Name: Luis C. Lopez
EID: LL9338
CS Login: LL9338
Email: LcLg21@utexas.edu

CS361 Questions: Week 5

Lecture 66

1. What is PGP?

Is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication.

2. What motivated Phil Zimmerman to develop it?

Because he had a strong distrust of the government, and believed strongly that everyone had an absolute right to privacy.

3. Does PGP provide effective security?

Yes because it uses the best available cryptographic algorithms as building blocks.

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

A lot of companies don't like to use freeware. They want parties that are available that they can actually call on to get maintenance and stuff like that.

Lecture 67

1. Explain the PGP authentication protocol.

A sender creates a message M and generates a hash of M. Then the sender signs the hash using his private key and prepends the result to the message. The receiver uses the sender's public key to verify the signature and recover the hash code. And finally the receiver generates a new hash code for M and compares it with the decrypted hash code.

2. Explain the PGP confidentiality protocol.

The sender generates a message M and a random session key K. Then M is encrypted using key K. K is then encrypted using the recipient's public key and prepended to the message. Then the recipient uses his private key to recover the session key and that key is used to decrypt the message.

3. How do you get both authentication and confidentiality?

We first apply the authentication step to the original message and then apply the confidentiality step to the resulting message.

Lecture 68

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

The services of compression, email compatibility, and segmentation to make the system more robust and efficient.

Name: Luis C. Lopez
EID: LL9338
CS Login: LL9338
Email: LcLg21@utexas.edu

2. Why is compression needed?
It is done to save bandwidth so you want to make them as small as possible.

3. Why sign a message and then compress, rather than the other way around?
Because we don’t want the signature to depend upon the compression algorithm.

4. Explain radix-64 conversion and why it’s needed?
It takes a standard group of three octets and converts them into four ASCII characters. This is needed because it expands the message by 33%.

5. Why is PGP segmentation needed?
Because it breaks long messages into broken segments and the signature and session key appear only once.

Lecture 69

1. What are the four kinds of keys used by PGP?
Session keys, Public keys, Private keys, and Passphrase-based keys.

2. What special properties are needed of session keys?
Each session key is associated with a single message and used only once and the key size depends on the chosen algorithm E.

3. How are session keys generated?
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. 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?
By generating a very large number of the appropriate size, usually primes numbers.

5. How are the private keys protected? Why is this necessary?
The private key is protected by encrypting with a passphrase. This is necessary because the private key can only be accessed trough a passphrase so it ensures security of the system.

Lecture 70

1. If a user has multiple private/public key pairs, how does he know which was used when he received an encrypted message?
By an ID that was generated to be unique for a given user. It uses the least significant 64-bits of the key as the ID.

2. What’s on a user’s private key ring?
A table of rows that contains the timestamp, key id, public and private key, and user ID.

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

A table of rows containing the timestamp, key id, public key, and user id.

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

First, PGP retrieves receiver’s encrypted private key from the private-key ring, using the key ID filed in the session key component of the message as an index. Second, PGP prompts the user for the passphrase to recover the unencrypted private key. Third, PGP recovers the session key and decrypts the message.

5. What is the key legitimacy field for?

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

6. How is a key revoked?

By issuing a signed key revocation certificate in which recipients are expected to update their public-key rings.

Lecture 71

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

In the consumer problem, the attacker gets logically between the client and service and somehow disrupts the communication. In the producer problem, the attacker produces, offers, or requests so many services that the server is overwhelmed.

2. Explain syn flooding.

Syn flooding happens when the attacker forges the return address on a number of SYN packets. The server fills its table with half-open connections.

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

Because the attacker can have more chances to attack.

Lecture 72

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

Because 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?

An intrusion detection system can analyze traffic patterns and react to anomalous patterns. An intrusion prevention system attempts to prevent intrusions by more aggressively blocking attempted attacks.

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

Over-provisioning the network means that if we have so many servers even there is so much traffic, they will not take me down. Filtering attack packets means that somehow it can distinguish the attack packets from regular packets. Slow down processing disadvantages all requestors but perhaps disproportionally disadvantages the attackers. Speak up solution request additional traffic from all requestors.

Lecture 73

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

A false positive is when a harmless behavior is mis-classified as an attack. A false negative is when a genuine attack is not detected. It depends on the scenario to classify it as being worse.

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

Accurate is when it detects all genuine attacks. Precise is when it never reports a legitimate behavior as an attack.

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

It says that we can report as everything being attack or report nothing as an attack.

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

It is the tendency when making judgments of the probability with which an event will occur to ignore the base rate and concentrate on other information.

Lecture 74

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

It attempted to infect machines if the date was between the 1st and 19th of the month and from the 20th to the 28th of the month, it would launch a DoS flooding attack on www1.whitehouse.gov.

2. Why was Code Red version 1 ineffective?

Because the IP address for the www1.whitehouse.gove was changed so the DoS attack failed.

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

That it resides in the volatile memory of the machine so if the machine was to be rebooted, the worm would go away.

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

It was more effective than version 1 because it was due to the sheer volume of hosts infected ad probes sent to infect new hosts.

Lecture 75

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

The same attackers used Code Red as a string on the code.

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

Because the attack keeps on going with is propagation scheme.

3. What did Code Red II attempt to do?

When it first infects the host, it determines if that host has already been infected. If not, the worm initiates it propagation mechanism, sets up a backdoor into the infected machine, becomes dormant for a day, and then reboots the machine.

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

Users usually don’t patch machines so it leaves a population of vulnerable hosts.

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

The lesson is that if they know that there is a fix for a particular problem, they should take care of that as soon as possible before an attacker finds out and takes advantage of the situation.

Lecture 76

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

Because most people don’t know or don’t have expertise to perform effective security buying skills to know what is best for the machine.

2. Explain the components of an evaluation standard.

Is 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 and a measure of the evaluation result indicating the trustworthiness of the evaluated system.

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

Because cryptology is a very sensitive area and there are not many experts in that area.

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

Level 1: basic security; at least one approved algorithm or function.
Level 2: improved physical security.
Level 3: Strong tamper-resistance and countermeasures.
Level 4: complete envelope of protection including immediate zeroing of keys upon tampering.

Lecture 77

1. What is the Common Criteria?

Is a set of documents and a methodology for applying the criteria.

2. What’s “common” about it?

That a lot of the countries tend respect all of the others criteria.

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

Because each country need privacy from other countries but can still continue applying certain things about the common criteria.

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

A protection profile is a set of implementation-independent security requirements for a category of products or systems. A security target is a set of security requirements to be used as the basis for the evaluation.

Lecture 78

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

To detect invalid ID tags, detect invalid bin-cleared messages and fault tolerance.

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

To identify possible threats to security.

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

The purpose is that if we fill out the matrix with security objective or requirement designed to counter a threat and if there is arrow with an X somewhere, then we know that we thought about that all the threats having some corresponding mechanism to counter them and all of the assumptions have a mechanism within the system which validates the assumption.

Lecture 79

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

To store properties of users, support automatic generation of passwords and specify password quality parameters.

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

A security target it is typically created by the user and it provides implementation of information assurance security requirements. And protection profile is a document used as part of the certification process according to the common criteria.

Lecture 80

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

The EALs are assurance levels under the common criteria that targets a specified level of rigor.

2. Who performs the Common Criteria evaluations?

The governments from their respective countries.

Name: Luis C. Lopez
EID: LL9338
CS Login: LL9338
Email: LcLg21@utexas.edu

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

Because those EALs were not formally designed and tested as opposed to being formally tested and designed.

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

Vendors cannot certify their own products because the evaluations must be tested by an 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?

Because then the person who reverse engineer the model will have the ability to code it back again and make their own version without being certified and sell it.