Freda Anderson fa3365

# CS361 Questions: Week 5

## Lecture 66

1. What is PGP?
    a. "Pretty Good Privacy" – a strong encryption to everyone, in the form of an email encryption system that is extremely strong, using state of the art cryptographic algorithms and easy to use and accessible to all.
2. What motivated Phil Zimmerman to develop it?
    a. Zimmerman had a strong distrust of the government and believed strongly that everyone had an absolute right to privacy.
3. Does PGP provide effective security?
    a. Yes, it is not 100% fool-proof, but it is difficult to decrypt.
4. If PGP is freeware, why would anyone bother to purchase support?
    a. Companies many want to purchase it through another professional entity for tech support and confidence in the product.

## Lecture 67

1. Explain the PGP authentication protocol.
    a. The sender creates a message M and generates a hash of M. Sender signs the hash using his private key and prepends the result to the message. Receiver uses the sender's public key to verify the signature and recover the hash code. Receiver generates a new hash code for M and compares it with the decrypt hash code.
2. Explain the PGP confidentiality protocol.
    a. The sender generates a message M and a random session key K. M is encrypted using key K. K is encrypted using the recipient's public key, and prepended to the message. The receiver uses his private key to recover the session key. The session key is used to decrypt the message.
3. How do you get both authentication and confidentiality?
    a. You apply authentication and then confidentiality to the message.

## Lecture 68

1. Besides authentication and confidentiality, what other "services" does PGP provide?
    a. Compression, email compatibility, and segmentation
2. Why is compression needed?
    a. Compression creates less traffic and lower bandwidth online
3. Why sign a message and then compress, rather than the other way around?
    a. Sign an uncompressed message so that the signature does not depend on the compression algorithm
    b. Versions of the compression algorithm behave slightly differently, though all versions are interoperable.
    c. Encryption after compression strengthens the encryption, since compression reduces redundancy in the message.
4. Explain radix-64 conversion and why it's needed?

    a. Encrypted texts contain 8 bit octets – many email systems would choke on these. Radix-64 conversion maps groups of three octets into 4 ASCII characters.
5. Why is PGP segmentation needed?
    a. Email systems often restrict message length.

# Lecture 69

1. What are the four kinds of keys used by PGP?
    a. Session keys
    b. Public keys
    c. Private keys
    d. Passphrase Based Keys
2. What special properties are needed of session keys?
    a. Session keys are used once and generated for each new message
3. How are session keys generated?
    a. The encryption algorithm E is used to generate a new n bit key from a previous session key and two n/2 bit blocks generated based on user keystrokes, including keystroke timing. The two blocks are encrypted using E and the previous key, and combined to form the new key.
4. Assuming RSA is used for PGP asymmetric encryption, how are the keys generated?
    a. A number is randomly generated and tested to see if it is a prime number. If it is a prime number, keep – else try again.
5. How are the private keys protected? Why is this necessary?
    a. They are encrypted with a supplied use passphrase. This is to protect data on the disk.

# 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?
    a. Generate an ID likely to be unique for a given user. Use the least significant 64-bits of the key as the ID.
2. What's on a user's private key ring?
    a. Timestamp/Key ID/Public Key/Private Key/User ID
3. What's on a user's public key ring?
    a. Timestamp/Key ID/Public Key/User ID
4. What are the steps in retrieving a private key from the key ring?
    a.
5. What is the key legitimacy field for?
    a. Used for trustworthiness
6. How is a key revoked?
    a. A compromise is suspected or to limit the period of the use of the key

# Lecture 71

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

    a. Consumer Problem – (man in the middle) – blocks the clients from sending things to the server
    b. Producer Problem – a server is overwhelmed by tons of bad traffic – This is more prevalent
2. Explain syn flooding.
    a. A SYN Flooding attack happens when an attacker forges the return address on a number of SYN packets. The server allocates space in its queue for half-open connections and sends the SYN/ACK packets. Because the return address has been faked, the receiver may be unavailable or unable to ACK. The server's queue is quickly filled by these half-open connections.
3. Why are the first three solutions to syn flooding not ideal?
    a. Add more space- just add more room for the attack
    b. Decrease TimeOut Table – DoS attack, slow clients are disadvantaged
    c. Filter Suspicious packets – hard to do

# Lecture 72

1. Why does packet filtering work very well to prevent attacks?
    a. It detects 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?
    a. Intrusion detection system can analyze traffic patterns and react to anomalous patterns. However, often there is nothing apparently wrong but the volume of requests. An IDS reacts after the attack has begun.
    b. An intrusion prevention system attempts to prevent intrusions by more aggressively blocking attempted attacks. This assumes that the attacking traffic can be identified.
3. Explain the four different solutions mentioned to DDoS attacks.
    a. Over-provisioning the network
    b. Filtering attack packets
    c. Slow down processing
    d. "Speak Up" Solution

# Lecture 73

1. Explain false positive and false negatives. Which is worse?
    a. It depends.
2. Explain what "accurate" and "precise" mean in the IDS context.
    a. Accurate – if it detects all genuine attacks
    b. 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?
    a. Accurate – flag everything as bad
    b. Precise – flag nothing as bad
4. What is the base rate fallacy? Why is it relevant to an IDS?
    a. There is generally a lot of traffic with a small portion as malicious. This means that it is going to get a lot of false positives.

# Lecture 74

1. What did Code Red version 1 attempt to do?
    a. If the data was between 1st and 19st – it would generate a random list of IP addresses and attempt to infect those machines. If it was between 20-28th, it would attack the White House.
2. Why was Code Red version 1 ineffective?
    a. Every instance of the worm generated the same IP addresses.
    b. They changed the IP address of the White House.
3. What does it mean to say that a worm is "memory resident"? What are the implications?
    a. It resides in the volatile memory of the machine (just needed to reboot).
4. Why was Code Red version 2 much more effective than version 1?
    a. It corrected some of the flaws like a true random generator. Some of the IP addresses where routers, modems….ect, it wrecked havoc on the internet.

# Lecture 75

1. How was Code Red II related to Code Red (versions 1 and 2)?
    a. The writer used the string "Code Red" in the code. It installed a backdoor in the machines it infected.
2. Why do you suppose Code Red II incorporated its elaborate propogation scheme?
    a. So that it was more likely to infect computers.
3. What did Code Red II attempt to do?
    a. It checks if the machine is already infected. Sometimes it generates a random IP address, other times it uses part of the IP address to infect other machines on the subnet. It installs a backdoor into the machine.
4. Comment on the implications of a large population of unpatched machines.
    a. The virus can still circulate.
5. Comment on the report from Verizon cited on slide 6. What are the lessons of their study?
    a. People don't patch their machines.

# Lecture 76

1. Why is a certification regime for secure products necessary and useful?
    a. It allows companies to not be expert in security and still buy a good security product.
2. Explain the components of an evaluation standard.
    a. A set of requirements defining security functionality
    b. A set of assurance requirements needed for establishing the functional requirements
    c. A methodology for determining that the functional requirements are met.
    d. A measure of the evaluation result indicating the trustworthiness of the evaluated system.
3. Why would crypto devices have a separate evaluation mechanism?
    a. Because there are fewer experts in the field.

4. Explain the four levels of certification for crypto devices.
    a. FIPS 140-1 – lowest level of security
    b. FIPS 140-2 – Improves physical security
    c. FIPS 140-3 – Attempts to deter an intruder gaining access to data
    d. FIPS 140-4 – Physical security mechanism provide a complete envelope of protection around the cryptographic module

# Lecture 77

1. What is the Common Criteria?
    a. The CC document, the CC Evaluation Methodology and country specific evaluation methodologies evaluation criteria for security.
2. What's "common" about it?
    a. It is world-wide (over 15 countries).
3. Why would there be any need for "National Schemes"?
    a. Country specific schemes in the Common Criteria
4. Explain the difference between a protection profile and a security target.
    a. Security target = metapolicy
    b. Protection profile = policy

# Lecture 78

1. Explain the overall goal of the protection profile as exemplified by the WBIS example.
    a. Want to protect, record, and keep track of the trash data and ID.
2. What is the purpose of the various parts of the protection profile (as exemplified in the WBIS example)?
    a. To charge the customer the correct amount.
3. What is the purpose of the matrix on slide 7?
    a. To show that all known threats are taken care of by a security object or requirement.

# Lecture 79

1. Explain the overall goal of the security target evaluation as exemplified by the Sun Identity Manager example.
    a. No unauthorized users on the system.
2. How do you think that a security target evaluation differs from a protection profile evaluation?
    a. Security target is more like the metapolicy and protection profile is more like a policy.

# Lecture 80

1. What are the EALs and what are they used for?
    a. EALs are defined levels of assurance. They are used to prove certain levels of security.
2. Who performs the Common Criteria evaluations?

    a. Government or companies certified by the government
3. Speculate why the higher EALs are not necessarily mutually recognized by various countries.
    a. If you are above EAL4, other countries won't recognize it. This might be due to the National Schemes that are specific to other countries.
4. Can vendors certify their own products? Why or why not?
    a. No, because they want a third eye to verify that the company did what they said they did.
5. If you're performing a formal evaluation, why is it probably bad to reverse engineer the model from the code?
    a. You want the module to reflect what the security policy might be, not what the code is.