Name: Joshua Waller
EID: jrw3839
CS Login: jrwall11
Email: jrwall11@utexas.edu

Week 5 Questions

Lecture 66

1. PGP is a cryptographic algorithm that could be used by anyone and not just the military.
2. Phil Zimmermann did not trust the government and he wanted to create an useful cryptographic algorithm to protect the common man.
3. Yes, the cryptographic algorithm is very strong and widely used among many users.
4. A lot of companies do not like to use freeware because they want someone available to help fix any problems.

Lecture 67

1. Authentication process starts by the sender creates a message M, the Sender generates a hash of M, Sender signs the hash using his private key and prepends the result to the message, Receiver uses the sender's public key to verify the signature and recover the hash code, and finally the Receiver generates a new hash code for M and compares it with the decrypted hash code.
2. For Confidentiality the Sender generates a message M and a random session key K, M is encrypted using key K, K is encrypted using the recipient's public key, and prepended to the message, Receiver uses his private key to recover the session key, and the session key is used to decrypt the message.

Name: Joshua Waller
EID: jrw3839
CS Login: jrwall11
Email: jrwall11@utexas.edu

3. To have both Authentication and Confidentiality they must apply the authentication step to the original message and apply the confidentiality step to the resulting message.

Lecture 68

1. PGP also provides compression, email compatibility, and segmentation.
2. Compression saves bandwidth over the Internet.
3. It is good to do it in that order so the signature doesn't depend on the compression algorithm.
4. Radix-64 takes three octets into for ASCII characters. Also appends a CRC for data error checking. By default, even ASCII is converted.
5. Segmentation is used because some mailers have a certain length a message can be sent. Segmentation breaks the message into segments and reassembles when they successfully send.

Lecture 69

1. PGP uses Session keys, Public keys, Private keys, and passphrase-based keys.
2. They should be high entropy and not easy to find out. To do this, they use keystrokes and keystroke timing to generate the key.
3. To do this, they use keystrokes and keystroke timing to generate the key.
4. They generate a public key and private key based of it is a prime. If the number is not prime, then anther random number is generated.

Name: Joshua Waller
EID: jrw3839
CS Login: jrwall11
Email: jrwall11@utexas.edu

5. Private keys are encrypted by a user-supplied passphrase and this prevents attackers from accessing your private key since they would not know the passphrase.

Lecture 70

1. They generate an ID likely to be unique for the given user.
2. The private-key ring has its own public/private key pairs.
3. The public-key ring ha the public keys of correspondents.
4. PGP retrieves receiver's encrypted private key from the private-key ring, using the Key ID field in the session key component of the message as index, PGP prompts the user for the passphrase to recover the unencrypted private key, and PGP recovers the session key and decrypts the message.
5. This serves to prove the authenticity that the PGP is a valid public key for this user.
6. They revoke the key based off the compromise is suspected, or to limit the period of use of the key.

Lecture 71

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

Name: Joshua Waller
EID: jrw3839
CS Login: jrwall11
Email: jrwall11@utexas.edu

2. A SYN Flooding attack happens when an attacker forges the return address on a number of SYN packets. The server fills its table with these half-open connections.
3. Increasing the server's queue size fails because typically only 8 connections are allowed; could consume considerable resources. Shorten the time-out period fails because it might disallow connections by slower clients. Filter suspicious packets fail because if the return address does not math the apparent source, discard the pack and that may be hard to determine.

Lecture 72

1. Packet filtering can help detect any suspicious activity that could cause a breach in security.
2. Intrusion detection system can analyze traffic patterns and react to anomalous patterns and begins after the attack has begun, and an intrusion prevention system attempts to prevent intrusions by more aggressively blocking attempted attacks and that is assuming that the attacking traffic can be identified.
3. DDos attack mentions over-provisioning the network, filtering attack packets, slow down processing, and "Speak-up" solution.

Lecture 73

1. False negatives are a genuine attack that is not detected and false positives are harmless behavior that is mis-classified as an attack.

Name: Joshua Waller
EID: jrw3839
CS Login: jrwall11
Email: jrwall11@utexas.edu

2. Accurate is if it detects all genuine attacks and precise is if it never reports legitimate behavior as an attack.
3. It is easy to make a IDS that is either accurate or precise by always reporting attacks or confirming a legitimate attack every time, but getting both at the same time is hard.
4. Base rate fallacy determine if attacks are rare and the information from the base rate fallacy can help determine if every alert is just a false positive.

Lecture 74

1. eEye Digital Security was a worm that uses a static seed in its random number generator and thus generates identical lists of IP addresses on each infected machine, each infected machine probed the same list of machines, so the worm spread slowly, and the IP address for the Whitehouse was changed so the DoS attack failed.
2. Rebooting or changing the IP address would allow the user to be unaffected.
3. A worm that can be disinfected by rebooting your computer.
4. This worm used a random seed generator and infected a greater amount of users and other devices causing the system to reboot or crash.

Lecture 75

1. CodeRedII used the line CodeRed in their attack, which was the only similar thing between the two.

Name: Joshua Waller
EID: jrw3839
CS Login: jrwall11
Email: jrwall11@utexas.edu

2. Using the same prefix would allow you to be on the same subnet of the machines running that software allowing infections of other machines to be easy.
3. It installs a mechanism for remote, root-level access to the infected machine. This backdoor allows any code to be executed, so the machines could be used as zombies for future attacks.
4. The large amount of unpatched machines represents that there are many machines out there vulnerable to the attack.
5. The study showed that many people are lazy and not careful when there is software to help prevent attacks from happening.

Lecture 76

1. It allows providing a certified secure system that is reliable based on the requirements it passes.
2. An evaluation standard provides the following: A set of requirements defining security functionality, a set of assurance requirements needed for establishing the functional requirements, a methodology for determining that the functional requirements are met, and a measure of the evaluation result indicating the trustworthiness of the evaluated system.
3. Cryptographic modules have different security requirements because it needs to be approved by the NSA or have been validated to FIPS 140-1 or 140-2.

Name: Joshua Waller
EID: jrw3839
CS Login: jrwall11
Email: jrwall11@utexas.edu

4. Level 1 is a basic security; at least on approved algorithm or function. Level 2 is improved physical security, tamper-evident packaging. Level 3 is a strong-tamper-resistance and countermeasures. Level 4 is complete envelope of protection including immediate zeroing of keys upon tampering.

Lecture 77

1. It comprises of the CC documents, the CC Evaluation Methodology, and country-specific evaluation methodologies called an Evaluation Scheme or National Scheme.
2. It “common” because it is used by 26 other countries.
3. A National Scheme will allow countries to accept or deny other country evaluations based on their own methodologies.
4. Protection profile is a description of a family of products in terms of threats, environmental issues and assumptions, security objectives, and requirements of the Common Criteria, and the security target is a document that contains the security requirements of a product to be evaluated, and specifies the measured offered by the product to meet those requirements and it may match a protection profile.

Lecture 78

1. WBIS is used to protect the authentication and integrity of ID tags on waste bins and trashcans.
2. The system ensures the data authentication, internal transfer integrity protection, and stored data integrity.

Name: Joshua Waller
EID: jrw3839
CS Login: jrwall11
Email: jrwall11@utexas.edu

3. The table shows the mapping from threats/assumptions to security objectives/requirements.

Lecture 79

1. The goals consisted of strong properties of users, support automatic generation of passwords, specify password quality parameters, the underlying OS provides reliable time, and the administrator assures not untrusted users or software on the host.
2. The Security Target is a specific system or class of systems submitted for evaluation, the policy may be specified "fresh" or as previously evaluated protection profiles, and the idea is to specify what security means for this product and how the product enforces that notion of security.

Lecture 80

1. EAL is the evaluation assurance level and gives the system a level ranking of assurance.
2. A vendor provides assurance that the corresponding rigor was applied during development and test.
3. Some countries have different requirements and do not require that level to be evaluated to receive the certificate.
4. No because the evaluation test must be performed by an independent organization accredited to perform CC testing.
5. Extensive documentation is required and the process is very expensive.