Name: Jessica Lucci
EID: jml3624
CS Login: jlucci
Email: jessicalucci14@gmail.com

Lecture 66

1. PGP (Pretty Good Privacy) is an extremely secure version of data encryption/decryption.
2. Zimmerman wanted to provide a strong encryption system that was easy to use, accessible to everyone and protected people's privacy (especially from government).
3. PGP has been proven to provide effective security, as it was undecipherable in 2003 by both the Italian police and FBI, and deemed "nearly impossible" to decrypt in 2006 by the American government.
4. PGP is freeware, but some people or businesses may choose to purchase support if they need help maintaining, implementing, etc, it.

Lecture 67

1. In the PGP authentication protocol, the sender sends both the message and a hash of the message encoded with their private key. The receiver then creates a hash of the received message, uses the sender's public key to decode the sent hash, and then finally compares the decoded sent hash to the self-generated hash.
2. In the PGP confidentiality protocol, the sender generates a session key, encrypts said key with the receiver's public key, encrypts the message with the session key, and then sends both of these objects to the receiver. The receiver then uses their private key to decrypt the session key, then uses the decrypted session key to decrypt the message.
3. In order to get both authentication and confidentiality in PGP, the authentication protocol is applied to the message, and then the confidentiality protocol is applied to that resultant message.

Lecture 68

1. In addition to authentication and confidentiality, PGP provides compression, email compatibility, and segmentation.
2. Compression is a needed step in PGP because compression reduces redundancy in the message to be sent, thus strengthening the overall encryption.
3. Messages are often signed before they're compressed so that the signature won't rely on the compression algorithm.
4. Radix-64 converts groups of 3-octets into 4 ASCII characters. This conversion is needed in PGP as encrypted text, which contains 8-bit octets, often contains bit strings that email systems would interpret as control commands.
5. Segmentation is needed in PGP as many email systems restrict message length (forces a message to be sent in segments, rather than as a whole).

Lecture 69

1. PGP uses session, public, private and passphrase-based keys.
2. Session keys may only be used once, and so must be generated for each new message.
3. *N*-bit Session keys are generated from a previous session key and from two *N*/2-bit blocks generated based on user keystrokes.
4. To create new RSA keys, PGP continuously generates a random odd number *n* until *n* is a prime number.
5. Private keys are protected by a user-generated passphrase. This passphrase is used to create a 160-bit hash code using SHA-1, and then that hash code is used in the CAST-128 encryption algorithm to encrypt the private key. This is necessary in order to prevent malicious parties from gaining access to the private key.

Lecture 70

1. If multiple public/private key pairs are being used, PGP generates an ID of each key that is the least significant 64-bits of the key. This ID is used whenever a user receives a message to see if the user has a matching key.
2. A user's private key ring has a timestamp, Key ID, public and private keys, and the user's ID.
3. A user's public key ring has a timestamp, Key ID, public key and the user's ID.
4. In order to retrieve a private key from a user's key ring, PGP first retrieves the encrypted private key using the Key ID field in the session key component of the message. PGP then asks the user for their key passphrase, uses said passphrase to recover the unencrypted private key, and then finally recovers the session key and decrypts the message.
5. The key legitimacy field is used to indicate the extent to which PGP trusts that the key is a valid public key for its' associated user.
6. A key is revoked by a user sending out a key revocation certificate.

Lecture 71

1. The consumer problem is when an attacker "gets between" the client and the service in a way that disrupts the communication between the two, while the producer problem is when an attacker produces, offers or request so many services that the service is disrupted or overwhelmed.
2. Syn flooding is an attack in which the attacker forges the return address on syn packets, and bombards a server with those packets. The server then eats up resources waiting for responses from the packets that will never come.
3. Increasing the server's queue size would only consume additional server resources during an attack, shortening the time-out period could potentially prevent slower clients from connecting and filtering suspicious packets would be very difficult to do accurately.

Lecture 72

1. Packet filtering can work sufficiently to protect attacks, but it's very difficult to accurately determine malicious packets from normal requests.
2. An intrusion detection system attempts to identify attacks that have already happened or are currently occurring, while an intrusion prevention system attempts to prevent attacks from occurring at all.
3. 4 ways to prevent DDoS attacks:
    a. *Over-Provisioning the Network*: Create excess resources, so that there are too many to be overwhelmed.
    b. *Filtering Attack Packets*: Institute a mechanism that filters out malicious packets.
    c. *Slow Down Processing*: Slow down server processes, so that attackers are disadvantaged.
    d. *"Speak-up" Solution*: Request additional traffic from all clients attempting to connect.

Lecture 73

1. A false negative means that an actual attack was not detected, while a false positive means that the system thinks attack occurred when in reality it hadn't. Which one of these is worse depends on the particular system and its goals/mechanisms.
2. An accurate IDS detects *all* genuine attacks, while a precise IDS *only* detects genuine attacks (won't produce any false positives).
3. It's easy to build an IDS that's accurate (just assume every request is an attack), and it's easy to build an IDS that's precise (don't report any attacks), but it's very difficult to build an IDS that's accurate and precise simultaneously.
4. The base rate fallacy is a type of error in thinking in which people tend to ignore base rate information and focus on specific information. For example, in IDS, people tend to focus on the probability that an alarm is for an actual attack, instead of the probability than alarm will go off in general. This leads to a gross overestimation of the accuracy of an IDS.

Lecture 74

1. CodeRed version 1 attempted to perform a DoS attack on www1.whitehouse.gov.
2. CodeRed version 1 was ineffective because the designers of the attack used a static seed random number generator (only a small number of IPs to infect was generated), and the IP address for www1.whitehouse.gov was changed.
3. If a worm is "memory resident", it means that the worm can be eradicated simply by rebooting the system it has infected. However, this doesn't mean that the system can't be reinfected once it comes back online.
4. CodeRed version 2 was much more effective than its' predecessor as it used a random seed in its random number generator. This meant that many more machines could be infected at a much quicker rate than in CodeRed version 1.

Lecture 75

1. Like CodeRed Versions 1 and 2, CodeRedII exploited a buffer-overflow vulnerability in Microsoft's IIS webservers by infecting vulnerable machines, and making those machines randomly generate IP addresses that the infected machine will try to also infect. However, CodeRedII had different goals for the worm, and was not memory resident.
2. CodeRedII implemented an elaborate propogation scheme that would more frequently infect systems with similar IPs, as many machines on the same networks/subnet are likely to be running similar software.
3. CodeRedII attempted to create back-door/root access to infected machines.
4. A large population of unpatched machines means that a large population of machines are open to attack. In CodeRedII's case, these unpatched machines were vulnerable to being infected, providing a massive amount of computing power for any future attacks (CodeRedII effectively creates zombie computers).
5. Verizon's study showed that many attacks could have been prevented by publicly available software, and that many people don't patch their machines. The main lesson to be learned from this study is keep up to date with software patches.

Lecture 76

1. A certification regime for secure products is necessary/useful, as many security product users don't have the necessary expertise to identify, purchase and install needed security products. Instead, they have to rely on some sort of certifiable intermediary to perform those functions for them.
2. An evaluation standard consists of a set of requirements that define 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 devices have a separate evaluation mechanism because cryptography is an extremely sensitive subject with a minimal amount of experts in the field.
4. Four levels of certification for crypt devices:
    a. *Level 1:* The lowest level of security, that covers basic security requirements, requiring the use of at least one approved algorithm and function. No specific physical security mechanisms are required.
    b. *Level 2:* Requires that the system have tamper-evident packaging, such as tamper-evident seals, or pick-resistant locks.
    c. *Level 3:* Requires strict tamper-resistance and countermeasures in order to deter intruders from gaining access to sensitive data.

d. *Level 4:* High level of security that attempts to create an envelope of protection with the intent of detecting and protecting against all attacks. Includes immediate zeroing of keys upon tampering.

Lecture 77

1. The Common Criteria is an evaluation criteria for secure systems that is currently used by 26 countries.
2. The Common Criteria consists of CC documents, the CC Evaluation Methodology, and for each specific country it's being used in, a set of country-specific evaluation methodologies called an Evaluation (or National) Scheme.
3. Different countries have National Schemes, as they each decided it was necessary to "tweak" the Common Criteria in a way that works better with their already established, country-specific mechanisms.
4. A security target (ST) is a set of security requirements to be used as the basis of an evaluation, while a protection profiles (PP) are a set of security requirements for a category of systems that are independent of the system implementation.

Lecture 78

1. The overall goal of the protection profile as shown in WIBS is to identify the potential threats to assets, and establish a set of security requirements to protect against those threats.
2. The protection profile from WIBS includes a set of assets (so the system knows what needs to be protected), a set of environmental assumptions (so the system knows what to expect), a list of threats (so the system knows what it's protecting against), and a list of security objectives and requirements (so the system knows what it should accomplish).
3. The matrix on slide 7 provides a systematic way of deciding whether threats/assumptions are being addressed by mechanisms and requirements.

Lecture 79

1. The overall goal of the security target evaluation as exemplified bythe Sun Identity Manager example is to manage user access privileges.
2. A security target is a product, and a protection profiles are abstract definitions of security. Therefore, an evaluation for a security target will have much more specific rules, while a protection profile evaluation will have more generalized, abstract rules.

Lecture 80

1. EALs are evaluation levels, and they are used to assign different levels of rigor to vendor's products.
2. The government of countries perform CC evaluations on their respective vendor's products.

3. Higher EALs are not mutually recognized by various countries, as high level EALs are extremely sensitive and difficult to perform correctly (not everyone trusts that other country's experts and methods are on par with theirs).
4. Vendors cannot certify their own products in order to prevent vendors from falsifying testing results.
5. It's bad to reverse engineer the model from the code, as you'd have to force your code to fit into certain specifications that it wasn't built for.