Brittany Kvanvig bmk447

CS361 Questions: Week 5

Lecture 66

1. What is PGP?

Pretty good Privacy: allows an average person to use strong encryption of emails

2. What motivated Phil Zimmerman to develop it?

He didn't trust the government

3. Does PGP provide effective security?

Yes, the government, mafia had great difficulty decrypting it

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

Many companies don't like to use freeware. They like to be able to call on a company for maintenance, questions etc

Lecture 67

1. Explain the PGP authentication protocol.

Hash the message, sign with sender's private key, then append to message and send the whole thing

2. Explain the PGP confidentiality protocol.

Generate new session key, encrypt message symmetrically with this key. Then encrypt key with receivers public key.

3. How do you get both authentication and confidentiality?

Combine both methods. Prepend signature to the message, then encrypted (message + signature) with session key. The session key is encrypted using receivers public key then prepended to message

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 PGP more efficient. It saves bandwidth

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

Because you don't want the signature to depend on the compression algorithm

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

It takes 3 octets and turns it into 4 ascii characters. Then everything in the message is ascii

5. Why is PGP segmentation needed?

Some mailers have limits on message length, so no mailer will reject the message.

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?

Associated with a single message and used only once

3. How are session keys generated?

The previous session key and two n/2-bit blocks generated based on user keystrokes, including keystroke timing

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

Generate a very large number, then test if it's prime. Keep doing it until you get a prime. Expensive, but used infrequently

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

They are encrypted with a passphrase-based key and stored that way. This is necessary to keep the private keys safe and therefore the entire system safe.

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?

   Keeps the pairs on a key ring based on a unique ID which is the least significant 60 bits of the public key

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

   Timestamp, key ID, public key, private key, user ID

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

   Timestamp, key ID, public key, user ID

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

   Retrieves encrypted private key, prompts user for passphrase, recovers the session key and decrypts the message

5. What is the key legitimacy field for?

   Tells if the public keys on public key ring are legitimate

6. How is a key revoked?

   If a compromise is suspected or if the public key is limited to a specific time.

Lecture 71

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

   Consumer: the attacker gets logically between the client and service and somehow disrupts the communication. Producer problem: attacker produces, offers, or requests so many services that the server is overwhelmed. Producer problem is more common.

2. Explain syn flooding.

   An attacker forges the return address on a number of SYN packets. The server fills its table with these half open connections. All the legitimate accesses are denied until the connection time-out.

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

Increasing the server’s queue size is expensive and the attacker can send more requests. Shortening time out period is an availability attack in and of itself. Filtering suspicious packets could throw away legitimate traffic.

Lecture 72

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

Because it only allows legitimate traffic.

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

Intrusion detection tries to detect an attack that has occurred and gotten past your firewall. An intrustion prevention system attempts to prevent the perimeter defence by not allowing traffic that could be malicious.

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

Over-provisioning the network: having too many servers to be overwhelmed. Filtering attack packets: somehow distinguish the attack packets from regular packets (which may be impossible). Slow down processing: disadvantages all requestors, but perhaps disproportionately disadvantages attackers. “Speak-up” solution: request additional traffic from all requestors.

Lecture 73

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

False positives attacks harmless behavior as if it’s malicious. False negatives thinks a genuine attack is harmless

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

Accurate means the IDS detects all genuine attacks. Precise means it never reports harmless behavior as an attack

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

Both are hard to do, but it’s easy to be accurate if you flag all activity, and it’s easy to be precise if you flag no activity.

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

Base rate fallacy measures how precise a system is. It tells how often a raised attack is a genuine attack.

Lecture 74

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

Hack the whitehouse website due to a published vulnerability.

2. Why was Code Red version 1 ineffective?

The pseudorandom generator used a static seed. So every instance of the worm generated the same IP addresses. So whitehouse.gov changed their IP address

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

It means the worm resides in the volatile memory of a machine so a machine can be disinfected by simply rebooting it.

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

It had a randomly generated seed which spread the worm much farther

Lecture 75

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

The code red II writer used coderedII in the code, so he knew about code red.

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

To be able to be better at being undetected

3. What did Code Red II attempt to do?

Sets up a backdoor and tries to propagate itself. This allows the computers to be zombies and run any code the attacker wants.

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

This means the worms will continue to circulate and spread because some machines are vulnerable.

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

We need to be better at patching machines if at all possible.

Lecture 76

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

To be able to assess the security of a machine without knowing anything about security

2. Explain the components of an evaluation standard.

set of requirements, set of assurance requirements needed for establishing the functional requirements, a methodology for determining that the functional requirements are met, a measurement of the evaluation result.

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

because many are used for governmental or highly confidential processes/information and they need different criteria to be met

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

Basic, improved with tamper-evident packaging, strong tamper resistance and countermeasures, and complete envelope of protection including immediate zeroing of keys upon tampering

Lecture 77

1. What is the Common Criteria?

secure systems evaluation criteria standard used by 26 countries

2. What's "common" about it?

A number of countries use the same criteria

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

so certain high levels of information isn't visible to all countries

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

Protection profile applies to a class of people (or systems) while a security target is a singular person (or system)

Lecture 78

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

   Keep track of a certain bins information and make sure it's secure so no one can change the info

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

   A.ID identifies the waste bin. A.Trusted says the crew is authorized and trustworthy. A.Access says the access to the system is protected. A.Check tells an operator to check the data at intervals to make sure the data transfers. A.Backup has the operator make backup copies of the data at intervals

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

   It shows if the ideas you're using are adequate to cover threats to your system.

Lecture 79

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

   Manage user access privileges

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

   Security target evaluation will be much more specific while the protection profile evaluation will be much more general for a wider range

Lecture 80

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

   They are evaluated assurance level. It describes how secure a system is under the common criteria

2. Who performs the Common Criteria evaluations?

The government or certifying agency

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

Because the higher EALs have more to lose if for some reason a country certifies a high EAL and it has a vulnerability. Surely dealing with such sensitive information would require additional testing.

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

No, because that 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?

Because the code could allow a vulnerability unseen by a reverse engineering.