Name: Olamide Fayemiwo
EID: oaf226
CSLogin: ofaye
Email: olamide.fayemiwo@live.com

Week 5

Lecture 66

1. PGP is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication.
2. Phil Zimmerman's distrust of the government motivated him to develop it because it strongly believed that everyone had an absolute right to privacy.
3. PGP provides effective security because it is difficult to decode/access the encrypted file. There is no known method which will permit a person to break a PGP encryption by cryptographic or computational means.
4. People will want to purchase it because some parties such as companies want to know that it is a secure third party that they are receiving it from and they also want to keep in contact with the purchaser to have maintenance on it.

Lecture 67

1. The PGP authentication protocol is a digital signature function in which a Sender creates a message M, then generates a hash of M, signs the hash using the private key and prepends the result to the message. Then the Receiver uses the sender's public key to verify the signature and recover the hash code in which the receiver generates a new hash code for M and compares it with the decrypted hash code.
2. The PGP confidentiality protocol is for encrypting messages sent or stored as files in which 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. The receiver uses his private key to recover the session key and the session key is used to decrypt the message. This protocol is applied to the resulting message from the authentication step.
3. Both authentication and confidentiality can be combined for a given message in PGP. The sender generates a signature for the plaintext message and prepends it to the message, the plaintext message plus signature is encrypted then the session key is encrypted using RSA and prepended to the message.

Lecture 68

1. PGP provides other services such as compression, email compatibility and segmentation.
2. Compression is needed to save bandwidth because they are sent over the internet and are needed to be made as small as possible.
3. It is better to sign a message then compress it rather than the other way around because you do not want the signature of the message to depend on the compression algorithm.
4. Radix-64 conversion is used to map groups of three octects into four ASCII characters; it appends a CRC for data error by checking. It expands the message by 33%, it is needed to help some email systems that fail when it comes to certain bit strings that are needed so as not to interpret them as control commands.
5. PGP segmentation is needed because email systems often restrict message length in which longer messages must be broken into segments and mailed separately.

Lecture 69

1. The four kinds of keys used by PGP are public keys, private keys, one-time session symmetric keys and passphrase-based symmetric keys.
2. The special properties needed of session keys are the encryption algorithm and the need for the key to be random.
3. Session keys are generated by the encryption algorithm which generates a new n-bit key from a previous session key and two n/2 bit blocks generated based on user keystrokes including keystroke timing. The two blocks are encrypted using the encryption and the previous key combined to form the new key.
4. The keys are generated by testing an odd number n of sufficient size (>200 bits) and if n is not prime, then repeat it with another randomly generated number until it is found. It takes about ln(2^200)/2 = 70 tries to get it right.
5. Private keys are protected in an encrypted form with a user-supplied passphrase. It is necessary because it protects messages from attackers due to the entire security of the system depends on the private key being kept private.

Lecture 70

1. The user knows which public/private key pairs was used when he receives an encrypted message by there being a generated ID unique for him/her.
2. A user's private key ring is a table of rows containing a timestamp, key ID , public key, private key and user ID
3. A user's public key ring is a table of rows containing a timestamp, key ID , public key and user ID
4. To retrieve a private key from the key ring, the receiver must use the Key ID in the session key component of the message as an index, then a passphrase is prompted to recover the unencrypted private key, PGP then recovers the session key and decrypts the message.
5. The key legitimacy field is for determining the extent as to which PGP trusts that the public key is a valid public key for the user. it is determined from certificates.
6. A key is revoked by the owner issuing a signed key revocation certificate.

Lecture 71

1. Consumer problem is when the attacker gets logically between the client and service and somehow disrupts the communication while the Producer problem is when the attacker produces, offers or requests so many services that the server is overwhelmed. The producer problem is more prevalent.
2. Syn flooding is a form of denial-of-service attack in which an attacker sends a succession of syn's requests to a targets system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.
3. The first three solutions to syn flooding are not ideal because the first solution suggests that the server should increase the queue size but only 8 connections are allowed, increasing the queue size could consume considerable resources. The second solution suggests that the time-out period should be shortened but it might disallow connections by slower clients. The third solution suggests that suspicious packets should be filtered out but it is a hard thing to do because it is hard to determine.

Lecture 72

1. Packet filtering works very well to prevent attack because it helps block messages in a pattern in the request stream; it discards incoming packets with source IP addresses outside of a given range.

2. Intrusion detection system (assumes they are already inside the wall) analyzes traffic patterns and reacts to anomalous patterns while an intrusion prevention system (never gets in) attempts to prevent intrusions by more aggressively blocking attempted attacks.
3. The four different solutions of DDos attacks are:
    a. Over-provisioning the network which means that many servers will be overwhelmed. This solution is expensive and unworkable.
    b. Filtering attack packets which somehow distinguishes the attack packets from regular packets. This solution may not be possible.
    c. Slowing down processing, this disadvantages all requestors but disproportionately disadvantages attackers.
    d. "Speak-up" solution which requests additional traffic from all requestors.

Lecture 73

1. False positives is when harmless behavior is mis-classifies as an attack while false negatives is when a genuine attack is not detected. False negatives are worse because you ignore genuine attacks to the wall.
2. In the IDS context, accurate means detecting all genuine attacks while precise means never reporting legitimate behavior as an attack.
3. The statement means that it easy to implement one or the other but not both simultaneously because it is hard to do.
4. Base rate fallacy is an error in thinking. In IDS, many packets are coming in and not all are malicious, the IDS are dealing with statistically rare events. It is relevant to IDS because it can tell the probabilities of attacks or legitimate behaviors and if it is not accurate, it will turn off because all the alarms will be false alarms.

Lecture 74

1. Code Red version 1 attempted to attack machines by running unpatched versions of Microsoft's IIS webserver.
2. Code Red version 1 was ineffective because there were flaws in the design, mainly the static seed which did very little damage. Once the machines were rebooted, they were disinfected.
3. To say a worn is memory resident means that the virus is only present in that current memory. The implications of it are that once the memory is wiped out, the worm is no longer a threat because it has been erased.
4. Code Red version 2 was much more effective than version 1 because of the amount of hosts it infected and probes sent to infect new hosts. It had major effects on some additional devices with web interfaces such as routers, switches, DSL modems and printers.

Lecture 75

1. Code Red II was related to Code Red versions 1 and 2 because it was a worm that exploited the buffer-overflow vulnerability in Microsoft's IIS webservers and it also contained the string "CodeRedII".
2. Code Red II incorporated its elaborate propagation scheme because it wanted to be able to infect machines without knowing quickly.
3. Code Red II attempted to infect a host, it checks if the host has been infected, if not, it sets a backdoor into the machine then becomes dormant for a day then reboots the machine. (It propagates itself).
4. The implications of a large population of unpatched machines are that they are widely still vulnerable to these worms and it means that it will keep on circulating due to the amount.

5. The lessons of their study are that we are lousy about patching machines which makes the internet much more vulnerable and there are machines out there susceptible to attacks.

Lecture 76

1. A certification regime for secure products is necessary and useful because it is assurance for the purchaser and commercial advantage for the vendor. it is done for medium and high impact systems it involves the vendors and an independent certifying authority to investigate the design, anticipated threats, incorporated controls, and vulnerabilities.
2. The components of an evaluation standard are a set of requirements defining security functionality.(Requirements for OS will be different from Cryptobox). A set of assurance requirements needed for establishing the functional requirements. 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 there is a standard for them and the topic of cryptography is very sensitive.
4. The four levels of certification for cryptographic devices are:
    - **Level 1**: basic security; at least one approved algorithm or function.
    - **Level 2**: improved physical security, tamper-evident packaging. Seals that must be broken to attain physical access to the plaintext cryptographic keys and critical security parameters (CSPs) within the module, or pick-resistant locks on covers or doors to protect against unauthorized physical access.
    - **Level 3**: strong tamper-resistance and countermeasures. Attempts to deter an intruder gaining access to data
    - **Level 4**: complete envelope of protection including immediate zeroing of keys upon tampering.

Lecture 77

1. The Common Criteria is an international standard for computer security certification. It is a framework in which computer system users can specify their security functional and assurance requirements through the use of Protection Profiles. It provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.
2. The Common Criteria is common because any country that wants to use it can do so.
3. There would be a need for 'National Schemes' because each country has a different issue when it comes to security so they need the it to be tweaked to be specific to their own country's needs.
4. A 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 while a Security target is a document that contains the security requirements of a product to be evaluated (TOE), and specifies the measures offered by the product to meet those requirements. PP is a formal description of security for a class of systems while a security target is a specific system or family of systems.

Lecture 78

1. The overall goal of the protection profile as exemplified by the WBIS example is to make sure that all threats are being identified and dealt with accordingly.

2. The purpose of the OT.Inv1 is to detect invalid ID tags, OT.Inv2 is to detect invalid bin-cleared messages, OT.Safe is for fault tolerance and P.Safe is for fault tolerant secondary backup of data within the truck.
3. The purpose of the matrix is designed to counter a threat or fulfil an objective. If x is marked on each level, then all of the threats have something to counter it. The matrix is a systematic way of determining if there are adequate policies to solve the problems presented.

Lecture 79

1. The overall goal of the security target evaluation is to secure user access privileges stored in directory services. No untrusted users can be allowed; authorized users cannot have bad passwords, abuse or mismanage the system etc.
2. A security target evaluation differs from a protection profile evaluation by its policy specified as 'fresh' or as previously evaluated protection profiles. it is a specific system or class of systems submitted for evaluation while a pp evaluation is a description of security for the class of systems.

Lecture 80

1. EALs are Evaluation Assurance Level and they are the level of certification sought. It is used to provide higher confidence that the systems principal security features are reliably implemented. It states as to what level the system was tested.
2. Common Criteria evaluations are performed by an independent organization accredited to perform the testing.
3. The higher EALs are not necessarily mutually recognized by various countries because it takes years for it to be evaluated and it is extremely costly as the levels rises. These levels must have been designed using formal methods, it can't be reversed engineered from the code and components should be kept small and independent.
4. Vendors cannot certify their own products because the evaluation has to be performed by an accredited independent organization in which they are paid to do so. Self-certification will not mean that the EAL is good.
5. It is bad to reverse engineer the model from the code because you need a formal model for them and it is pretty expensive to get it. Automatic theorem prove is needed to reverse engineer the model only which the NSA can do.