Name: Jordan Graves
EID: jlg3585
CS Login: jgraves
Email: j.l.graves03@gmail.com

Lecture 66

1. What is PGP?

A collection of the strongest cryptographic algorithms put together by Phil Zimmermann for the purpose of making this form of privacy available to everyone.

2. What motivated Phil Zimmerman to develop it?

To make the best available cryptographic algorithms available to the average person.

3. Does PGP provide effective security?

Yes. It uses some of the most sophisticated encryption algorithms.

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

Yes. A lot of companies do not like to use freeware because it usually comes with less support.

Lecture 67

1. Explain the PGP authentication protocol.

A sender simply encrypts a message with his private key, then the receiver uses the sender's public key to decrypt the message. Although the message is sent in the open, (anyone could read it), you know that the message came from the sender because no one else could have signed the message with the sender's private key.

2. Explain the PGP confidentiality protocol.

A sender generates a random key (session key) and uses it to encrypt a message. The sender then encrypts the session key with the receiver's public key. When the receiver gets

the message, he decrypts the session key with his private key then uses the session key to decrypt the original message.

3. How do you get both authentication and confidentiality?

By combining both of these protocols.

Lecture 68

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

Compression, email compatibility and segmentation.

2. Why is compression needed?

To make the messages as small as possible.

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

You don’t want the signature to depend upon the compression algorithm. Encryption after compression strengthens the encryption.

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

It expands 3 bytes into 4 bytes so that they may be represented by ASCII characters. This allows for any computer in the world to handle the message since any computer can handle ASCII.

5. Why is PGP segmentation needed?

Some mailer have a limit on the size of messages they can send. PGP breaks the message up into smaller sizes that all mailers can handle.

Lecture 69

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

one-time session symmetric keys, public keys, private keys, passphrase-based symmetric keys.

2. What special properties are needed of session keys?

Each session key is associated with a message and is only used once. Key size depends on encryption algorithm. Session keys should be highly random with alot of entropy.

3. How are session keys generated?

CAST-128 is used to generate the key from a previous session key and two 64-bit blocks generated based on user keystrokes, including keystroke timing. The two 64-bit blocks are encrypted using CAST-128 and the previous key, and concatenated to form the new key.

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

An odd number *n* of sufficient size (usually >200 bits) is generated and tested for primality. If it is not prime, then repeat with another randomly generated number, until a prime is found. The prime is then used to generate a key.

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

Private keys are stored in encrypted form. Whenever the system needs to access the keys, a passphrase must be entered.

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?

An id is generated from a public key that is the last 64-bits of a public key. This id is sent along with a message. A receiver can then do a search and find the full public key.

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

The user's own key information.
64-least significant digits of public key, timestamp of when pair was generated, public and private keys, and a user id.

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

Keys of others that the user may want to communicated with.
Timestamp of when entry was made, Key id (64 least significant digits of pub key, the public key, user id (owner of key).

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

The system asks for a passphrase when it wants to access the keys. The user provides the passphrase and is then hashed and used to decrypt the public and private keys.

5. What is the key legitimacy field for?

To determine how like a key really belongs to the person it says it does.

6. How is a key revoked?

An owner issues a revocation certificate which advises that the key has been revoked and should not be used.

Lecture 71

1. Explain the difference between the consumer and producer problems. Which is more prevalent?
Consumer problem prevents consumers from reaching producer by blocking them directly. Producer problems prevents consumers from reaching producer by blocking the producer with an overwhelming amount of requests. The producer problem is more prevalent.

2. Explain syn flooding.

A rogue client/person sends several packets to the server in attempt to fill the servers open connections.

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

Increase size of table: There is a limit to how large a table can be and the attacker can just send more requests.

Reduce lifetime of connections: slower clients may time out before completing handshake.

Filter package: hard to determine if a package is legitimate or not. May through away legit traffic.

Lecture 72

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

One can prevent packets from a certain client which seems malicious. But it really does not work very well because it is hard to implement. Even addresses of the packets may be forged.

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

Intrusion detection systems looks in system to see if an attack has occurred while a prevention systems attempt to prevent attacks.

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

Overprovisioning the network: involves having so many servers that you can handle any amount of traffic.

Filter attack packets, only allow packets that are not malicious through. It is hard to deteremine which packets are actually malicious.

Slow down processing: disadvantages everyone.

Speek-up solution: If you see that you are under attack, then request everyone to send you more packets, then determine the percent of traffic increase from the clients. Bots usually are maxed out in the amount of traffic they can send.

Lecture 73

1. Explain false positive and false negatives. Which is worse?
False positive occurs when a genuine attack is not detected.
A false negative occurs when harmless behavior is mis-classified as an attack.
Which is worse depends on the scenario.

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

Precise means the system never reports legit behavior as an attack and has no false positives.

Accurate means it detects all genuine attacks and has no false negatives.

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

A fully precise system could just report nothing as an attack.
A accurate system could just report everything as an attack.
It hard to build a system which accomplishes both of these simultaneously.

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

Lecture 74
1. What did Code Red version 1 attempt to do?

Infect a bunch of machines at random and launch a DOS attack with them against the White House website.

2. Why was Code Red version 1 ineffective?

The random number generator used to generate random ip addresses used a static seed which limited the number of machines that were infected.

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

The worm resided in the volatile memory of the machine. The memory could be fluched just by rebooting the machine.

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

It had a randomly generated seed so could infect many more machines.

Lecture 75
1. How was Code Red II related to Code Red (versions 1 and 2)?

The writer of Code Red II seemed to know about Code Red 1 and 2 because the String “CodeRedII” was in the code. The virus also attempted an attack on the White House.

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

When choosing which Ip addresses, the virus could more efficiently select machines by choosing machines on the same subnet since they are likely to be running the same software. The scheme also avoided things like printers and routers.

3. What did Code Red II attempt to do?

Install a backdoor on infected machines to potentially set up a botnet.

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

The internet is much more vulnerable. Unpatched machines can more easily be used as a weapon by attackers. So, not applying patches potentially arms these attackers.

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

People should be more active about installing patches because most attacks can be avoided by simply patching machines.

Lecture 76

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

Most people don't have the expertise to identify the products that are necessary.

2. Explain the components of an evaluation standard.

A set of requirements defining security functionality - The requirement that a system must meet in order to be considered secure.

Assurance requirements, the policies on the systems.

A methodology for applying the evaluation - perhaps a formal process of how the evaluation is carried out.

A measure, or grade, of the effectiveness or integrity of the system.

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

The evaluation mechanism is dependent upon the context in which the system will be used.

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

The levels signify the strength of verified security offered by a system. The levels range from simple security system used by the average person the security systems used by larger entities such as government to protect highly classified information.

Lecture 77

1. What is the Common Criteria?

A criteria developed for security evaluation.

2. What's "common" about it?

It can be recognized across several countries.

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

Countries have different ethnical backgrounds and values so require different implementations of security.

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

A protection profile a class of products, a security target is the product which is evaluated against the protection profile.

Lecture 78

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

To prevent someone from blocking or corrupting the information from the sensor on the trash bin to the truck.

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

To set concrete rules which allow the security goals to be accomplished. The parts define the specifics of the profile.

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

To provide a visual representation of what threats have a mechanism to protect against it.

Lecture 79

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

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

Lecture 80

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

Evaluation Assurance Level - A specification of how much evidence a party puts forward that an evaluation is going to succeed.

2. Who performs the Common Criteria evaluations?

Independent labs that are certified by certain organizations.

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

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

No. This is a conflict of interest.

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

It makes the evaluation much more difficult if not impossible if all that is given is the code.