Name: Matt Hendrickson
EID: mjh2793
CS Login: mjh2793
Email: matthewjames@utexas.edu

Lecture 66
1. What is PGP?
Pretty good privacy,
2. What motivated Phil Zimmerman to develop it?
provide strong ecryption to the public for free
3. Does PGP provide effective security?
Yes
4. If PGP is freeware, why would anyone bother to purchase support?
maybe they have a special problem that a normal user doesnt have

Lecture 67
1. Explain the PGP authentication protocol.

2. Explain the PGP confidentiality protocol.

3. How do you get both authentication and confidentiality?
apply the authentication procedure to the plaintext message.
then apply the confidentiality procedure to the encrypted message

Lecture 68
1. Besides authentication and confidentiality, what other "services" does PGP provide?
compression
segmentation
email compatibility
2. Why is compression needed?
to make the algorithm more efficient
3. Why sign a message and then compress, rather than the other way around?
you dont want the compression algorithm to mess with the signature
4. Explain radix-64 conversion and why it's needed?

5. Why is PGP segmentation needed?

Lecture 69
1. What are the four kinds of keys used by PGP?
session keys

public keys
private keys
passphrase-based keys

2. What special properties are needed of session keys?

each is generated for each message

3. How are session keys generated?

the algorithm takes into account the user's keystrokes and the previous key used.

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

based on if the number is 200 or more bits and if its prime.

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

by a user generated password

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?

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

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

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

5. What is the key legitimacy field for?

6. How is a key revoked?

Lecture 71

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

The producer problem is more prevalent. The producer makes too many request for service that the provider cannot handle all that extra traffic.

2. Explain syn flooding.

An attacker sends many SYN packets to a target server. The server responds with a SYN/ACK packet and the connection remains half open until the attacker sends back an ACK packet. What happens in syn flooding is the attacker never sends back the ack packet so the connection is never closed, thus flooding the connection with bogus requests

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

They discriminate towards legitimate clients

Lecture 72

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

It can detect patterns in the incoming stream of packets but it can be hard to differentiate legitimate requests from bad ones

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

intrusion detection onvolves finding intruders as they attempt to attack or after they have attacked
intrusion prevention involves setting up a defense system to block intruders from doing malicious activity

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

overprovisioning - have too many servers and computing power so you cant be slowed down
packet filtering - sniff incoming packets to find an attacker
slowdown - disadvantages everyone but hopefully disproportionately disadvantages attackers
speak up - request more traffic from everyone. This is good only if the attackers network is maxed out.

Lecture 73

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

false negative - a genuine attack is not detected
false positive - a legit request is misclassified as an attack - This one is worse because it blocks legitimate traffic. This is more likely to happen

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

accurate - detects all attacks
precise - never reports legit behavior as an attack

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

It would be easy to build a system that is pure in either direction. You can make it report everything as an attack(accurate) or make it let everything in (precise)

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 as many random computers as possible
DoS attack on whitehouse.gov
deface webpages with "hacked by chinese"

2. Why was Code Red version 1 ineffective?

It is easily cleansed from the machines because it is memory resident.

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

you just have to reboot a machine to get rid of it.

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

it used a "random seed" instead of a "static seed" to generate the list of target IP addresses. Thus version 2 was able to spread much faster.

Lecture 75

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

It exploited the same vulnerability

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

scheme?
Made it harder to contain. If you don't know where it's going to go then its harder to prevent it from spreading
3. What did Code Red II attempt to do?
create a botnet
4. Comment on the implications of a large population of unpatched machines.
Because the virus remains dormant until it is activated those machines very well could be infected.
5. Comment on the report from Verizon cited on slide 6. What are the lessons of their study?
Always keep your machines up to date on the latest patches.

Lecture 76
1. Why is a certification regime for secure products necessary and useful?
It helps the consumer know what they should buy.
2. Explain the components of an evaluation standard.
a set of required security reqs defining functionality
set of reqs for establishing the functional reqs
methodology for determining if the functional reqs have been met
measure of trustworthiness of the system
3. Why would crypto devices have a separate evaluation mechanism?

4. Explain the four levels of certification for crypto devices.
Level 1 - basic security, at least one approved algorithm
Level 2 - improved physical security, tamper evident packaging
Level 3 - string tamper resistance and countermeasures
Level 4 - complete protection including zeroing of keys upon detection

Lecture 77
1. What is the Common Criteria?
a set of rules in evaluating secure systems. 26 countries follow these rules
2. What's "common" about it?
26 different countries follow it.
3. Why would there be any need for "National Schemes"?
Sos different countries can adapt the Common Criteria to their laws and computing specifications
4. Explain the difference between a protection profile and a security target.
protection profile - is a formal descriptions of security for a class of systems
security target - a specific system or family system

Lecture 78
1. Explain the overall goal of the protection profile as exemplified by the WBIS

example.
to keep track of each trash bins information. its important to make sure each bin has been emptied on schedule.
2. What is the purpose of the various parts of the protection profile (as exemplified in the WBIS example)?

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

Lecture 79
1. Explain the overall goal of the security target evaluation as exemplified by the Sun Identity Manager example.
manages access privileges stored in directory services
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?
Levels of certification within the common criteria
2. Who performs the Common Criteria evaluations?
It differs from nation to nation, in the U.S. its the National Institute for Standards in Technology. They certify independent labs to provide the testing.
3. Speculate why the higher EALs are not necessarily mutually recognized by various countries.
Because different countries have different standards
4. Can vendors certify their own products? Why or why not?
No, it has to be unbiased.
5. If you're performing a formal evaluation, why is it probably bad to reverse engineer the model from the code?
It wouldnt follow the formal rules?