Name: Scott Stephens
EID: sts768
CS Login: scott483
Email: stevo4932@gmail.com

Lecture 66

1. What is PGP?
   A strong encryption system that is extremely strong, easy to use, and accessible to all.
2. What motivated Phil Zimmerman to develop it?
   He distrusted the government and wanted a way to protect information from them.
3. Does PGP provide effective security?
   Yes the FBI and Italian police couldn't crack it.
4. If PGP is freeware, why would anyone bother to purchase support?
   A lot of companies don't like freeware since they like to have someone they can call for support.

Lecture 67

1. Explain the PGP authentication protocol.
   Create message M and generate a hash. Sign the hash using private key and perpend the result to the message. Receiver uses public key to verify signature and then creates a new hash to compare with the one received.
2. Explain the PGP confidentiality protocol.
   Sender generates M and a random session key K. M is encrypted with K. Then K is encrypted with receivers public key. Whole package is sent to receiver. Reviver is then able to use their private key to unlock K which unlocks M.
3. How do you get both authentication and confidentiality?
   Take both above pieces and use them together.

Lecture 68

1. Besides authentication and confidentiality, what other “services” does PGP provide?
   compression, Email compatibility, segmentation.
2. Why is compression needed?
   To save bandwidth.
3. Why sign a message and then compress, rather than the other way around?
   You don't want the signature to depend on the encryption algorithm.
4. Explain radix-64 conversion and why it’s needed?
   To remove the potential for the sting to be interpreted as control commands instead ACSII.
5. Why is PGP segmentation needed?
   Some mailers have limits on size and so PGP segments the message into sizes that all mailers can handle.

Lecture 69

1. What are the four kinds of keys used by PGP?
   Session Keys, Public Keys, Private Keys
2. What special properties are needed of session keys?

3. How are session keys generated?
   An encryption algorithm is used on the previous session key combined with two encrypted n/2bit blocks randomly generated.

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

Generate large number of size N and test using primality. If it's not you throw it away and try again. Probability says it will converge.

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

They are stored encrypted with a user-supplied passphrase so that an attacker does not learn the key by breaking the users personal computer.

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?

generate an ID for the pair which is unique. It's the last 64 bits of the key.

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

keep your own private key and information to recognize them. (timestamps, key id, public key, etc)

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

keys that you store with the people you communicate with. (timestamps, key id, public key, user id).

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

PGP retrieves the encrypted private key then pomps for the passphrase. If it matches it is returned.

5. What is the key legitimacy field for?

A measure of how strongly you feel the key belongs to a particular user. (error prone but necessary).

6. How is a key revoked?

Issue a signed key revocation certificate. Recipients are expected to stop use.

Lecture 71

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

The attacker gets between the client and service as opposed to the attacker requesting so many services that the server is overwhelmed.

2. Explain syn flooding.

Attacker forges the return address on a number of syn packets. The server fills it's table with these half-open connections that fill up server tables.

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

Increase table size: consumes considerable resources and attacker can just send more requests.
Shorten time out period: might disallow connections by slower clients.
Filter suspicious packets: May be hard to determine.

Lecture 72

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

It is very hard to be able to discriminate patterns of attack from patterns of standard usage.

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

Intrusion detection is about recognizing current intrusions while prevention tries to stop intrusions from occurring at all.

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

Over-Provisioning the network – have to many servers to be overwhelmed. Expensive and

unworkable.

Filtering attack packets – distinguish attack packets from regular packets (may not be possible)

Slow down processing – disadvantages all requests but more so on attackers.

Speak-up solution – requests more packets with the idea being that the bots are maxed out and can't while the legit requests can.

Lecture 73

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

False negatives are when attacks are not detected and False positives are classifying legit requests as attacks. False Negatives would be a bigger problem as harm can be done to the system where as a False positive just prevents actions. Both pretty bad though.

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

Accurate is if all genuine attacks are detected. Precise is if no legit actions are reported as attacks.

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

It's easy to go to the extremes where you report everything as an attack or nothing.

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

Frequent false alarms can lead to the system being disabled or ignored due to annoyance and uselessness. The rate of False negatives and positives is important for a useful IDS.

Lecture 74

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

Infect machines from the 1st to the 16th of the month then launch a DoS attack on whithouse.gov on the 20th to the 28th. Also defaced some pages with the words hacked by Chinese.

2. Why was Code Red version 1 ineffective?

It used a static seed so that each a few Ips were ever targeted and white house just changed their Ip address in anticipation so the DoS attack failed.

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

It resided in the volatile memory of a machine. So every reboot wiped it out.

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

corrected flaws. Randomly generated seed (spread more widely), affected other web interfaces such as routers, switchers, and printers.

Lecture 75

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

It contained the string “CodeRedII.”

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

To stay hidden from view so that it can spread easily and undetected.

3. What did Code Red II attempt to do?

Install a back door which allowed remote root-level access to be used as zombies in future attacks.

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

Large vulnerabilities allow these worms to continue to populate and circulate.

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

That we are not good about patches which causes the Internet to be less safe since there are

systems which are more susceptible to attack. It's like that one person who doesn't get vaccinated and keeps spreading the disease around.

Lecture 76

1. Why is a certification regime for secure products necessary and useful?
   Supplies assurances of the trustworthiness of a system for those who do not have the capacity to test individually.
2. Explain the components of an evaluation standard.
   Method to determine the functional requirements and if they are met. Requirement that define security functionality. A measure of the evaluation result.
3. Why would crypto devices have a separate evaluation mechanism?
   It is a sensitive area with less experts so more attention is needed.
4. Explain the four levels of certification for crypto devices.
   Level 1 -basic security; one approved algorithm.
   Level 2 – improved physical security, tamper-evident packaging.
   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?
   A set of documents and methodology for applying the criteria. Also have country specific evaluation methodologies. In general if it passes one country the other countries accept it (except at the very high levels).
2. What's "common" about it?
   If it passes one country it passes in the others (for the most part).
3. Why would there be any need for "National Schemes"?
   If there infrastructure is set up different than another or if they want to ensure a higher quality product than the standard.
4. Explain the difference between a protection profile and a security target.
   Security target is evaluation of a product (firewall). A protection profile is a document stating what your security requirement for a whole category of products will be.

Lecture 78

1. Explain the overall goal of the protection profile as exemplified by the WBIS example.
   To ensure that the correct weight was recorded and was not tampered with.
2. What is the purpose of the various parts of the protection profile (as exem-exemplified in the WBIS example)?
   To detect invalid ID Tags, Detect invalid bin-cleared messages and fault tolerance.
3. What is the purpose of the matrix on slide 7?
   If you fill it in with an object designed to met a threat and every row has an x then every threat has a way to be solved.

Lecture 79

1. Explain the overall goal of the security target evaluation as exemplified by the Sun Identity Manager example.
   To securely store and access user information.
2. How do you think that a security target evaluation differs from a protection profile evaluation?

It is more specific to what the mechanisms are for the protection as opposed to an overview of what needed to be done which may or may not include implementations.

Lecture 80

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

Evaluation levels that provide assurance that the corresponding rigor was applied during development and test.

2. Who performs the Common Criteria evaluations?

Governments of each participating country have testing labs that evaluate systems. These labs are commercial and in the U.S. they are certified by NIST.

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

Some countries may want to only produce the highest possible quality of products that go above the standard. Others may want to seem more exclusive and make it to where their rating is perceived to be more rigorous.

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

They can not since there are obvious conflicts of interest. Needs to be independent.

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

It is then possible for others to do the same which may lead to a security risk.