Questions for CS 361, Week 1

Mark Watts (csid:markw,eid:mw27428,email:mark.watts@utexas.edu)

Lecture 1

1. What uses of the term “security” are relevant to your everyday life?

   To list them: computer security, information security, home security, personal security,network security. In other words, being secure in my person, communications, data, and physical property.

2. What do these have in common?

   Home security and personal security are outside of the domain of computer security. Information, network, and computer security are equally concerned with the loss of data.

3. Have you been a victim of lax security?

   Yes. Computer users unfamiliar with internet threats have inadvertently downloaded malware that hogs our internet connection.

4. What is the likelihood that your laptop is infected? How did you decide?

   On a scale of 1-10: 2. There are probably bugs that I'm unaware of, but I don't download and run strange software or visit many unfamiliar websites.

5. What security measures do you employ on your laptop?

   Encrypted home directory, semi-regular backups of personal data, yearly re-install of OS.

6. Do you think they are probably effective?

   Against data lossage they could be better, for instance I could have more regular or more complete backups. Home directory encryption may not be effective for the most likely threats.

7. Consider the quote from the FBI official on slide 10. Do you think it overstates the case? Justify your answer.

   Whether this is an overstatement depends on whether key strategic computers such as those that have access to infrastructure or weapons systems are accessible to unauthorised people or programs. The quote implies that's the case for virtually every computer, but this 'virtually' may be exclusive of these key systems. The other qualifier to this statement is that the access, even taken together with a motive, is not sufficient to elevate the risk to sensational levels. In addition to these factors, we would need to calculate the risk the adversaries are put at by conducting the attack as well as how they *perceive* that risk. It may be the case that potential adversaries avoid attacking the United States for fear that the giant will fall on their house --- that the interconnectedness of the United States could lead to damage for the attacker's homeland or person if it were fatally harmed.

8. What is the importance in learning about computer security?

   For the population generally, it would mitigate one of the points on slide 7, the low threshold to access. By making the average user more knowledgeable about potential threats, it is less of an issue that more people can access computer systems. However, this assuming that the people who learn security employ their knowledge effectively and for good. For computer programmers, it is vital because computer programs are components of infrastructure in our modern day. Insufficient regard for security concerns leads to preventable errors in software. These concerns affect everyone working in the IT sector as well since computer security deals with factors surrounding computers -- who has physical access, where data centers are located, training for users of critical systems, etc. -- as well as within them.

Lecture 2

1. Consider the five reasons given why security is hard. Can you think of other factors?

   Different ideas of security based not only on their actual values and needs, but also on what others have told them. The *label* of security can sometimes be a barrier to achieving true security.

2. Is there a systematic way to enumerate the “bad things” that might happen to a program? Why or why not?

If to enumerate is to list *all* of the bad things, then probably not. Part of the reason is contained in 'might happen': we're talking about an arbitrary system, so we can consider one for which requirements change over time. Requirements mean features, mean new attack scenarios not previously considered because they didn't exist. We could still consider a system of enumeration that can be continued incrementally from earlier enumerations, but it seems to me that this denies the possibility of interaction between features which could *create* weaknesses or obscure ones previously accounted for. Furthermore, this is a assuming a static set of assets.

3. Explain the asymmetry between the defender and attacker in security.

   Attackers only need to break one system one time to make a payoff, but defenders must defend against innumerable attackers at any time to prevent the harms of an attack.

4. Examine the quotes from Morris and Chang. Do you agree? Why or why not?

   Perfect security means, to me, that no information could be gotten from a system which would not be publicly exposed --- publicly exposed meaning those outputs from the system that are specified for return from valid inputs (if any) to the system. Given what I've read about 'side-channel' attacks, employing seemingly innocuous physical access to subvert or monitor a system, I would agree with the quotes. We could always imagine an attacker that was physically the same as a fully authorised user, differing only in his malicious intent. Providing any access provides this 'doppelganger' attacker with harmful capability.

5. Explain the statement on slide 8 that a trade-off is typically required.

   Going back to the previous question, we need our computer systems to be useful -- to have some *outputs* corresponding to some *inputs* -- to even bother securing them. However, there should be a point at which access must give way to the threats of data lossage, corruption, or unwanted exposure. Restated, the assets which we have are assets, effectively, because they expose themselves to threats, so security must designed to minimize necessary threats.

Lecture 3

1. Define “risk”

   The possibility that a particular threat will adversely affect an information system.

2. Do you agree that software security is about managing risk?

   Yes. Perfect security is not possible in any useful system, but threats can be identified, if not exhaustively, at least extensively and the risk associated with each can be addressed.

3. Name and explain a risk you accept, one you avoid, one you mitigate, and one you transfer?

   Accept: Struck by lightning. You have to go out some time and I love thunderstorms. Avoid: Mugging. I don't go downtown at night. Mitigate: Government seizure of funds. I maintain a collection of off-shore accounts. Transfer: Poison. I have a designated taster check all of my meals.

4. Evaluate annualized loss expectancy as a risk management tool.

   Annualized loss expectancy doesn't take into account some of the danger that a particular event happening which would be catastrophic -- it's a linear model (linear in the cost of the threat). The example from class is of a bank that can't sustain a great loss which, however, is unlikely to happen. The ALE may be low, but there should still be significant protection against this because the threat isn't in proportion to the ALE.

   We've also addressed the question of whether ALE is the appropriate risk assessment model and compared it to the human model of risk assesment. For me, the comparison is crucial-- not because we care to model human risk assesment as a psychological phenomenon, but rather because the we define risk to the defender in terms of his perceived assets and harms. In the bank example we use dollars lost, but a weakness of the form of ALE that we have seen is that it is only in one dimension, excluding other dimensions which may affect the abstract notion of risk. Brining in these other dimensions may be difficult because we still need to order them, but I think it's definitely worthwhile to think about them at least informally.

5. List some factors relevant to rational risk assessment.

   - Asset quantification
   - Threat identification
   - Exploit probability - probability that an asset will be lost/devalued through a threat
   - Risk assessment
   - Trade-offs

  - Technical concerns - how to implement desired security measures

Lecture 4

1. Explain the key distinction between the lists on slides 2 and 3.

   Slide 2 describes aspects of security which items in the second slide are meant to enable.

2. Consider your use of computing in your personal life. Which is most important: confidentiality, integrity, availability? Justify your answer.

   Integrity is most important to me. Very few of my actions in computer systems actually need to be hidden: my financial transactions are could be publicised without damage to me, my work is publicly displayed, and even my personal actions are incredibly banal. Availability is a close second because I rely heavily on data sources to be correct for me to function. However, most of these data which I require to be available are out of my control, so I don't actively concern myself with them. Integrity of my transactions is absolutely crucial to my life and work and it is something I can effect by keeping my own transaction logs and regulating edit access to my information.

3. What does it mean “to group and categorize data”?

   Data assets can be put into categories based on threats associated with their use and misuse. These groupings go into a policy describing who can access data and in what ways. More sensitive data is more tightly regulated against exposure.

4. Why might authorizations change over time?

   An authorised individual could be fired, demoted, promoted, transfered, given additional responsibilities, work from a different location. Almost any change in the working conditions of agents in a system might merit a change in authorisation.

5. Some of the availability questions seem to relate more to reliability than to security. How are the two related?

   Reliability describes the software and machinery on which a system operates. Reliability provides availability in the face of faults.

6. In what contexts would authentication and non-repudiation be considered important?

   Non-repudiation is useful primarily in transactions of goods, services, and money. Bitcoin (and technical successors) provide this through the 'blockchain' and public identifiers. Authentication is important in virtually every online community as it is the primary means of establishing identity in otherwise anonymous contexts.

Lecture 5

1. Describe a possible metapolicy for a cell phone network? A military database?

   GSM Cell Network

   > Meta-policy: Voice and messages are directed towards the intended recipient. Policy: SIM cards must be associated with only one phone number.

   Military database

   > Meta-policy: Enemies cannot gain any knowledge about troop positions. Policy: All personnel are given a unique pass-phrase for access to the database.

2. Why do you need a policy if you have a metapolicy?

   A meta-policy gives no specific instruction on how to achieve the goal set out, but a policy contains implementation detail.

3. Give three possible rules within a policy concerning students’ academic records.

   1. No student can access records of another student.
   2. Grades must remain on record indefinitely.
   3. A student can request to have academic records restricted to teaching faculty and the registrar's office.

4. Could stakeholders’ interest conflict in a policy? Give an example.

Yes.

5. For the example given involving student SSNs, state the likely metapolicy.

   To mitigate the possibility that a student's identity can be stolen through unauthorised access to university documents.

6. Explain the statement: ”If you don’t understand the metapolicy, it becomes difficult to justify and evaluate the policy.”

   As stated, each policy rule is one remove from the over-arching goal. Taken separately, each policy rule, may cannot embody the entirety of the goal. Together the *interactions* of the rules make them more than the sum of their parts, but even this can be hard to interpret for complex policies without knowing the meta-policy.

Lecture 6

1. Why is military security mainly about confidentiality? Are there also aspects of integrity and availability?

   Our modern military operates by hiding the truth of its high-level motives from the people who actually carry out orders. Higher level orders, if exposed to lower level operatives, would likely lead to uncertainty or exposure of secrets to the public or to enemies.

   I think the focus on confidentiality is a function of our own interests:

   > For any military, integrity is important for communications of mission critical information like troop and target positions and attack timelines.
   >
   > Availability is necessary for communications and navigation on the field. In particular, the early internet as a military project was designed to be resilient to faults so that communications would available in the face of sabotage to some subset of the network.

2. Describe the major threat in our MLS thought experiment.

   The major threat is that someone without appropriate respect for the sensitivity of the facts in our data store exposes them to enemies.

3. Why do you think the proviso is there?

   Our only concern in this scheme is with confidentiality -- the other security concerns are not addressed

   Also, the (perhaps unwarranted) assumption is that the classifications given to agents correspond to their trustworthiness.

4. Explain the form of the labels we’re using.

   The labels are grouping classifiers. One set describes the type of information and the other sensitivity level. These labels are assigned to people and documents for the usage described on the slides.

5. Why do you suppose we’re not concerned with how the labels get there?

   Assigning labels is about trust. Assignments are fundamentally a human issue and outside of the scope of this scheme.

6. Rank the facts listed on slide 6 by sensitivity.

   Least 1 3 5 4 2 6 Most

7. Invent labels for documents containing each of those facts.

   1: (Unclassified, {Personnel, Publications, President}) 2: (Top Secret, {Army, Officers, President}) 3: (Unclassified, {Cafeteria, Financial, Supplies, President}) 4: (Secret, {Financial, Officer-General, President}) 5: (Secret, {Financial, Officer-General, President}) 5: (Top Secret, {Officer-General, President})

8. Justify the rules for “mixed” documents.

   For Rule 1: The goal is to protect sensitive information. Hiding the sensitive outweighs exposing for the sake of unprivileged. For Rule 2: Hiding information could limit an agent's ability to do work, but exposing information from other categories isn't necessarily damaging.

Lecture 7

1. Document labels are stamped on the outside. How are “labels” affixed to humans?

   Rank insignia, biological factors, work uniform, id cards.

2. Explain the difference in semantics of labels for documents and labels for humans.

   - Human labels indicate clearance, what can be accessed by that person.
   - Document labels indicate confidentiality, who can access that document.

3. In the context of computers what do you think are the analogues of documents? Of humans?

   Documents = Files in POSIX systems

   Humans = Humans + Programs

4. Explain why the Principle of Least Privilege makes sense.

   We assume that anyone has the potential to leak information. Giving them the least information necessary prevents leaks.

5. For each of the pairs of labels on slide 6, explain why the answers in the third column do or do not make sense.

   1. Makes sense because the clearance is above the document security level.
   2. Makes sense because the clearance is below the document security level.
   3. Makes sense because the clearance categories include {} and the clearance is above the document security level.

Lecture 8

1. Why do you think we introduced the vocabulary terms: objects, subjects, actions?

   They are commonly used in the literature.

2. Prove that dominates is a partial order (reflexive, transitive, antisymmetric).

   Note: $\geq'$ is used as the partial order on security levels

   Reflexive: Let $L = (A, B)$.

      $A \geq' A$ is true as $\geq'$ is a partial order. $B \subseteq B$ is true of all sets. Therefore, $L \geq L$

   Transitive: Let $A \geq B$ and $B \geq C$,

      where

      - $A = (a,b)$
      - $B = (c,d)$
      - $C = (e,f)$

      1. $a \geq' c$ and $c \geq' e$, both by definition of the dominates relationship. $\geq'$ is a partial order, so $a \geq' e$
      2. $d \subseteq b$ and $f \subseteq d$, both by definition of the dominates relationship. $\subseteq$ is a partial order, so $f \subseteq b$

      1 and 2 together give $A \geq C$

   Antisymmetric: Assume, by way of contradiction, that $A \geq B$ and $B \geq A$, but $A != B$,
      where

      - $A = (a,b)$
      - $B = (c,d)$

   1. $a \geq' c$, but also $c \geq' a$. Thus, $a == c$.
   2. $d \subseteq b$, but also $b \subseteq d$. Thus, $d == b$.

   1 and 2 demand $A == B$, contradicting $A!=B$, therefore $\geq$ is antisymmetric.

3. Show that dominates is not a total order.

   Let $A = (1, \{a,b\})$ and $B = (1, \{b,c\})$

{a,b} is not a subset of {b,c}, nor is {b,c} a subset of {a,b}: A and B cannot be ordered.

4. What would have to be true for two labels to dominate each other?

   They would have to be the same label -- a partial order is anti-symmetric

5. State informally what the Simple Security property says.

   A subject has read access to an object if it has a security level above the object and it deals with all categories associated with the object.

6. Explain why it’s “only if” and not “if and only if.”

   The subject clearance dominating the object sensitivity is merely necessary, not sufficient in all cases to grant access.

Lecture 9

1. Why isn’t Simple Security enough to ensure confidentiality?

   Authorised readers can write to any document.

2. Why do we need constraints on write access?

   An authorised user could down-grade the contents of a document by reading them at his clearance level and then writing them to a document below his clearance.

3. What is it about computers, as opposed to human beings, that makes that particularly important?

   Subjects in a computer system may be computer programs acting on behalf of a human, but with unknown levels of trustworthiness.

4. State informally what the *-Property says.

   A user with clearance C can only write to documents at or above his clearance.

5. What must be true for a subject to have both read and write access to an object?

   His clearance label must be equivalent to the sensitivity label of the object.

6. How could we deal with the problem that the General (top secret) can’t send orders to the private (Unclassified)?

   We can declassify the order or create a new document with a sensitivity level appropriate to the private.

7. Isn’t it a problem that a corporal can overwrite the war plan? Suggest how we might deal with that.

   It is a problem, but it's a problem of integrity rather than confidentiality. We could deal with it by having ownership of documents -- then the corporal can't overwrite the war plan because it isn't owned by him.

Lecture 10

1. Evaluate changing a subject’s level (up or down) in light of weak tranquility.

   I assume there is a memory for a subject such that they can carry some bits of information with them between levels when they are upgraded or downgraded. For confidentiality, there is no harm in upgrading a person's label -- they can access more information, but the bits they carry over are still accessible to them anyway. Downgrading on the otherhand would allow the subject to carry privelged information to a lower level and potentially write out privileged information to documents of a lower classification.

2. Why not just use strong tranquility all the time?

   Strong tranquility would be difficult to work with in an actual system. As discussed in lecture 4, question 4, there are many reasons for a subject's authorization to change, but some of these could retain the spirit of the security meta-policy.

3. Explain why lowering the level of an object may be dangerous.

   It could expose confidential information.

4. Explain what conditions must hold for a downgrade (lowering object level) to be secure.

   A human with respect for the confidentiality of the document has to review the contents and possibly make redactions prior to downgrading. The reviewer is a trusted subject.

Lecture 11

1. Suppose you wanted to build a (library) system in which all subjects had read access to all files, but write access to none of them. What levels could you give to subjects and objects?

   All subjects would have the same level.

2. Why wouldn’t you usually build an access control matrix for a BLP system?

   Access permissions can be computed using simple security and the star property on the fly.

Lecture 12

1. Suppose you had hierarchical levels L, H with L < H , but only had one category A. Draw the lattice. (Use your keyboard and editor to draw it; it doesn’t have to be fancy.)

Transitive labels are ommitted

```
(L, {}) --> (H, {}) --> (H, {A})
   |                      ^
   |                      |
   +-->(L, {A})-----------+
```

2. Given any two labels in a BLP system, what is the algorithm for finding their LUB and GLB?

   LUB:

   Let the two labels be called A and B.

   1. Enumerate the items that dominate A.
   2. Enumerate the items that dominate B.
   3. Iterate over the labels dominating A from least to greatest, stopping on the first label that is also among the labels dominating B. This label is the least upper bound of A and B.

   GLB:

   Let the two labels be called A and B.

   1. Enumerate the items dominated by A.
   2. Enumerate the items dominated by B.
   3. Iterate over the labels which A dominates from greatest to least, stopping on the first label that is also among the labels dominating B. This label is the greatest lower bound of A and B.

3. Explain why upward flow in the lattice really is the metapolicy for BLP.

   Upward flow is a description of the direction in which information moves among the lattice of labels. In a BLP system, the flow is only from lower labels to higher, indicating that *legal* information flow goes to more privileged subjects from less.

Lecture 13

1. Explain how the BLP rules are supposed to enforce the metapolicy in the example on slide 1.

   A read moves information to the reader and a write from the writer. Simple security says that a reader can move information from L to H (or L to L, or H to H), but not from L to H. Likewise, the *-property says a writer can move information from L to H (or L to L, or H to H), but not in the reverse direction.

2. Argue that the READ and WRITE operations given satisfy BLP.

   A READ only returns the explicit information of the object when S dominates O. A WRITE only executes when O dominates S.

3. Argue that the CREATE and DESTROY operations given satisfy BLP.

   A CREATE is like a write which writes an object at the level of the subject. Dominates is a reflexive relation, so the 'write' should succeed. A DESTROY is like also like a write. The destroy only succeeds if O dominates S, satisfying the *-property.

4. What has to be true for the covert channel on slide 5 to work?

   The namespace of objects has to be shared between H and L security levels.

5. Why is the DESTROY statement there?

   So we can put these one-bit send programs in sequence to send arbitrary messages.

6. Are the contents of any files different in the two paths?

   The file named F0 has a 0 in the first and a 1 at the end by the end of the program.

7. Why does SL do the same thing in both cases? Must it?

   It does the same thing because it's passively receiving bits. If SL knew which behaved differently at different times it would either be irrational or predicting the bits ahead of time and then would have no need of SH's transmissions.

8. Why does SH do different things? Must it?

   It's sending bits. I suppose SH could send all ones or all zeroes, but regardless of the code it would need to send something in the same channel or outside to communicate any more than one bit of information.

9. Justify the statement on slide 7 that begins: “If SL ever sees...”

   Any variation can be encoded as one or more bits. The key is that the bits depend on SH's actions -- they are *determined* by those actions, and not random.

Lecture 14

1. Explain why “two human users talking over coffee is not a covert channel.”

   Their communication isn't within the system.

2. Is the following a covert channel? Why or why not?

```
Send 0           | Send 1
-------------------------------------
Write (SH, F0, 0) | Write (SH, F0, 1)
Read (SL, F0)     | Read (SL, F0)
```

```
Presumably, the read by SL returns fail in either case. This would not be a covert channel because the same bit is returned every time.
```

3. Where does the bit of information transmitted “reside” in Covert Channel #1?

   The resource status.

4. In Covert Channel #2?

   The delay between subsequent scheduling times for q.

5. In Covert Channel #3?

   The disk head location.

6. In Covert Channel #4?

   The evenness of h.

7. Why might a termination channel have low bandwidth?

   To distinguish between non-termination and noise in the system requires a wait time that is significantly longer than fluctuations in run-time. These fluctuations can be on the order of milliseconds.

8. What would have to be true to implement a power channel?

   There would have to be some way of identifying power consumption within the system by an un-authorised process.

9. For what sort of devices might power channels arise?

   Mobile devices with constrained power usage.

Lecture 15

1. Explain why covert channels, while appearing to have such a low band-width, can potentially be very serious threats.

   Assuming low bandwidth is on the order of the one described in 13, allowing even 1s for the whole process that's still fast enough to send 3600 bits in an hour in a tight loop. That's a huge amount of information given appropriate context.

2. Why would it be infeasible to eliminate every potential covert channel?

   There could be thousands of them in a modern operating system.

3. If detected, how could one respond appropriately to a covert channel?

   Monitor, eliminate, or corrupt it.

4. Describe a scenario in which a covert storage channel exists.

   There are two labels in a system, H and L, with H < L. There are also two subjects in the system with labels H and L called h and l. All users can get the count of objects in the system with their same level with a COUNT operation. READ, WRITE, CREATE, DESTROY are the same as in lecture 13.

   Covert Channel:

   Transmit 0

   - l COUNTs
   - h CREATEs F0
   - l CREATEs F0
   - l COUNTs
   - h DESTROYs F0
   - l DESTROYs F0

   Transmit 1

   - l COUNTs
   - h does nothing
   - l CREATEs F0
   - l COUNTs
   - h does nothing
   - l DESTROYs F0

5. Describe how this covert storage channel can be utilized by the sender and receiver.

   To begin, l reads the file count. A transmission sequence happens. If the second count l reads has remained the same, then l registers an 0. Otherwise, the count will increase on the second count and l registers a 1.

Lecture 16

1. Why wouldn't the "create" operation have an R in the SRMM for the "file existence" attribute?

   The creator doesn't get any information about *prior* file existence from creating the file.

2. Why does an R and M in the same row of an SRMM table indicate a potential channel?

   Because the receiver and modifier subjects could be distinct and have labels that indicate they shouldn't be able to communicate.

3. If an R and M are in the same column of an SRMM table, does this also indicate a potential covert channel? Why or why not?

   No. The y axis in the table indicates the shared attribute. Unless the attributes interact in someway not encoded in the table, there is no threat of a covert channel here.

4. Why would anyone want to go through the trouble to create an SRMM table?

   Properly constructed, it eliminates interactions in the system which must be checked for covert channels.