Name: Tyler Kemme
UTEID: tpk266
CS ID: tpkemme

CS361 Questions: Week 5
Lecture 66
1. What is PGP?
"Pretty Good Privacy", a collection of cryptographic algorithms used for encrypting email traffic.

2. What motivated Phil Zimmerman to develop it?
Phil Zimmerman was motivated by a distrust for the government and a belief that the public had the right to privacy through strong cryptographic algorithms

3. Does PGP provide effective security?
PGP is strong enough that the American government was not able to crack the encryption system

4. If PGP is freeware, why would anyone bother to purchase support?
People that purchase support don't have the time or technical skill to maintain PGP code.

Lecture 67
1. Explain the PGP authentication protocol.
The sender signs a message hash with a private key and the receiver uses the sender's public key to get the message hash and compares it to the hash the receiver created.

2. Explain the PGP confidentiality protocol.
The sender generates a message with a session key. The sender then encrypts the message with the session key and encrypts the session key with the receiver's public key. The receiver uses his/her private key to get the session key and uses that to decrypt the message.

3. How do you get both authentication and confidentiality?
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

2. Why is compression needed?
Compression is done to save bandwidth by making a message smaller using a compression algorithm.

3. Why sign a message and then compress, rather than the other way around?
Because then the signature would depend on the encryption algorithm's result from encrypting the message.

4. Explain radix-64 conversion and why it's needed?
A radix-64 conversion takes 3 bytes into 4 bytes so that every binary string is an ASCII

character.

5. Why is PGP segmentation needed?
Segmentation breaks messages into segments so that large messages do not take too much bandwidth.

Lecture 69
1. What are the four kinds of keys used by PGP?
The four types of keys used by PGP are session keys, public keys, private keys, and passphrase-based keys

2. What special properties are needed of session keys?
Session keys need to be specifically-sized random messages. They need to be random so an attacker cannot guess them.

3. How are session keys generated?
Session keys are generated by creating a new session key from the previous session key and then encrypting that block with two blocks based off of user keystrokes.

4. Assuming RSA is used for PGP asymmetric encryption, how are the keys generated?
For RSA keys, a large odd number is generated and checked to see if it is prime. If it is not prime, a new number is generated and it is tested. When a prime number is found, it is used as the key.

5. How are the private keys protected? Why is this necessary?
Private keys are kept private by passphrase supplied by the user who wants access to the key.

CS361 Questions: Week 5.2
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 user needs to know what unique ID is associated with each key pair.

2. What's on a user's private key ring?
The private key ring contains a timestamp of when the key pair was made, the key id, the public and private key, and the user id.

3. What's on a user's public key ring?
The public key ring contains a timestamp of when the key was made, the key id, the public key, and the user id for the owner of the publc key.

4. What are the steps in retrieving a private key from the key ring?
To access the private key, the user needs to select a passphrase and supply it to the system.

5. What is the key legitimacy field for?
The key legitimacy field shows how much the PGP system trusts that the public key is actually for the specified user.

6. How is a key revoked?

A key is revoked using a signed key revocation certificate which should cause receivers to update their public key ring.

Lecture 71

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

The consumer problem is when the attacker gets between the consumer and the service causing a disruption in availability. The producer problem is when an attacker causes so much traffic or so many requests for services that the server crashes.

2. Explain syn flooding.

Syn flooding involves forging the return address for packets that set the synchonize flag. This allocates space in an internal table for a new connection. The connection is left half open until the server receives as ACK (acknowledgement) packet from the fake return address. This causes a large number of half open connections.

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

They are not ideal because they all involve drawbacks that either affect customer usability or cause an increase in resources used by the server.

Lecture 72

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

It works very well to prevent attacks because it is very strict and only allow certain IP address to send packets to the user.

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

Intrusion prevention systems prevent threats from infecting the system. Intrusion detection software is for discovering when attacks have already begun.

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

over-provisioning the network: have so many servers that losing a couple will not affect overall performance. (expensive)

filtering attack packets: filter out the attack packets from the regular ones. (probably impossible)

slow down processing: make throughput slower for everyone. Inconvenience for attackers and customers.

Speak-up solution: request additional traffic from all requesters.

Lecture 73

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

A false positive is when an IDS says an attack has occurred but it hasn't. A false negative is when an attack has occurred but the IDS did not detect it.

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

accurate: the ability to detect all attacks

precision: the ability to never report false positives.

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

Either an IDS is very strict and considers almost everything an intrusion, or it never produces false positives but possibly produces false negatives.

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

The base-rate fallacy essentially says that an IDS must be accurate or almost all connections will be classified as attacks.

Lecture 74CS361 Questions: Week 5.3

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

Code Red version 1 propagated a virus that attempted DoS attacks and defaced some websites.

2. Why was Code Red version 1 ineffective?

It used a static seed to generate IP addresses so each machine generated identical lists of IP addresses.

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

The worm is memory resident because if the system is rebooted then the worm is disinfected from the system.

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

Code Red 2 was more effective because it used a random seed so it created different IP addresses at each machine.

Lecture 75

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

The worm in Code Red II first determined if a host was already infected. If it was not, then it would get into the machine by creating a back door and begin the process of propagating througout the network.

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

3. What did Code Red II attempt to do?

Code Red II setup a backdoor for root access to the infected machine so that it could be used as a zombie in a future attack.

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

Large populations of unpatched machines can cause viruses/worms to propagate extremely rapidly.

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

Even though patches exist, users usually are attacked because they have not installed the patch. The lesson is: install patches.

Lecture 76

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

They are necessary because they involve a mostly-subjective evaluation of secure products.

2. Explain the components of an evaluation standard.

The evaluation methodology has a set of functional security requirements for the secure product, assurance requirements for establishing functional requirements, a way of evaluating if the functional requirements have been met, and an indication of the trustworthiness of the system based off of the evulatiion result.

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

Cryptographic devices need a separate evaluation mechanism because their requirements change depending on the confidentiality of the information being protected.

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

Level 1: Basic security with basic approval

Level 2: security measures that show evidence of tampering

Level 3: security measures that deter an intruder from gaining unauthorized access to data.

Level 4: security measures to prevent unauthorized access to the cryptographic module.

Lecture 78CS361 Questions: Week 5.4

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

The goal of the protection profile concerning trash bags is to ensure that the few threats that exist do not cause a significant risk to the service.

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

The purpose is to figure out what threats are possible and what security requirements are need to ensure that these threats don't affect the system.

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

The purpose of the matrix is to map threats to their associated assumptions and security policies.

Lecture 79

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

The overall goal of this evaluation is to ensure that passphrases are secure assuming a trustworthy user.

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

A security target evaluation involves evaluating the effectiveness of implementing a certain sercurity policy.

Lecture 80

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

EALs are used to show how effectively the security implementation was tested.

2. Who performs the Common Criteria evaluations?

NIST

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

Different countries might not trust other counties to comment on the trustworthiness of their very sensitive data.

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

No because they would be biased.

Well done!