**Name: Kasey Sandarusi**
**EID: kjs2685**
**CS Login: ksand**
**Email: kassem@ksandarusi.com**

# CS361 Questions: Week 5

## Lecture 66

**1. What is PGP?**

A system of encryption that utilizes common encryption algorithms to encrypt messages and files.

**2. What motivated Phil Zimmerman to develop it?**

His general distaste for the government, and strong fervor for privacy.

**3. Does PGP provide effective security?**

Yes

**4. If PGP is freeware, why would anyone bother to purchase support?**

Purchasing support can provide faster hotfixes and potentially shift some of the liability on the provider.

## Lecture 67

**1. Explain the PGP authentication protocol.**

Hash of the message and signs with private key. Receivers decrypts with public key and verifies the hash.

**2. Explain the PGP confidentiality protocol.**

Sender uses a random session key to encrypt the message. Session key is encrypted with recipient's public key. Receiver decrypts session key, then decrypts message.

**3. How do you get both authentication and confidentiality?**

Authentication with the signing of sender's private key for the hash. Confidentiality by encrypting session key with receiver's public key.

## Lecture 68

**1. Besides authentication and confidentiality, what other "services" does PGP provide?**

Compression, segmentation, email compatibility.

**2. Why is compression needed?**

It reduces redundancies in the plaintext.

**3. Why sign a message and then compress, rather than the other way around?**

Compression algorithms may sign files differently, signing message verifies the original contents of the message.

**4. Explain radix-64 conversion and why it's needed?**

Prevents issues with email systems 'choking' on certain bit strings.

**5. Why is PGP segmentation needed?**

Emails may be restricted to a certain length.

# Lecture 69

**1. What are the four kinds of keys used by PGP?**

Session keys, public keys, private keys, passphrase-based keys.

**2. What special properties are needed of session keys?**

Used only once for each message.

**3. How are session keys generated?**

Generated from the previous session key and two n/2-bit blocks generated based on user keystrokes and keystroke timing. The two blocks are encrypted with an encryption algorithm using the previous session key.

**4. Assuming RSA is used for PGP asymmetric encryption, how are the keys generated?**

Generate a sufficiently large odd number, test for prime. Repeat til prime is found.

**5. How are the private keys protected? Why is this necessary?**

Protected with a passphrase-key system, in order to maintain a 'key ring' of keys while achieving security. Never stores passwords, simply calculates hashes.

# 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?**

By generating an ID that is most likely unique for a given user.

**2. What's on a user's private key ring?**

His own public/private key pairs. Timestamp, key id, public key, private key, user id

**3. What's on a user's public key ring?**

Public keys of correspondents. Timestamp, key id, public key, user id.

**4. What are the steps in retrieving a private key from the key ring?**

PGP prompts user for passphrase after retrieving receivers encrypted private key from the private key-ring.

**5. What is the key legitimacy field for?**

Maintaining trust levels for various public keys.

**6. How is a key revoked?**

The owner issues a signed key revocation certificate. Recipients update their key rings.

# Lecture 71

**1. Explain the difference between the consumer and producer problems. Which is more prevalent?**

Attacker gets between client and server for consumer. Attacker overwhelms server with requests for producer. The producer problem is more prevalent.

**2. Explain syn flooding.**

Initiating a TCP handshake with a server and not completing the handshake. Causes connections to be left half open on the server.

**3. Why are the first three solutions to syn flooding not ideal?**

Can all be circumvented and only really 'buffer' attacks. Also provide a limited amount of usability.

# Lecture 72

**1. Why does packet filtering work very well to prevent attacks?**

It doesn't work very well. I'm not sure why this question is being asked. It is very hard to filter requests if they are perfectly legal.

**2. What are the differences between intrusion detection and intrusion prevention systems?**

IPS is preventative. IDS is reactive.

**3. Explain the four different solutions mentioned to DDoS attacks.**

over-provisioning the network -- basically having more firepower than the attackers. filtering attack packets -- attempting to filter illegal packets and malicious packets. Slow down processing -- slows down speed at which requests are processed, hopefully disproportionately disadvantages attackers. speak-up -- basically requesting legitimate requestors to increase packet volume as well.

# Lecture 73

**1. Explain false positive and false negatives. Which is worse?**

Purely contextual, highly-sensitive areas would prefer false positives. Low-sensitive areas would prefer less false positives (therefore more false negatives).

**2. Explain what "accurate" and "precise" mean in the IDS context.**

Accuracy -- detecting attacks. Precision -- level of false positives.

**3. Explain the statement: "It's easy to build an IDS that is either accurate or**

**precise?**

For a 100% accurate system I can prevent all actions entirely. For high precision I can let everything happen.

**4. What is the base rate fallacy? Why is it relevant to an IDS?**

Base rate fallacy explains that even though something may be a low percent, the base rate tips the probability in its favor. Even highly accurate and highly precise systems can still raise a significant amount of false positives.

# Lecture 74

**1. What did Code Red version 1 attempt to do?**

Infect machines for the first 20 days of a month, then launch a DOS attack on whitehouse.gov

**2. Why was Code Red version 1 ineffective?**

Static seed and static IP address used for whitehouse.gov

**3. What does it mean to say that a worm is "memory resident"? What are the**

**implications.**

The worm resides in RAM and can simply be removed by rebooting. It implies the worm is short lived in a system.

**4. Why was Code Red version 2 much more effective than version 1?**

It used a random seed.

# Lecture 75

**1. How was Code Red II related to Code Red (versions 1 and 2)?**

It exploited the same vulnerability and had a related name.

**2. Why do you suppose Code Red II incorporated its elaborate propogation scheme?**

To infect as quickly as possible before patches, and ‘permanently’ infect a machine so a patch wouldn’t help.

**3. What did Code Red II attempt to do?**

Infect machines deeply enough that root access was gained and computer could be used as a zombie.

**4. Comment on the implications of a large population of unpatched machines.**

Stupid yet understandable. Most pieces of software don’t notify when a serious security threat has been patched so users may not see it.

**5. Comment on the report from Verizon cited on slide 6. What are the lessons of their study?**

UPDATE YOUR SYSTEMS PLEASE.

# Lecture 76

**1. Why is a certification regime for secure products necessary and useful?**

Helps standardize security requirements and gives knowledge as to what the product is secured against.

**2. Explain the components of an evaluation standard.**

1) definiting functionality defines what is required from security. 2) assures the functional requirements. 3) verifying functional requirements are met to make sure a system works as expected. 4) establishes the level of certainty a system is secure.

**3. Why would crypto devices have a separate evaluation mechanism?**

The systems are much more proprietary and must adhere to specific FIPS requirements.

**4. Explain the four levels of certification for crypto devices.**

1) use official functions for basic security to ensure basic security works. 2) create basic physical security to ensure it hasn’t been tampered with. 3) more robust version of level 2. 4) stronger version of level 3 and includes failsafe countermeasures.

# Lecture 77

**1. What is the Common Criteria?**

A standard for secure system evaluation.

**2. What's "common" about it?**

It is an international standard.

**3. Why would there be any need for "National Schemes"?**

If a country is interested providing their own secondary evaluation scheme.

**4. Explain the difference between a protection profile and a security target.**

Protection profile is a formal description of security for a class of systems. Security target is for a specific system.

# Lecture 78

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

Establish a set of security requirements for trash containers.

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

assets are what need to be protected. environmental assumptions are what are required for the system to work. threats are potential attacks. security policies are for attack prevention. security objectives are goals for attack prevention and detection. security requirements are the necessity to implement the objectives.

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

To verify that every requirement is met.

# Lecture 79

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

To verify that a product meets the requirements for a protection profile.

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

Protection profile establishes requirements for a class of systems, a security target is a specific system and its implementation.

# Lecture 80

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

Evaluation levels for certification of a system.

**2. Who performs the Common Criteria evaluations?**

Accredited organizations (NIST and NSA for example).

**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?**

No, it requires an impartial judge.

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

Looking at the code can alter the perception of the system.

**Well done!**