WEEK 4 QUESTIONS

Name: Charu Sharma
EID: cs36739
CS Login: charu
E-mail: charu.sharma@utexas.edu

LECTURE 66

1. PGP is a system that puts cryptographic algorithms and protocols together in a very neat way.
2. Phil Zimmerman wanted to make cryptography possible for the average person through a packaging of existent algorithms. Zimmerman's personal distrust of government persuaded him to create PGP, almost landing him in jail.
3. Yes, PGP is so effective that national governments cannot even decrypt PGP.
4. The commercial version is necessary so that parties are available so that they can call them for support and maintenance.

LECTURE 67

1. In the PGP authentication protocol, a sender creates a message M, and a hash of M. The sender signs this hash with his private key and prepends that result to the message. The receiver uses the sender's public key to verify the signature and recover the hash code. Then the receiver generates a new hash code for M and compares it to the decrypted hash code.
2. In the PGP confidentiality protocol, the sender generates a message M and random session key K. M is encrypted with key K, and K is encrypted using the recipient's public key and is prepended to the message. The receiver uses his private key to recover the session key. The session key is used to decrypt the message.
3. You can apply the authentication step to the original message and the confidentiality step for the resulting message.

LECTURE 68

1. PGP also offers compression, email compatibility, and segmentation.
2. Compression is needed to compress a message with a zip algorithm to save bandwidth.
3. You sign a message and then compress, because you don't want the signature to depend on the encryption algorithm used.
4. Radix-64 conversion is necessary to map groups of three octets into four ASCII characters. It appends a CRC for data error checking. By default, even ASCII is converted. It expands the message by 33% and makes sure that everything is an ASCII character.
5. PGP segmentation breaks the message into segments since email systems often restrict message lengths. It also creates mail headers.

LECTURE 69

1. The four kinds of keys used by PGP are session keys, public keys, private keys, and passphrase-based keys.
2. Session keys must have a size dependent on the chosen encryption algorithm E, and is associated with a single message and used only once. They must also be high entropy. You take the previous session key and a new key to encrypt that with. You collect entropy.
3. An encryption algorithm E generates a new n-bit key from a previous session key and two n/2 bit blocks are generated based on user keystrokes, including keystroke timing.

The two blocks are encrypted using E and the previous key, and combined to form the new key.
4. An odd number, n, of sufficient size (usually >200 bits) is generated and tested for primality. If it is not prime, repeat with another randomly generated number until a prime is found.
5. Private keys are protected with a passphrase.

LECTURE 70

1. Generate an ID *likely* to be unique for a given user.
2. The private key ring has the timestamp, key ID, public key, private key, and user ID.
3. The public key ring has the timestamp, key ID, public key, and user ID.
4. PGP retrieves the receiver's encrypted private key from the private key ring, using the key ID field in the session key component of the message as an index. PGP prompts the user for the passphrase to recover the unencrypted key. PGP recovers the session key and decrypts the message.
5. The legitimacy field indicates the extent to which PGP trusts that this is a valid public key for the user.
6. A key is revoked when the owner issues a signed key revocation certificate. Recpients update their public key rings.

LECTURE 71

1. In the consumer problem, the attacker gets logically between the client and service to disrupt the communication. In the producer problem, the attacker produces, offers or reqests so many services that the server is overwhelmed. The producer problem is more prevalent.
2. Syn flooding is an example of using a handshake protocol in which the attacker does not respond so the server ties up resources waiting for a response.
3. The first three solutions to syn flooding are not feasible because you don't want to consume considerable resources with increased queue size, disallow connections by slower clients by shortening the time-out period, or go through the difficulty of determining suspicious packets to filter them.

LECTURE 72

1. Packet filtering works well to prevent attacks, because you can sniff incoming packets and discard those with source IP addresses outside a given range.
2. An intrusion detection system analyzes traffic patterns to anomalous patterns, while an intrusion detections system tries to prevent intrusions by more aggressively blocking attempted attacks, assuming the attacking traffic can be identified.
3. Overprovisioning the network means to have too many servers be overwhelmed. Filtering attack packets means to somehow distinguish the attack packets from regular packets. Slowing down processing means disadvantaging all requestors but disproportionately slowing attackers. Speak up means requesting additional traffic from all requestors.

LECTURE 73

1. A false positive is when harmless behavior is mis classified as an attack and a false negative is when a genuine attack is not detected. A false negative would be worse.
2. Accurate means a system detects all genuine attacks, while precise means a system never reports legitimate behavior as an attack.
3. If you eliminate false negatives, you are vulnerable to false positives, and vis a versa.

4. Base rate fallacy occurs when a system is so accurate that there is a high chance of a false positive, making all raised alarms fake for an IDS.

LECTURE 74

1. Code Red version 1 attempted to infect randomized IP address machines, commit a DoS flooding attack on the white house website, and write "Hacked by Chinese" on some webpages.
2. Code Red version 1 was ineffective, because it used a static seed and the worm was memory resistant, allowing a machine to be disinfected by simply rebooting it.
3. A worm is memory resident if a machine can be disinfected simply by rebooting it.
4. Code Red version 2 was more effective, because it used a random seed in a random generator making it harder to detect.

LECTURE 78

1. Code Red II was a worm but made by different people than Code Red.
2. It would need some kind of secure access to the OS kernel in order to do this and probably had to study the machine for a while. It could open up a reboot window causing the user to reboot on his or her own, too.
3. Code Red II generated a random IP address and applied a mask to produce the addresses to probe.
4. A large population of unpatched machines were still vulnerable to the same or a similar attack.
5. More attention needs to be paid to security in order to avoid harmful virus worms. If security is taken care of ahead of time, crisis moments like Code Red II can be avoided easily.

LECTURE 76

1. A certification regime is necessary for secure products, because buying security products should involve assessing needs to determine requirements, identifying the product that will meet those requirements, and purchasing the product and deploying it.
2. The components of an evaluation standard are 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. Crypto devices have a separate evaluation mechanism, because federal agencies are required to use products that have either been approved by the NSA or validated to FIPS security requirements.
4. The four levels of certification for crypto devices are basic security, improved physical security, strong tamper-resistance, and a complete envelope of protection.

LECTURE 77

1. The Common Criteria is evaluation criteria for secure systems that has been adopted by 26 countries including the United States. It comprises of CC documents, CC Evaluation Methodology (CEM) and country specific evaluation methodologies called an Evaluation Scheme or National Scheme.
2. It is common in that it is common to 26 countries.
3. A National Scheme is necessary, because evaluations to a certain level by one signing country are respected by all of the others.

4. A protection profile is a set of implementation independent security requirements for a category of products or systems, while a security target is against a specific security target.

LECTURE 78

1. The overall goal of the protection profile is to find a way to protect from the security threats by protecting assets, in this case records that a waste bin was cleared.
2. The purpose of the protection profile is to protect records that a waste bin was cleared, or to generally protect assets from security threats by creating accountability.
3. The purpose of the matrix is to map from threats/assumptions to security objectives/requirements.

LECTURE 79

1. The overall goal of security target evaluation is to protect against threats by a specific security target and secure a specific asset.
2. Security target evaluation is more specific than a profile, because it targets specific assets rather than general assets.

LECTURE 80

1. EALs are evaluation levels under the Common Criteria that specify levels of rigor. They are important because the vendor provides assurance that the corresponding rigor was applied during development and test.
2. CC evaluations are performed by independent accredited organizations.
3. Higher EALs are not necessarily mutually recognized by various countries, because there are too high stakes if the country disagrees on vendor protocol. Higher EAL levels are necessary for more secure items that can't be taken a risk on.
4. Vendors can't certify their own products, because that is self-certification, so instead an independent organization is accredited to perform CC testing. The NIST does it for the US.
5. It is bad to reverse engineer the model from the code, because you will run into the same threats you didn't account for in the code.