likely show up 3 times in the 32 flips yielding an expected transmission of 3 * 2 bits = 6 bits. TH (110) on the other hand yields an expected transmission of 3 * 3 = 9 bits. Finally TT (111) yields an

expected transmission of 1 * 3 = 3 bits since of the 32 flips this combination is only expected to occur once. Adding up the expected number of bits to be transmitted for all events we get 27 total bits needed to transmit the most likely scenario of 32 coin flips with our encoding scheme. The efficiency can then be measured as 27 bits / 32 flips ≈ 0.844, a good deal better than the naïve encoding with the efficiency of 32 bits / 32 flips = 1.

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

4. What is the entropy of this language?

Roll	likelyhood
1	6/20
2	6/20
3	3/20
4	3/20
5	1/20
6	1/20

   $h = -(2(6/20 \log_2(6/20)) + 2(3/20 \log_2(3/20)) + 2(1/20 \log_2(1/20))) \approx 2.295$

5. Find an encoding more efficient than the naïve encoding for this language.
   1 = 0
   2 = 10
   3 = 110
   4 = 1110
   5 = 11110
   6 = 11111

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

   Suppose the dice is rolled 20 times

Roll	count	code	bits
1	6	0	6
2	6	10	12
3	3	110	9
4	3	1110	12
5	1	11110	5
6	1	11111	5
			49 total bits

In the naïve approach each dice roll took 3 bits to transmit. For 20 rolls it would take on average 3 * 20 = 60 bits to communicate the results

The encoding scheme above costs only 49 bits on average to communicate the results of 20 rolls making it the more efficient option.