CS361 Questions: Week 5

Name: Daniel Ricaud

UTeid: dr25237

CSid: dr25237

Lecture 66

1. What is PGP?

   Pretty Good Privacy, a military grade encrypted email system

2. What motivated Phil Zimmerman to develop it?

   He believed everyone had the right to privacy

3. Does PGP provide effective security?

   Extremely effective

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

   Because the commercial version satisfies businesses needing vendor support

Lecture 67

1. Explain the PGP authentication protocol.

   The sender hashes whatever message M it's sending and signs it with his public key, then the receiver uses the sender's public key to decode the message, the receiver then generates a new hash for M

2. Explain the PGP confidentiality protocol.

   The sender has a message M and a random session key K that he uses to encrypt M, K is encrypted using the public key of the receiver, then the reciver uses his private key to decrypt K

3. How do you get both authentication and confidentiality?

   Apply the authentication protocol to the original message and then apply the confidentiality protocol to the resulting message.

Lecture 68

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

2. Why is compression needed?

It lowers the size of the message and strengthens the encryption.

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

   Because it is a stronger encryption to encrypt and already compressed message since compressed messages have already had all redundancy removed.

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

   It groups 8 bit strings into chunks of 4 ascii characters, this is needed because some email systems choke on single 8 bit strings interpreting them as commands

6. Why is PGP segmentation needed?

   Because many email systems restrict length.

Lecture 69

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

   Session, public, private, passphrase-based

2. What special properties are needed of session keys?

   They are associated with a single message and used only once

3. How are session keys generated?

   From the previous session key and 2 blocks generated by user keystrokes with timing taken into consideration.

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

   It randomly generates numbers until it finds a prime

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

   Using a passphrase system, because the security of the entire system depends on protecting the private keys.

Lecture 70

1. If a user has multipleprivate/publickey pairs, how does he know which was used when he receives an encrypted message?

   The least significant 64 bits of the key are used as the ID

Timestamp, Key id, public key, private key, user id

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

Timestamp, key id. Public key, user id

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

   PGP retrieves the receiver's encrypted private key from the private key ring and uses the key id field in the session key as an index. PGP then asks the user for the passphrase to recover the unencrypted private key. Finally, PGP recovers the session key and decrypts the messasge.

6. What is the key legitimacy field for?

   It indicates the extent to twhich PGP trusts that this is a valid public key for this user.

7. How is a key revoked?

   Compromise is suspected or to limit the period of use of the key.

Lecture 71

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

   Consumer involves somehow blocking access by intercepting communication, producer involves overwhelming the service so all communication comes to a standstill. I believe producer problems are worse due to botnets.

2. Explain syn flooding.

   The server runs out of resources waiting on a response from the attacker while running a protocol that requires a response.

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

   Because they heavily slow down the system.

Lecture 72

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

   Because it blocks messages that fit a certain request pattern.

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

   Detection analyzes traffic patterns to detect anomalous patterns but it only reacts once the attack has begun, intrusion tries to prevent the attack from

Over-provisioning is having so many servers an attack wouldn't even slow you down anyways, filtering attack packets is trying to somehow distinguish malevolent packets from good ones, slow down processing slows down everyone to prevent attacks including the attackers, speak up is to try and request additional traffic from all requestors.

Lecture 73

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

   False negative is when a real attack is undetected, false positive is when something harmless is considered an attack. A false negative is worse because a real attack is occurring.

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

   A system is accurate if it detects all genuine attacks, and it is precise if it never reports normal behavior as an attack.

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

   It is difficult to accomplish both but easy to accomplish one.

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

   It gives you the chances that an attack is actually genuinely detected.

Lecture 74

CS361 Questions: Week 5

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

   DoS attack whitehouse.gov

2. Why was Code Red version 1 ineffective?

   Because it used a static seed.

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

   It can be destroyed simply by refreshing the memory when you reboot.

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

   Because it used a random seed in the random number generator.

Lecture 75

It still exploited the vulnerability in Microsoft's IIS webservers

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

   So that it could permanently reside in the machine

2. What did Code Red II attempt to do?

   Set up root access backdoor for future zombie use

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

   They are machines that are waiting to be compromised.

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

   You need to update your computer, most attacks could have been prevented by having the latest patch.

Lecture 76

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

   Because most customers don't have the expertise

2. Explain the components of an evaluation standard.

   Security requirements, assurance requirements, methodology for determining that functional requirements are met, a way to quantify the trustworthines

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

   For an added level of security

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

   Level 1 contains at least one approved algorithm or function, level 2 contains improved physical security, level 3 contains strong tamper resistance and countermeasures, leve 4 contains immediate protection and zeroing of keys upon tampering.

Lecture 77

1. What is the Common Criteria?

   A common mutual recognition among countries of each others security clearances.

2. What's "common" about it?

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

   So that sensitive information is not reveled to someone who may be a spy.

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

   A protection profile is a description of a family of products in terms of threats, environmental issues and assumptions, security objectives, and requirements of the common criteria. A security target is a document that contains the security requirements of a product to be evaluated.

Lecture 78

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

   To receive accurate information from the trash bins

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

   To verify that accurate information is being stored

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

   To see in what step of the protocol certain threats could strike.

Lecture 79

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

   To assure reliable identity authentication

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

   It doesn’t really they list the same information.

Lecture 80

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

   To provide assurance as to how rigorously the product was developed and tested

The government of the country

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

   Because each separate government gives out its own EAL certification

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

   No because that would be biased it has to be a third party.

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

   Because it's been designed using formal methods.

Well done!