CS 491/591 Computer Security and Privacy

Reading Assignments

Reading assignments are due by the beginning of class on the due date, *i.e.*, 1:00pm sharp based on the timestamp in my gmail account. As Shakespeare said, "Brevity is the soul of wit." Your answers should be as short as possible. I'll have a couple of dozen of these to grade so the more succinct you are, the happier I'll be. Your answers should be in the body of the email. I will not grade anything that I have to open an attachment for. The grade will be out of 5 points and will reflect how your knowledge of the reading material and thoughtfulness about it are reflected in your answers.

Typically, one to three sentences for each question will be good. For the "say something insightful" questions, one sentence is fine, and two sentences is the max. You may exceed this maximum if your insight is very compelling. An insight can be an opinion, a question, a research idea, or anything so long as it primarily comes from you and is not just a regurgitation of something you read in the chapter(s). It should be related to the material you read. The same is true in general for your answers to all questions, your answer should relate to the reading material in some way even if the question does not do so directly itself.

Gray Hat book Ch. 1 and 2

Due Friday, 22 January.

1. Why do you suppose I teach attack techniques in this class?

2. Give one example of something you can imagine yourself doing (a prank that involves a little hacking, a workaround to get around unnecessary network restrictions, *etc.*) that you think would be no big deal but could be misconstrued as illegal using the laws described in chapter 2.

3. Say something insightful.

Gray Hat book Ch. 3

Due Monday, 25 January.

1. Is it ever ethical for a researcher to release the details of a vulnerability before the vendor has had a chance to develop and distribute a patch?

2. Say something insightful.

Gray Hat book Ch. 7

Due Wednesday, 27 January.

You might consider browsing chapter 6, too, depending on your programming background.

1. In his seminal paper on computer viruses, Cohen said, "information only has meaning in that it is subject to interpretation." How does this quote relate to chapter 7?

2. Say something insightful.

Gray Hat book Ch. 8

Due Friday, 29 January.

1. Revisit your chapter 7 answer about "information only has meaning in that it is subject to interpretation" in the context of format string vulnerabilities and heap overflows.

2. The table on page 193 seems to suggest that randomizing the address space and similar defenses make you invulnerable to attacks based on memory corruption. Do you think this is so?

3. Say something insightful.

Gray Hat book Ch. 9 and 10

Due Monday, 1 February.

1. Is shellcode dangerous if it's just sitting in a file on your machine?

2. Herbert Simon said, "An ant, viewed as a behaving system, is quite simple. The apparent complexity of its behavior over time is largely a reflection of the complexity of the environment in which it finds itself." What can we learn from this quote in regards to differences between Linux shellcode vs. Windows shellcode vs. Cisco IOS shellcode vs. BSD shellcode, etc.

3. Say something insightful.

Bishop Ch. 12 (13 in the brown book)

Due Wednesday, 3 February.

1. Why is a TOCTTOU vulnerability an example of the need for the principle of complete mediation?

2. Give an example of the principle of least common mechanism (can be a positive or negative example, i.e., something airports do or that they should do) that you might see at an airport that has nothing to do with computers. It can be hypothetical or something you've seen.

3. Say something insightful.

Bishop Ch. 20 (23 in the brown book)

Due Friday, 5 February.

1. Which types of vulnerabilities did the various studies (RISOS, PA, etc.) tend to all have in common?

2. Why is generalization from a few specific vulnerabilities found to a general model of that type of vulnerability so important?

3. Say something insightful.

Bishop Ch. 8 (9 in the brown book)

Due Monday, 8 February.

1. Why do you suppose asymmetric cryptography (commonly called public key cryptography) uses fancy number theory whereas symmetric crypto tends to mostly be based on simple substitutions and bitwise operations?

2. Cryptographic hashes and checksums have been in the news lately, and the ones most commonly used in practice have all been broken. What challenges do you think hashes and checksums present to cryptographers that they haven't already solved in their work on plain old symmettric encryption/decryption?

3. Say something insightful.

Bishop Ch. 10 and 28 (11 and 30 in the brown book)

Due Wednesday, 10 February.

You may skim everything about networks rather than read it carefully, i.e., from page 153 until the beginning of 10.4.3 on page 167 you can just skim the text quickly if you like.

1. What are the key important differences between a stream cipher and a block cipher?

2. Say something insightful.

Bishop Ch. 11 (12 in the brown book)

Due Friday, 12 February.

1. Lots of programs, such as WordPress, read a password and store/check the MD5 sum (a cryptographic hash) of the password which is stored on the server in plaintext. What types of threats does this leave these programs vulnerable to that they would not be vulnerable to if they did salting?

2. What type of dictionary attack are we trying to address by shadowing the password file in modern UNIX systems?

3. Say something insightful.

Bishop Ch. 1 (also 1 in the brown book)

Due Monday, 15 February.

1. Why don't we just all agree on one security policy for all situations?

2. What is the difference between a threat and a vulnerability?

3. Say something insightful.

Bishop Ch. 2 and 3 (also 2 and 3 in the brown book)

Due Wednesday, 17 February.

1. In practice, what does it really mean that finding rights leaks in the access control matrix model is undecidable in general? Why do we care?

2. Say something insightful.

Bishop Ch. 4 (also 4 in the brown book)

Due Friday, 19 February.

1. Give an example of one mandatory access control and one discretionary access control here on campus at UNM (that is specific to universities).

2. Say something insightful.

Bishop Ch. 5 and 27 (5 and 30 in the brown book)

Due Monday, 22 February.

You might also skim chapter 13, just to make sure you know what cookies are.

1. Is it possible to build a computer that faithfully implements Bell-LaPadula with no possible way to violate the policy? If not, is defining policies in this manner still useful?

2. Say something insightful.

Bishop Ch. 6 and 7 (also 6 and 7 in the brown book)

Due Wednesday, 24 February.

1. Besides being "no writes up, no reads down" as opposed to "no reads up, no writes down", how are integrity policies fundamentally different than confidentiality policies?

2. What kinds of consistency properties might the UNM records office that handles grades encode into a Clark-Wilson model?

3. Say something insightful.

Gray Hat book Ch. 16

Due Friday, 26 February.

1. If you wanted to build a software tool to mine a Windows system's access controls for rights leaks, for what possible reasons might you choose the take-grant model over the access control matrix model?

2. If you wanted to build a software tool to mine a Windows system's access controls for rights leaks, for what possible reasons might you choose the access control matrix model over the take-grant model?

3. Say something insightful.

Bishop Ch. 15 (16 in the brown book)

Due Monday, 1 March.

1. If I built Fenton's Data Mark machine, could I compile Linux for it and then all of my information flow problems (like my credit card getting stolen) would be solved? Why or why not?

2. Why are labels in information flow defined as lattices?

3. Say something insightful.

Bishop Ch. 16 (17 in the brown book)

Due Wednesday, 3 March.

1. Do you think that a solution to the confinement problem, that accounts for covert timing channels and everything, is possible in theory?

2. Say something insightful.

Bishop Ch. 14 (15 in the brown book)

Due Friday, 5 March.

1. Consider Saltzer and Schroeder's principle of complete mediation. How can access control lists lead to mistakes that cause a violation of this principle? Conversely, the same for capabilities?

2. Name something that is not normally thought of as a capability but is in fact, essentially, a capability-like access control mechanism rather than an access control list.

3. Say something insightful.

Bishop Ch. 18 (21 in the brown book)

Due Monday, 8 March.

You can skim this chapter if you like, you just need to be aware of the different criteria and some of the history.

1. Is a system that has a higher Common Criteria certification harder to hack into than one with a lower certification?

2. Why might I purchase a system with a higher Common Criteria certification and pay the extra money?

3. Say something insightful.

Gray Hat book Ch. 13 and 14

Due Monday, 19 April.

1. If you were a virus writer and wanted to hide what your virus does from someone who will be analyzing it with IDA Pro, how would you do this? (Generalizations are okay, I don't expect you to know the intricacies of x86 assembly to answer this question).

2. Say something insightful.

Gray Hat book Ch. 20 and 21

Due Wednesday, 21 April.

1. The antivirus game largely goes like this: you as the AV company release a signature and send it out to your customers, the malware author changes their malware to no longer match that signature, then you detect the new strain and analyze it to release a new signature. Focus on the "detect the new strain" part. What is the fundamental nature of this game. I.e., we know that we can use honeypots and that the attacker can evade our honeypots, but what is fundamentally going on?

2. Say something insightful.

Gray Hat book Ch. 17

Due Friday, 23 April.

1. Why does state kept by the process being fuzzed make fuzz testing more challenging?

2. Name an analogue of fuzz testing that occurs in the natural world.

3. Say something insightful.