Lena Ko
UTEID: lk5399
CS: lk5399
Ko.lena92@gmail.com

Lecture 66

1. PGP is pretty good privacy, the closest you're going to get to military-grade encryption. Extremely strong algorithms packaged in a nice way. Email encryption.

2. Zimmerman's motivation was his strong distrust of the government and believed everyone had the right to privacy.

3. PGP provides effective security because the US government finds it difficult it access PGP-encrypted files.

4. Companies do not like to use freeware and like parties to call on for support.

Lecture 67

1. PGP authentication protocol: uses a digital signature function. Sender sends message and signs. Take hash of message and sign with private key of sender and append to message and send whole thing. The receiver knows it originates with Sender.

2. PGP confidentiality: Sender generates a message and a random session key K, M is encrypted using K, K is encrypted using the recipients public key and prepended to message. Receiver uses his private key to recover session key and the session key is used to decrypt the message.

3. You get both authentication and confidentiality by applying both pieces together.

Lecture 68

1. PGP also provides compressions, email compatibility, and segmentation.

2. Compression is done to save bandwidth.

3. You want to sign before compress so that the signature does not depend on the compression algorithm.

4. Radix-64 conversion maps groups of 3 octets into four ASCII characters. Also appends a CRC for data error checking. It makes sure there are no

anomalous characters in the message. It guarantees no arbitrary binary strings, all ascii. It expands the message by 33%.

5. Some email systems restrict message length. Longer messages must be broken.

Lecture 69

1. PGP uses session keys, public keys, private keys, and a passphrase based key.

2. Session keys should be random appearing and not guessable. High entropy.

3. Session keys are generated by the 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 algorithm and the previous key, and combined to form the new key. Easy.

4. Using primes generates the keys. Difficult and expensive.

5. The private key needs to be protected so that no one can use them to decrypt. Supplying a passphrase generates them. When a new public/private key is generated, the system asks for the passphrase. A 160 bit hash code is generated from the passphrase which is discarded. The private key is encrypted using CAST 128 with 128 bits of the hash code as key. The key is then discarded. Whenever the user wants to access the private key, he must supply the passphrase.

Lecture 70

1. If a user has multiple private/public key pairs, he knows which was used when he receives an encrypted message by generating an ID likely to be unique for a given user. It uses the least significant 64 bits of the key as the iD.

2. A table of timestamp, key id, public key, private key, and user ID is on a user's private key ring.

3. A table of timestamp, key id, public key, and user id is on the public key ring.

4. You retrieve a private key by typing in a passphrase. This is hashed and then used to recover the encrypted private key. PGP recovers the session key and decrypts the message.

5. The key legitimacy field indicates the extent to which PGP trusts that this is a valid public key for this user. Legitimacy is determined from certificates and chains of certificates, the user's assessment of the trust to be assigned to the key, and various heuristics for computing trust.

6. A key is revoked by sending out a revocation certificate. Recipients are expected to update their public–key rings.

Lecture 71

1. The difference between the consumer and producer problem: Consumer problem is also called man in the middle attack. The attacker gets logically between the client and service and somehow disrupts the communication. The producer problem is when the attacker produces, offers or requests so many services that the server is overwhelmed. A typical producer attack overwhelms the server so that it cannot respond to other attacks, tying its resources. Block traffic from clients vs. flood server.

2. Syn flooding is relying on the properties of a protocol. An 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. All legitimate access are denied until the connections time-out. The half open connections fill up the table and disallows legit clients to use server.

3. The first 3 solutions to syn flooding are not ideal because
    a. Limit to how much you can increase server's queue size
    b. Shorten time out period: might disallow connections by slower clients.
    c. Filter suspicious packets: if return address doesn't match source, discard packet: may be hard to determine..to aggressive may be a denial of service attack.

Lecture 72

1. Packet filtering can work well to prevent attacks by detecting patterns of identifiers in the request stream and block messages in that pattern but it is very expensive.

2. The difference between intrusion detection and intrusion prevention systems: IDS can analyze traffic patterns and react to anomalous patterns. Often there is nothing apparently wrong with the volume of requests, an IDS reacts after the attack has begun. An IPS attempts to prevent intrusions by more aggressively blocking attempted attacks. This assumes that the attacking traffic can be identified.

3. DDoS attack comes when an attacker takes over a number of nodes in a network and uses them as bots to launch a coordinated producer attack. The four different solutions mentioned to DDoS attacks are:

    a. Over-provisioning the network: have too many servers to be overwhelmed (expensive and unworkable)
    b. Filtering attack packets: somehow distinguish the attack packets from regular packets(difficult maybe impossible)
    c. Slow down processing: disadvantages everyone even legit clients
    d. Speak up solution: request additional traffic from all requestors.

Lecture 73

1. False positives and false negatives: false positives are harmless behavior is mis-classified as an attack. False negatives are when a genuine attack is not detected. False negatives are the bigger problem.

2. Accurate(false negatives) and precise(false positives) IDS context : IDS is accurate if it detects all genuine attacks, and it is precise if it never reports legitimate behavior as an attack.

3. It's easy to build an IDS that is either accurate or precise. It is difficult to do both simultaneously.

4. Base rate fallacy. Relevancy to IDS. An undetected attack might lead to problems but frequent false alarms lead to the system being disabled. IDS suffer from the base rate fallacy. 1% of traffic are actually attacks and the detection accuracy of your IDS is 90%. This means IDS classifies an attack as an attack with probability 90%. IDS classifies a valid connection as attack with probability 10%. Must be very accurate or it will suffer from base rate fallacy. If attack rate is rare, IDS must be accurate to be useful.

Lecture 74

1. Code Red version 1 attempted to attack a vulnerability and attempted to infect machines, and if from 20-28th it launched a denial of service flooding attack against the white house.

2. Code Red version 1 was ineffective because the worm used a random list of IP addresses to attack but the random generated used a static seed always starting from the same starting point, so the same machines were attacked over and over again. The white house changed the IP address.

3. A worm is memory resident when it resides in the memory of the machine and can be disinfected by simply rebooting it. Once rebooted, remains vulnerable because it probes the same list of IP addresses.

4. Code Red version 2 was more effective because it used a random generated seed, spreading the worm more widely. It had a greater impact due to the volume of hosts infected and probes sent to infect new hosts because ip addresses corresponded to routers and printers instead of computers, so many crashed.

Lecture 75

1. Code red II related to code Red (1 and 2) because he used the code red string in the code. Writer knew about first versions.

2. Code Red II incorporated its elaborate propogation scheme because ip addresses with the same prefix are on the same part of the internet and more likely that the machines on that subnet are running the same software. You will have more luck infected those machines. Code Red II aimed from computers so stayed away from some ip addresses.

3. Code Red II attempted to install a backdoor machine and propogate itself.

4. Implications of a large population of unpatched machines: There is a huge amount of computers that are vulnerable to the same or similar attack. There are a low percentage of patches

5. Verizon 230 million compromised customer records found that 9 out of 10 breaches attributed to hacking attacks took advantage of a vulnerability for which a fix was available.

Lecture 76

1. A certification regime from secure products are necessary and useful because it assures the purchaser and commercial advantage for the vendor.

2. Components of an evaluation standard are:

    a. A set of requirements defining security functionality
    b. A set of assurance requirements needed for establishing the functional requirements
    c. A methodology for determining that the functional requirements are met
    d. A measure of the evaluation result indicating trustworthiness of the evaluated system.

3. Crypto devices have a separate evaluation mechanism because it may need to be secure on a higher level.

4. The four levels of certification for crypto devices
    a. Level 1: basic security, one approved algorithm
    b. Level 2: Improved physical security, tamper evident packaging
    c. Level 3 strong tamper resistance and countermeasures
    d. Level 4 complete envelope of protection including immediate zeroing of keys upon tampering.

Lecture 77

1. Common Criteria is a evaluation for secure systems comprised of the CC documents, the CC evaluation methodology.

2. It is common because many countries have adopted it.

3. National Schemes may be needed because it may need to be specific for a country's own standards or situations.

4. The differences between a protection profile and a security target are a protection profile – a document describing a security policy of a class of systems. Ie. A firewall should have specific policies. A security target evaluation is an evaluation of a product. Ie. A firewall.

Lecture 78

1. The overall goal of the protection profile as exemplified by the WBIS example is to detect invalid ID tags, detect invalid in cleared messages, and fault tolerance.

2. The purpose of the various parts of the protection profile to be thorough in protecting the system, requirements. It illustrates the security means for a particular class of systems. IT provides a systematic way of deciding whether threats and assumptions are being addressed by the mechanisms proposed.

3. The purpose of the matrix is to show a mapping from threats/ assumptions and the objectives/requirements. The idea is that if you fill in matrix every row in table has X in a you have thoroughly checked and they are adequate to solve the problems.

Lecture 79

1. The overall goal of the security target evaluation as exemplified by the Sun Identity Manager example is show how the product enforces the notion of security of what it means for a product.

2. 2. A security target evaluation differs from a protection profile evaluation because it focuses on how the product enforces the policies while the protection profile defines those policies.

Lecture 80

1. EALs are evaluation assurance levels.

2. Independent organizations accredited to perform CC testing perform the Common Criteria evaluations at lower levels. Government at higher levels.

3. The Higher EALs are not necessarily mutually recognized by various countries because specific agencies of countries are used to evaluate higher levels.

4. Vendors certify their own products because it needs to be secured by government agencies that are certified.

5. The formal levels must have been designed using formal mathematical levels methods.