```
Name: Cohen Ellis
EID: cce335
CS Login: coel09
Email: coel09@yahoo.com
```

CS361 Questions: Week 5

Lecture 66

1. What is PGP?

   PGP is a cryptographic program that takes the best algorithms from popular cryptography to be useful for the average person to use for email.

2. What motivated Phil Zimmerman to develop it?

   Zimmermann had a strong distrust of the government.

3. Does PGP provide effective security?

   Yes, it has been seen as unbreakable.

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

   Many are wary of freeware and see purchased product as safer.

Lecture 67

1. Explain the PGP authentication protocol.

   The sender hashes a message and encrypts with their private key, while the receiver decrypts with their public key and makes a new hash code for the message and compares it to the decrypted message.

2. Explain the PGP confidentiality protocol.

   The sender creates a message and a session key used once and encrypts the message using the key and the receiver’s public key, while the receiver decrypts using his private key and the session key to decrypt the message.

3. How do you get both authentication and confidentiality?

   You get both by using both the authentication and confidentiality protocol.

Lecture 68

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

   Compression, Email compatibility, and segmentation and reassembly.

2. Why is compression needed?

   Compression reduces redundancy.

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

   So that the signature does not depend on the compression algorithm, and encryption after compression strengthens the encryption.

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

   This conversion maps groups of three octets into four ASCII characters and appends a CRC for data error checking. All email systems permit ASCII.

5. Why is PGP segmentation needed?

   So that all long messages are already segmented and the signature and session key appear only once.

Lecture 69

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

   Session, Public, Private, Password Encrypted.

2. What special properties are needed of session keys?

   Need to be very random and are only used once.

3. How are session keys generated?

   Using a previous key and a randomized algorithm.

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

   Randomly generates a number of fixed sufficient length and tested for primality. If not prime, pick another randomly generated number until a prime is found.

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

   Keys are encrypted using a user generated passcode. This is so the private key can be stored without being attacked.

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?

   The message has the key ID attached, which is the last 64 bits of the private key.

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

   Timestamp, key ID, encrypted private key, public key and user id.

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

   Timestamp, key ID, public key, User ID

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

   The user must present the passcode for the decryption of the key.

5. What is the key legitimacy field for?

   To ensure the trustworthiness of the key.

6. How is a key revoked?

   The user sends out a signed revocation certificate requesting users not to use the associated key anymore.

Lecture 71

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

   Producer problems are more prevalent and involve an overload of requests while attackers pretend to be the consumer and block items from the consumer.

2. Explain syn flooding.

   The attack sends a syn with a false return address leaving the connection open while the server waits for a reply.

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

They may be DoS with slower clients.

Lecture 72

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

   It can detect patterns of identifiers in the request stream and block messages in that pattern

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

   (IDS) can analyze traffic patterns and react to anomalous patterns while (IPS) attempts to prevent intrusions by more aggressively blocking attempted attacks

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

   a. *over-provisioning the network*---have too many servers to be overwhelmed (expensive and unworkable);
   b. *filtering attack packets*---somehow distinguish the attack packets from regular packets (may not be possible);
   c. *slow down processing*---disadvantages all requestors, but perhaps disproportionately disadvantages attackers;
   d. *"Speak-up" solution* (Mike Walfish)---request *additional* traffic from all requestors.

Lecture 73

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

   False negatives: a genuine attack is not detected.
   False positives: harmless behavior is mis-classified as an attack.

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

   accurate: if it detects all genuine attacks;
   precise: if it never reports legitimate behavior as an attack.

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

   Either everything is an attack or nothing is an attack.

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

If you have an IDS in place, it must be very accurate or you'll soon turn it off because *almost all* of your alarms will be false alarms.

Lecture 74

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

   CodeRed virus began attacking machines running unpatched versions of Microsoft's IIS webserver

2. Why was Code Red version 1 ineffective?

   Because of flaws in the design, especially the static seed, CodeRed version 1 did very little damage.

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

   An infected machine can be disinfected by simply rebooting it.

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

   It uses a *random seed* in the random number generator

Lecture 75

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

   CodeRedII began to exploit the buffer-overflow vulnerability in Microsoft's IIS webservers

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

3. What did Code Red II attempt to do?

   CodeRedII generates a random IP address and then applies a mask to produce the IP address to probe. The length of the mask determines the similarity between the IP address of the infected machine and the probed machine.

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

   covering 500 forensic investigations, involving 230 million compromised customer records, found that nine out of 10 breaches attributed to hacking attacks took advantage of a vulnerability for which a fix was available at least six months prior to the attack.

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

DoS attacks have serious financial and social consequences ($2.6 Billion according to one estimate). A known vulnerability may be exploited very quickly. Attackers adapt quickly. Unpatched machines remain vulnerable. An infected machine becomes a potential weapon.

Lecture 76

1. Why is a certification regime for secure products necessary and useful?
2. Explain the components of an evaluation standard.

   - A set of requirements defining security functionality.
   - A set of assurance requirements needed for establishing the functional requirements.
   - A methodology for determining that the functional requirements are met.
   - A measure of the evaluation result indicating the trustworthiness of the evaluated system.

3. Why would crypto devices have a separate evaluation mechanism?
4. Explain the four levels of certification for crypto devices.

Level 1: The lowest level of security. Basic security requirements, including use of at least one Approved algorithm or Approved security function. No specific physical security mechanisms required.

Level 2: Improves physical security mechanisms by requiring features that show evidence of tampering, including tamper-evident coatings or seals that must be broken to attain physical access to the plaintext cryptographic keys and critical security parameters (CSPs) within the module, or pick-resistant locks on covers or doors to protect against unauthorized physical access.

Level 3: Attempts to deter an intruder gaining access to data. Physical security mechanisms are intended to have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module. E.g., strong enclosures and tamper detection/response circuitry that zeroizes all plaintext data when the removable covers/doors of the cryptographic module are opened.

Level 4: Physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate zeroization of all plaintext CSPs.

Lecture 77

1. What is the Common Criteria?

- the CC documents,
- the CC Evaluation Methodology (CEM),
- country-specific evaluation methodologies called an *Evaluation Scheme* or *National Scheme*.

Evaluations (to a certain level) by one signing country are respected by all of the other

2. What's "common" about it?

   Over 15 countries have agreed to adopt common evaluation criteria

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

   Evaluations (to a certain level) by one signing country are respected by all of the others.

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

Protection profiles are a set of implementation-independent security requirements for a category of products or systems, a security target is specifically what the profiles protect.

Lecture 78

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

- OT.Inv1: detect invalid ID tags
- OT.Inv2: detect invalid bin-cleared messages
- OT.Safe: fault tolerance

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

- Data authentication (FDP_DAU.1)
- Internal transfer integrity protection (FDP_ITT.1)
- Stored data integrity (FDP_SDI.1)

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

There is a mapping from Threats to Assumptions/policies/security objectives.

Lecture 79

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

- O.ManagedData: store properties of users
- O.PasswordGen: support automatic generation of passwords
- O.PasswordQual: specify password quality parameters
- OE.Time: the underlying OS provides reliable time
- ON.NoUntrusted: the administrator assures no untrusted users or software on the host

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

The Security Target is more thorough and detailed while protection profiles are a more general set of objectives.

Lecture 80

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

There are the seven defined levels of assurance.

2. Who performs the Common Criteria evaluations?

NIST is responsible for managing this process in the U.S. Independent labs test up to EAL4.

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

   This depends on the amount of trust from other countries.

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

   Product vendors cannot self-certify; evaluation tests must be performed by an independent organization accredited to perform CC testing.

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

   This is because it is generally expensive to create this code and very hard to attain.