Brian Chow
EID/CS login: bc23784
Email: brianj.chow@yahoo.com
CS 361 (90155)
For 07/10/14

Week 5 Questions

Lecture 66

1) What is PGP?
    1. Pretty Good Privacy is an encryption program.
2) What motivated Phil Zimmerman to develop it?
    1. A “strong distrust of the government” and a strong belief that “everyone had an absolute right to privacy.”
3) Does PGP provide effective security?
    1. Yes; it uses a wide variety of encryption algorithms that have been extensively reviewed, and the likelihood of a successful decryption is nearly 0.
4) If PGP is freeware, why would anyone bother to purchase support?
    1. One reason would be accountability - anyone can modify a distribution of PGP to insert malicious code with almost complete impunity, but those distributions purchased from a company should be free of any malicious code.

Lecture 67

1) Explain the PGP authentication protocol.
    1. The sender's message is hashed, which is then signed using the sender's private key and the result prepended to the message. The receiver uses the sender's public key to “verify the signature and recover the hash code,” which is then compared against a new hash generated for the message.
2) Explain the PGP confidentiality protocol.
    1. The sender generates a random session key and uses it to encrypt its message. The random session key is then encrypted using the receiver's public key, and the result is prepended to the message. The receiver then uses its “private key to recover the session key”, which is then used to decrypt the message.
3) How do you get both authentication and confidentiality?
    1. “Apply the authentication step to the original message”, and then “apply the confidentiality step to the resulting message.”

Lecture 68

1) Besides authentication and confidentiality, what other “services” does PGP provide?
    1. In addition to those, it provides compression, email compatibility, and segmentation. Those additional “services” are better classified as “engineering features designed to make PGP efficient and robust.”
2) Why is compression needed?
    1. Compression “reduces redundancy in the message”, and thus “strengthens the encryption.”

3) Why sign a message and then compress, rather than the other way around?
    1. So that the signature doesn't "depend on the compression algorithm", and also because "versions of the compression algorithm behave slightly differently, though all versions are interoperable."
4) Explain radix-64 conversion and why it's needed.
    1. It is needed to prevent certain systems (e.g., email) from interpreting some (encrypted) 8-bit octets as control commands. With radix-64 conversion, groups of three octets are mapped to groups of four ASCII characters. Radix-64 conversion also "appends a CRC for data error checking."
5) Why is PGP segmentation needed?
    1. For the same reason why data transmitted over the Internet is split up instead of being transmitted all at once (higher arrival success rate), as well as the fact that some systems (e.g., email) restrict message length.

Lecture 69

1) What are the four kinds of keys used by PGP?
    1. Session keys, public keys, private keys, and passphrase-based keys.
2) What special properties are needed of session keys?
    1. Each must be "associated with a single message and used only once."
3) How are session keys generated?
    1. Using a chosen encryption algorithm, a new key is generated from a previous session key and two blocks are "generated based on user keystrokes, including keystroke timing. The two blocks are encrypted using [the chosen encryption algorithm] and the previous key, and combined to form the new key."
4) Assuming RSA is used for PGP asymmetric encryption, how are the keys generated?
    1. ". . . an odd number of sufficient size (usually > 200 bits) is generated and tested for primality. If it is not prime, repeat the process with another randomly-generated number until a prime number is found."
5) How are the private keys protected? Why is this necessary?
    1. They are protected by encrypting them with a user-supplied passphrase, which helps prevent access to and/or generation of a private key for a user by unauthorised parties.

Lecture 70

1) If a user has multiple private/public key pairs, how does he know which was used when he receives an encrypted message?
    1. An ID that is "likely to be unique for a given user" is generated, which is then used by the receiver to "verify that he has such a key on his 'key ring'. The associated private key is used for the decryption."
2) What's on a user's private key ring?
    1. The user's own public/private key pairs.
3) What's on a user's public key ring?
    1. The public keys of the user's correspondents.
4) What are the steps in retrieving a private key from the key ring (PGP)?
    1. The receiver's encrypted private key is retrieved from the private-key ring "using the Key ID

field in the session key component of the message as an index." The user is then prompted for his/her passphrase "to recover the unencrypted private key", which is then used to "recover the session key and decrypt the message."

5) What is the key legitimacy fold for?
   1. It "indicates the extent to which PGP trusts that this is a valid public key for the user." It 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) How is a key revoked?
   1. The key's owner "issues a signed key revocation certificate" to his/her correspondents, who "are expected to update their [own] public-key rings."

Lecture 71

1) Explain the difference between the consumer and producer problems. Which is more prevalent?
   1. They are classifications of denial-of-service attacks. The consumer problem (aka "man-in-the-middle attack") occurs when "the attacker gets logically between the client and the service and somehow disrupts the communication." The producer problem occurs when the server is overwhelmed by the volume of requests by the attacker ("the attacker produces, offers, or requests so many services that the server is overwhelmed").
2) Explain SYN flooding.
   1. SYN flooding occurs when an attacker attempts a transaction that involves some handshake protocol and intentionally does not respond to the server, causing the server to wait. Examples include establishing a TCP connection (the server waits for a never-coming acknowledgment (ACK) signal from the attacker until time-out) and a syn flooding attack, which occurs "when an attacker forges the return address on a number of SYN packets", flooding the server with half-open and slowing down/denying legitimate accesses.
3) Why are the first three solutions to SYN flooding (in the way TCP connections are established) not ideal?
   1. "Increase the server's queue size" - more resources are required, and an attacker could probably get around this quite easily by attempting more connections.
   2. "Shorten the time-out period" - connections by slower clients and/or physically-distant clients could be disallowed.
   3. "Filter suspicious packets (if the return address does not match the apparent source, discard the packet)" - may be difficult to determine suspiciousness (e.g., redirects).

Lecture 72

1) Does packet filtering (detecting patterns of identifiers in the request stream and block messages in that pattern) work well to prevent attacks?
   1. It can, if (for example) there is a well-defined pattern of standard usage, and the filter is not so aggressive as to deny legitimate requests.
2) What are the differences between intrusion detection and intrusion prevention systems?
   1. The former only reacts after an attack has begun; it "analyzes traffic patterns and reacts to anomalous patterns", which may not work very well if "there is nothing apparently wrong but the volume of requests." The latter actively attempts to prevent an attack/intrusion

from occurring by “more aggressively blocking attempted attacks, [which] assumes that the attacking traffic can be identified.”

3) Explain the four different solutions mentioned in DDoS attacks.
    1. “Over-provision the network (have too many servers to be overwhelmed)” - this is only feasible in an environment with unlimited space, money, and resources.
    2. “Filtering packet attacks (somehow distinguish the attack packets from regular packets)” - it may be very difficult or even impossible to observe such a distinction.
    3. “Slow down all processing” - it “disadvantages all requestors, but perhaps disproportionately disadvantages attackers.”
    4. “'Speak-up' solution (request additional traffic from all requestors)” - this “assumes that the attacker's bots are already maxed out, [raising] the proportion of valid to invalid requests.”

Lecture 73

1) Explain false positives and false negatives. Which is worse?
    1. False positives occur when “harmless behaviour is misclassified as an attack.” False negatives occur when “a genuine attack is not detected.” In general, a false positive is more likely to be destructive and/or have drastic consequences, and is worse (assuming a system has some override procedure in place and cannot be manually shut off).
2) Explain what “accurate” and “precise” mean in the IDS context.
    1. An accurate IDS is one that “detects all genuine attacks.” A precise IDS is one that “never reports legitimate behaviour as an attack.”
3) Explain the statement: “It's easy to build an IDS that is either accurate or precise”.
    1. Balancing accuracy and precision is difficult since different attacks don't have to take the same form, just as legitimate behaviour doesn't always occur in one predefined manner.
4) What is the base rate fallacy? Why is it relevant to an IDS?
    1. It is the tendency to ignore base rate (generic/general) information when it is presented concurrently with specific information. It is relevant to an IDS when analyzing false positives and negatives. For example, a given IDS falsely classifies harmless behaviour as an attack 5% of the time and never fails to detect a genuine attack. If 1/1000 transactions are actual attacks, and the IDS detects that the current transaction is an attack, then the probability that it is actually an attack is roughly 0.02 (not 0.95).

Lecture 74

1) What did Code Red v1 attempt to do?
    1. It took advantage of a buffer-overflow vulnerability in Microsoft's IIS webservers to infect unpatched machines, which were then used to infect other machines. Collectively, the machines were to launch a DoS flooding attack on www1.whitehouse.gov.
2) Why was Code Red v1 ineffective?
    1. A static seed was used in its random number generator, resulting in identical lists of IP addresses being used to infect new machines and hindering the worm's distribution.
    2. The IP address for www1.whitehouse.gov was changed, resulting in the failure of the DoS attack.
    3. The worm was memory-resident; a simple reboot would have removed it (but the machine

was still susceptible to re-infection).

3) What does it mean to say that a worm is "memory-resident"? What are the implications?
    1. It means that the worm "exists" in the RAM (random-access memory) of the system, and upon a hard reboot or a shutdown/bootup cycle will effectively disappear, since state is not preserved during the restart/shutdown procedures. However, unless the means by which the worm got into the system in the first place is blocked/prevented or patched/fixed, the worm can easily re-enter the system (e.g., boot sector and file infector viruses). Memory-resident worms can affect system performance, depending on their size and what they do, on top of potentially infecting writable media, data files, and/or file executables.
4) Why was Code Red v2 much more effective than Code Red v1?
    1. It was modified to use a random seed in its random number generator, resulting in a vastly-larger number of systems being infected. It could also cause "routers, switches, DSL modems, and printers" to "crash or reboot when an infected machine attempted to send them a copy of the worm."

Lecture 75

1) How was Code Red II related to Code Red v1 and v2?
    1. It also randomly generated an IP address to serve as its next victim.
2) Why do you suppose Code Red II incorporated its elaborate propagation scheme?
    1. In order to increase its infection rate; instead of wasting time and resources attempting to infect a machine that may not even exist, attempt to infect machines on a Class A or B network (the networks with the largest number of possible hosts on them).
3) What did Code Red II attempt to do?
    1. "Install a [backdoor] mechanism for remote, root-level access to the infected machine", allowing "any code to be executed so that the machines could be used as zombies for future attacks."
4) Comment on the implications of a large population of unpatched machines.
    1. By not installing patches as they become available, the large population of unpatched machines is essentially a large population of machines available for use as zombies in future attacks, so long as they remain "infect-able".
5) Comment on the report from Verizon cited on slide 6. What are the lessons of their study?
    1. It states that the vast majority of data breaches (~90%) occurred due to attacks on a vulnerability that had been patched at least half a year earlier, indicating that patch installation rates are very low.

Lecture 76

1) Why is a certification regime for secure products necessary and useful?
    1. It is necessary because the customer usually does not have the expertise, time, resources, and/or money to perform such a certification on their own.
2) Explain the components of an evaluation standard.
    1. An evaluation standard is comprised of "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.” It provides a “certified level of confidence for security products.”

3) Why would crypto devices have a separate evaluation mechanism?
    1. Just as there are multiple confidentiality/integrity levels for individual access to an object, there are different levels for crypto devices that certify how trustworthy/safe a device is, ranging from basic protection to complete protection. Secure products do not necessarily have to undergo such classification (unless offering multiple versions).
4) Explain the four levels of certification for crypto devices.
    1. The first level offers basic protection, with “at least one approved algorithm or function.” The second level offers “improved physical security [with] tamper-evident packaging.” The third level provides “strong tamper-resistance and countermeasures”, which may include physical key access or the employment of multiple crytographic algorithms/procedures. The fourth and highest level provides a “complete envelope of protection, including immediate zeroing of keys upon tampering.”

Lecture 77

1) What is the Common Criteria?
    1. Evaluation methodologies employed in evaluating secure products such that if one signatory (country) evaluates and deems a product secure according to the methodologies, the other signatories will have reason to believe that the product is secure.
2) What's “common” about it?
    1. The evaluation methodologies and results are shared all signatories.
3) Why would there be any need for “National Schemes”?
    1. One country may wish to impose additional requirements on top of the standard requirements in order for a product to be certified for use within its borders.
4) Explain the difference between a protection profile and a security target.
    1. The former is “a description of a family of products in terms of threats, environmental issues and assumptions, security objectives, and requirements of the Common Criteria.” It sets out “implementation-independent security requirements for a category of products or systems.” The latter is “a document that contains the security requirements of a product to be evaluated, and specifies the measures offered by the product to meet those requirements.” It is specifically targeted towards a product; thus, a security target may match a protection profile.

Lecture 78

1) Explain the overall goal of the protection profile as exemplified by the WBIS example.
    1. To “describe what security means for a particular class of systems” (here, the waste bin identification system) and provide a “systematic way of deciding whether threats and assumptions are being addressed by [the systems'] mechanisms and requirements.”
2) What is the purpose of the various parts of the protection profile as exemplified in the WBIS example?
    1. To set out the various “preconditions” (assumptions) of the system, and to ensure that there are measures in place to handle “damaged” or “irregular” data and what action(s) should be taken upon encountering them.
3) What is the purpose of the matrix on slide 7?

    1. To map which threats/assumptions are handled by which security objectives/requirements.

Lecture 79

1) Explain the overall goal of the security target evaluation as exemplified by the Sun Identity Manager example.
    1. To apply the concepts of security laid out in a protection profile evaluation to a specific product/system/class of systems.
2) How do you think that a security target evaluation differs from a protection profile evaluation?
    1. A security target evaluation targets a specific product and may match a protection profile evaluation. A protection profile evaluation only "describes what security means for a particular class of systems", and for obvious reasons cannot match a security target evaluation.

Lecture 80

1) What are the Evaluation Assurance Levels (EALs), and what are they used for?
    1. They are levels representing how far a product has been evaluated that are used by the product's vendor to provide "assurance that the corresponding rigor was applied during development and test." The levels range from EAL1 ("functionally tested") to EAL7 ("formally verified design and tested").
2) Who performs the Common Criteria evaluations?
    1. They are performed by "an independent organization accredited to perform CC testing." In the US, accreditation is handled by the National Institute of Standards and Technology (NIST).
3) Speculate why the higher EALs are not necessarily mutually recognized by various countries.
    1. Above EAL4, the level of knowledge necessary for the evaluation dramatically increases, with a corresponding increase in the stringency requirements of the program ("can't reverse-engineer the model from the code", "components should be kept small and independent"), and the process must be extensively documented. These requirements become that much more important if the product is to handle matters of national security.
    2. Being a signatory to the Common Criteria does not guarantee that the evaluation was actually performed and that the documentation is genuine.
    3. In the US, only the NSA can perform EAL5/EAL6/EAL7 testing.
4) Can vendors certify their own products? Why or why not?
    1. No; this would be similar to nepotism or self-promotion, and could result in scenarios where the vendor prioritizes monetary gain over ensuring that its products are truly secure.
5) If you're performing a formal evaluation, why is it probably bad to be able to reverse-engineer the model from the code?
    1. It could lead to the complete destruction of the security protocols/algorithms/etc the product employs, rendering the product essentially useless.