CS361 Questions: Week 5

These questions relate to Modules 15, 16 and 17. Type your answers and submit them on Canvas.

Lecture 66

1. What is PGP?
2. What motivated Phil Zimmerman to develop it?
3. Does PGP provide effective security? What’s your evidence for that?
4. If PGP is freeware, why would anyone bother to purchase support?

Lecture 67

1. Explain the PGP authentication protocol.
2. Explain the PGP confidentiality protocol.
3. How do you get both authentication and confidentiality?

Lecture 68

1. Besides authentication and confidentiality, what other “services” does PGP provide?
2. Why is compression needed?
3. Why sign a message and then compress, rather than the other way around?
4. Explain radix-64 conversion and why it’s needed?
5. Why is PGP segmentation needed?

Lecture 69

1. What are the four kinds of keys used by PGP?
2. What special properties are needed of session keys?
3. How are session keys generated?
4. Assuming RSA is used for PGP asymmetric encryption, how are the keys generated?
5. How are the private keys protected? Why is this necessary?

Lecture 70

1. If a user has multiple private/public key pairs, how does he know which was used when he receives an encrypted message?
2. What’s on a user’s private key ring?
3. What’s on a user’s public key ring?
4. What are the steps in retrieving a private key from the key ring?
5. What is the key legitimacy field for?
6. How is a key revoked?

Lecture 71

1. Explain the difference between the consumer and producer problems. Which is more prevalent?
2. Explain syn flooding.
3. Why are the first three solutions to syn flooding not ideal?

Lecture 72

1. Why does packet filtering work very well to prevent attacks?
2. What are the differences between intrusion detection and intrusion prevention systems?
3. Explain the four different solutions mentioned to DDoS attacks.

Lecture 73

1. Explain false positive and false negatives. Which is worse?
2. Explain what “accurate” and “precise” mean in the IDS context.
3. Explain the statement: “It’s easy to build an IDS that is either accurate or precise?”
4. What is the base rate fallacy? Why is it relevant to an IDS?

**Lecture 74**

1. What did Code Red version 1 attempt to do?
2. Why was Code Red version 1 ineffective?
3. What does it mean to say that a worm is “memory resident”? What are the implications.
4. Why was Code Red version 2 much more effective than version 1?

**Lecture 75**

1. How was Code Red II related to Code Red (versions 1 and 2)?
2. Why do you suppose Code Red II incorporated its elaborate propogation scheme?
3. What did Code Red II attempt to do?
4. Comment on the implications of a large population of unpatched machines.
5. Comment on the report from Verizon cited on slide 6. What are the lessons of their study?

**Lecture 76**

1. Why is a certification regime for secure products necessary and useful?
2. Explain the components of an evaluation standard.
3. Why would crypto devices have a separate evaluation mechanism?
4. Explain the four levels of certification for crypto devices.

**Lecture 77**

1. What is the Common Criteria?
2. What’s “common” about it?
3. Why would there be any need for “National Schemes”? 
4. Explain the difference between a protection profile and a security target.

**Lecture 78**

1. Explain the overall goal of the protection profile as exemplified by the WBIS example.

2. What is the purpose of the various parts of the protection profile (as exemplified in the WBIS example)?

3. What is the purpose of the matrix on slide 7?

**Lecture 79**

1. Explain the overall goal of the security target evaluation as exemplified by the Sun Identity Manager example.

2. How do you think that a security target evaluation differs from a protection profile evaluation?

**Lecture 80**

1. What are the EALs and what are they used for?

2. Who performs the Common Criteria evaluations?

3. Speculate why the higher EALs are not necessarily mutually recognized by various countries.

4. Can vendors certify their own products? Why or why not?

5. If you’re performing a formal evaluation, why is it probably bad to reverse engineer the model from the code?

Well done!