UTEID: dpk326;
FIRSTNAME: David;
LASTNAME: KO;
CSACCOUNT: davidko;
EMAIL: davidpeterko@gmail.com;

CS361 Questions: Week 5
These questions relate to Modules 15, 16 and 17. Type your answers and submit them on Canvas by 5pm on Thursday, July 9.

Lecture 66

1. What is PGP?

   pretty good privacy

2. What motivated Phil Zimmerman to develop it?

   create a good secure mail system

3. Does PGP provide effective security?

   yes

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

   possibility to be fixed by support if anything bad happens

Lecture 67

1. Explain the PGP authentication protocol.
   1. creates message
   2. generate a hash
   3. sign the hash using his PK and prepends to the message
   4. receiver uses the public key to verify the signature and recover hash
   5. receiver generates a new hash for the message and compares it with the decrypted hash
2. Explain the PGP confidentiality protocol.
   1. sender generates message and a random session key K
   2. M is encrypted using K
   3. K is encrypted using the recivers public key and prepend to the message
   4. Receiver uses his private key to recover the session key
3. How do you get both authentication and confidentiality?

   you get authenticity on the original message, and confidentiality on the resulting message

Lecture 68

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

   it can provide compression, segmentation and email compatibility

2. Why is compression needed?

   encryption after compression is better because there is less redundancy after compression

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

the signature will be the same

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

it substitutes certain bit strings into ascii strings sot hat emails wont interpret them as commands

5. Why is PGP segmentation needed?

segmentation limits how large the email is and how big you can send. because of this you may have a large message in different sections

Lecture 69

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

session key, public, private, passphrase based key

2. What special properties are needed of session keys?

sessions keys can only be used once and each time a message is generated, a new one is sent

3. How are session keys generated?

generated by an encyrption algorithm that generates a n-bit key from prev session key and n/2-bit blocks generated based on use

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

it keeps generating an odd number of n bit until n is prime, which will be very long and large value

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

private keys are encrypted with a user password. it is done because it needs to make surethat there would be no way to guess the private key

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?

each user has an id which is unique

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

on the private key ring, it has a timestamp, key id, public and private key, and user id

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

on the public key ring there is a timestamp, key id, public key and user id, no private key

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

1. retrieve private key from PKR using the key id
2. decrypt the private key with password
3. recover session key and decrypt the message

5. What is the key legitimacy field for?

it shwos the extent to which PGP trusts that this is a valid public key for the user

6. How is a key revoked?

owner has rights and issues a key revocation certificate, 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?

consumer: the consumer gets attacked and needs to figure out howto defend

producer: the producer needs to preemptively defend

2. Explain syn flooding.

the attacker forges the return address on SYN packets.

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

a bigger queue just means thye will send more packets

a shorter time window, they will just send faster

it is hard to differentiate between suspicious IPs

Lecture 72

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

it doesnt

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

intrusion detection is being able to sense when you are penetrated by analyzing patterns, intrusion prevention attempts to prevent instrusion by blocking attacks

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

1. have many servers, out do the attack
2. fitlering attack packets
3. slow down the processing
4. request traffic from all other servers

Lecture 73

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

false negative is when something that is bad is not detected

false positive is when a attack is detected but itsnt real

a false positive is worse beause it can prevent employees and users from accessing what they need if this happens

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

accurate is when it detects all attacks

precise: is when it never reports legitimate attacks

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

you can block evertyhing, then it will block all attacks, genuine or fake.

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

base rate fallacy is based on the idea of false positives. In the intrusion detection system, there is a high chance of a false positive

Lecture 74

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

in Code REd v1, if the date is between 1-19, it generates a random list of IP addresses and attempt to infect. it tried to taake down the white house with a ddos attac

2. Why was Code Red version 1 ineffective?

it only probed the same list of ips, memory resident and static

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

the code is living in the memory, so it will clear when you restart the computer (RAM)

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

it used a random seed instead of static. meaning it could target more machines and spread faster

Lecture 75

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

it attmempted to take over a network of machines and use them as master and slave

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

it wanted to spread teh code faster and more efficient than its predeceessors.

3. What did Code Red II attempt to do?

created slave machines while it had a master and it could run as many processes as it wanted

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

if unpatched, that machine could release the same virus

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

the users that usually downlaoded the patches were hacker and wanted to find more vulnerabilities.

Lecture 76

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

it helps theuser realize what the producers and employers want

2. Explain the components of an evaluation standard.

1. requirements defining security
2. set of assurances to set functional requirements
3. checks to see what functional requirements are not met
4. measure of the evaluation result indicatinf how trusting the system is

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

more wya to break the system and break security

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

1. basic security
2. improved physical security
3. strong tamper resistance and counters
4. complete envelope of protection

Lecture 77

1. What is the Common Criteria?

1. documents
2. evaluations
3. country specific evaluation methodologies

2. What's "common" about it?

common in a sense that this method is common to evaluate secure systems

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

in case of a national break

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

protection profile: description of a family of products in terms of threats

security target: document that has 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.

make sure that all waste bins are collected and cleared

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

to be able to put in place counter measures

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

it helps us understand which threats are accounted for by which part of the profile

Lecture 79

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

it is used to create a system on which you can set a standard by which to submit for evaluation

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

security target can be more vast than the proection profile itself

Lecture 80

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

EAL is the eavluation under the common criteria that targets something specific

2. Who performs the Common Criteria evaluations?

the government

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

the methodology differs from place to palce

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

no, then vendors would always certify their own products

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

you are onyl testing scenarios for which the code was designed