Name: **Zhenyu Zhu**

Date: **7/5/2014**

EID: **cike**

CS login: **zhenyu**

Email: **zhu_zhenyu@utexas.edu**

CS361 Questions: Week 5

Lecture 66

1. What is PGP?

   It stands for “Pretty Good Privacy”, and it is in the form of an email encryption system that is extremely strong, using state of art cryptographic algorithms, easy to use and accessible to all average users.

2. What motivated Phil Zimmerman to develop it?

   Zimmerman has strong distrust of the government, and strong belief that everyone had an absolute right to privacy.

3. Does PGP provide effective security?

   Yes, it does provide extreme strong security.

4. If PGP is freeware, why would anyone bother to purchase support?

   Because commercial company didn’t want to use freeware, they want the parties that are available that they can actually call on to get maintenance and that sort of support. Freeware does not provide these types of support, where most people in the commercial company that using the PGP does not has computer science background.

Lecture 67

1. Explain the PGP authentication protocol.

   Sender created a message M and generated a 160-bit hash value of M using SHA. Then sender signs the hash using his private key and append the results to the message within PKI. Assuming receiver knows send’s public key, he can use this key to verify the signature and recover the hash code. Receiver can generate a new has code with the message M and compare it to the decrypted hash code to check the integrity of the M.

2. Explain the PGP confidentiality protocol.

Sender generates a message M, and a random 128-bit session key K for this session only. M is encrypted using K; K is encrypted using the recipient's public key and appended to the message with PKI. Receiver uses his private key to recover the session key, and use this key to decrypt the message.

3. How do you get both authentication and confidentiality?

Let M' = $(\{h(M)\}_{K_S^{-1}}, M)$, then S → R: $\{K\}_{K_r}, \{M'_K\}_K$

Lecture 68

1. Besides authentication and confidentiality, what other "services" does PGP provide?

Compression, Email compatibility, and Segmentation.

2. Why is compression needed?

It helps strengthen the encryption by reduces redundancy in the message, also can save bandwidth of the channel.

3. Why sign a message and then compress, rather than the other way around?

Because it is preferable to sing an uncompressed message so that the signature does not depend on the compression algorithm.

4. Explain radix-64 conversion and why it's needed?

It is needed because many email systems permit only ASCII text and PGP's encrypted text contains arbitrary 8-bit octets and can be interpreted by the mail system as control commands. Radix-64 conversion is to map groups of three octets (24 bits) into four ASCII character (32 bits), and appends a CRC for data error checking. By default, even ASCII is converted.

5. Why is PGP segmentation needed?

Because email systems often restrict message length, and PGP automatically segments message that are too large after all the other steps, and at the receiving end, PGP strips off mail headers and reassembles the message from its component pieces.

Lecture 69

1. What are the four kinds of keys used by PGP?

One –time session symmetric key, public key, private key, and passphrase-based symmetric keys.

2. What special properties are needed of session keys?

Each session key is associated with a single message and used only once.

3. How are session keys generated?

Combining the two encrypted n/2-bit block with encryption algorithm E and the previous session key generate the new key. The two n/2-bit blocks generated based on user keystrokes, including keystroke timing, so it will be random enough that an attacker can't guess.

4. Assuming RSA is used for PGP asymmetric encryption, how are the keys generated?

The generation of large prime key pairs is handled as in RSA. An odd number n of sufficient size (> 200 bits) is generated and tested for primality. If it is not a prime, then repeat with a randomly generated number, until a prime is found, usually takes 70 tries since we exclude even numbers to find a prime of around 200 bits.

5. How are the private keys protected? Why is this necessary?

The private key is stored encrypted with a user-supplied passphrase; the passphrase is hashed and used to encrypt the private key. It is necessary because the entire security of the system depends on protecting private keys.

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?

By the Key ID attached with the message, which is the least significant 64-bits of the public key used to encrypted the message.

2. What's on a user's private key ring?

Timestamp; Key ID; Public key; Private key; and User ID.

3. What's on a user's public key ring?

Timestamp; Key ID; Public Key; User ID.

4. What are the steps in retrieving a private key from the key ring?

a) PGP retrieves receiver's encrypted private key from the private-key ring, using the Key ID filed in the session key component of the message as an index.
b) PGP prompts the user for the passphrase to recover the unencrypted private key.

5. What is the key legitimacy field for?

    It is used to indicate the extent to which PGP trusts that this is a valid binding between the user and his public key.

6. How is a key revoked?

    The owner issues a signed key revocation certificate, recipients are expected to update their public-key rings.

Lecture 71

1. Explain the difference between the consumer and producer problems. Which is more prevalent?

    Consumer problem is about attacker blocking the client to send request to server by somehow disrupting the communication. Producer problem is about the attacker overwhelms the server by sending large volume of the request or tie up server's request with some false handshake protocol.

    The producer problem is typical more prevalent.

2. Explain syn flooding.

    It is relying on the property of three-way handshake between a client establishes a TCP connection with a server. It happens when an attacker forges the return address on a number of SYN packets, then the server fill its table with these half-open connections, which leaves no room for all legitimate access. Since the return address has been faked, the receivers may be unavailable or unable to ACK. Sender table is filled and have to wait for connections to time out, which blocks all other legitimate access.

3. Why are the first three solutions to syn flooding not ideal?

    Increase the server queue size could consume considerable resources since each internal table takes about average 600 bytes per request to fill. Shorten the time-out period is a DoS attack on its own, since it might disallow connections by slower clients. Filter suspicious packets are hard to determine since how can you decide if a packet is valid or not just by examine the return address.

Lecture 72

1. Why does packet-filtering work very well to prevent attacks?

    It can but its expensive to do it deeply, as I asked on Piazza, it is hard trying to filter/block the flooding attack by detect patterns of identifiers, it is still very hard to be able to discriminate patterns of attack and can't be overly aggressive.

2. What are the differences between intrusion detection and intrusion prevention systems?

   IDS react after the attack has begun where the attack already pass your defense parameter, and IPS is trying to prevent intrusion by more aggressively blocking attempted attack to get in.

3. Explain the four different solutions mentioned to DDoS attacks.

   a) Over-provision the network is trying to have too many servers to be overwhelmed, but it is expensive and unworkable because bot net can be very large.
   b) Filtering attack packets is trying to distinguish the attack packets from regular legitimate packets, which might not be possible.
   c) Slow down processing disadvantages all requestors (legitimate or not), but perhaps disproportionately disadvantages attackers, since attacker sends more packets.
   d) Speak-up solution is requesting additional traffic from all requestors, which assumes that the attacker's bots are already maxed out.

Lecture 73

1. Explain false positive and false negatives. Which is worse?

   False positives are about harmless behavior is misclassified as an attack, where false negatives are about a genuine attack is not detected. Which is worse depends on the scenario, such as what do you want to protect, what do you want to control, how critical your data is, etc.

2. Explain what "accurate" and "precise" mean in the IDS context.

   Accurate means if an IDS system can detects all genuine attacks, where precise mean if it never reports legitimate behavior as an attack.

3. Explain the statement: "It's easy to build an IDS that is either accurate or precise?

   Because if IDS system reporting everything is an attack, then it must be accurate since it detects all genuine attack, but it is not precise, since all legitimate behavior is also reported as an attack. If an IDS system report nothing is an attack, then the system is precise, since no legitimate behavior is mistaken as an attack, but it fails being accurate, since it detects no genuine attacks.

4. What is the base rate fallacy? Why is it relevant to an IDS?

   Base rate fallacy is an error in thinking. If presented with related base rate information and specific information, the mind tends to ignore the former and focus on the latter. In our example, it is relevant to an IDS since if the there are a lot of traffics and the attacks are rare, then you need an very accurate IDS for the system to be useful, even with a 90% detection rate, will have an approximately 92% chance that the raised alarm is false.

Lecture 74

1. What did Code Red version 1 attempt to do?

   Depends on the day of the attack within a month, if the date is between 1st and 19th of the month, it will generate a random list of IP addresses and attempted to infect those machines with the buffer-overflow vulnerability within Microsoft's webservers. On 20th to 28th of the month, Code Red launch a DoS flooding attack on www1.whitehouse.gov, and also the worm defaces some webpages with the words "Hacked by Chinese."

2. Why was Code Red version 1 ineffective?

   Because it used static seed in its random number generator and thus generates identical list of IP address on each infected machine making the spread slowly. And since the flooding attack on the white house was found and failed after website was changed.

3. What does it mean to say that a worm is "memory resident"? What are the implications?

   It means the worm was resides inside the volatile memory of the system, such as RAM. Simply rebooting the infected machines can disinfect the worm.

4. Why was Code Red version 2 much more effective than version 1?

   Because it changed from static seed to a random seed in its random number generator, so different lists of IP addresses were generated on different infected machines. So it had a much greater impact due to sheer volume of hosts infected and probes sent to infect new hosts. Also cause a lot of web device using those IP addresses crashed or rebooted, since they are routers, switches, modems, and printers, which can not handle the load as computer.

Lecture 75

1. How was Code Red II related to Code Red (versions 1 and 2)?

   It exploited the same buffer-overflow vulnerability in Microsoft's IIS webservers as Code Red, and it contains the string "CodeRedII" in the code.

2. Why do you suppose Code Red II incorporated its elaborate propogation scheme?

   Because machines on the same network or subnets (has the same prefix IP address) are likely to be running the similar software, so an infected machines maybe more likely to probe a susceptible machine than machines on unrelated IP address.

3. What did Code Red II attempt to do?

It installs a mechanism for remote, root-level access to the infected machine. This installed “backdoor” allows any code to be executed, so the machines can be used as zombies in a botnet for future attack.

4. Comment on the implications of a large population of unpatched machines.

A large number of machines remained vulnerable to the same or similar attack, so worms will keep circulating since there is enough target to infect. It’s hard to wipe this worm off Internet, as these machines remain unpatched.

5. Comment on the report from Verizon cited on slide 6. What are the lessons of their study?

That most of the successful attacks were related to user ignorance and laziness. Attacker only need to find the weakest link to attack, if we don’t use the tool provided to us, then it is our own responsibility to get infected and has a responsible role in making Internet more vulnerable.

Lecture 76

1. Why is a certification regime for secure products necessary and useful?

Certification standards for security products would help the consumer understand why they need and what they are buying, since most customers don’t have the security expertise to assess the security need or find the proper product.

2. Explain the components of an evaluation standard.

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 the trustworthiness of the evaluated system.

3. Why would crypto devices have a separate evaluation mechanism?

Because the information that needs to use crypto device to protect is much more sensitive than unclassified information for everyday use. Also the standard evaluation does not involve evaluating cryptographic algorithm, which needs to be evaluated for its effectiveness, and needs compliance/conformance testing of its module.

4. Explain the four levels of certification for crypto devices.

a) Level 1: basic security; at least one approved algorithm or function.
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. What is the Common Criteria?

   It is a secure system evaluation criteria adopted by some 26 countries, including the U.S. It comprises the CC documents, CEM (CC Evaluation Methodology), and National Scheme (country-specific evaluation methodologies).

2. What's "common" about it?

   Because it is adopted by some 26 countries with compatible standard, and evaluations (to a certain level) by one signing country are respected by all of the other countries.

3. Why would there be any need for "National Schemes"?

   Because each country has different security requirements and assurance requirements, therefore it needs country-specific evaluation methodology. Also at the very high level of certification, each country will refuse to use CC but their own scheme to protect its own interest.

4. Explain the difference between a protection profile and a security target.

   PP (protection profile) is a document that describes a security policy or set up security requirement for a particular class of systems, is a formal descriptions of security for a class of systems. A security target is a product or a specific system or family of system; it can be evaluated against protection profile.

Lecture 78

1. Explain the overall goal of the protection profile as exemplified by the WBIS example.

   Protect the integrity of the record, detect invalid ID tags, invalid bin-cleared messages and have some fault tolerance.

2. What is the purpose of the various parts of the protection profile (as exemplified in the WBIS example)?

   It is the component of a PP describes in terms of assets, threats, environmental assumptions, security objects and requirements for WBIS. It is saying what needs to be implemented to meet all the security goals and not how to implement.

3. What is the purpose of the matrix on slide 7?

   It is a mapping from threats/assumptions to security objects/requirements. It provides a systematic way of deciding whether threats and assumptions are being addressed by mechanisms and requirements.

Lecture 79

1. Explain the overall goal of the security target evaluation as exemplified by the Sun Identity Manager example.

   To managing user access privileges stored in directory services, and to manage store data of the user, support automatic generation of passwords and specify password quality parameters. Also that all the assumptions are satisfied and threats are counter by mechanism enforce this particular system at the end of day.

2. How do you think that a security target evaluation differs from a protection profile evaluation?

   PP evaluation is about what general policy or model of security policy is needed to implement a particular class of system, it is a collection of document that describes all parts of the policy. It doesn't relate to any specific product, but describes what security means for a particular class of systems.

   A security target is a specific product or system or class of systems submitted for evaluation against protection profile or "fresh" policy. The idea is to specify what security means for this product and how the product enforces that notion of security.

Lecture 80

1. What are the EALs and what are they used for?

   Evaluation Assurance Level (1-7), it defines the care with which the product was developed and the rigor of the evaluation process. It evaluates the amount of evidence you provided for a correspondence between the artifacts you developing and the security model you claiming that implements.

2. Who performs the Common Criteria evaluations?

   Evaluation tests must be performed by an independent organization accredited to perform CC testing. By independent labs who are licensed by the national testing authority with an evaluation fee.

3. Speculate why the higher EALs are not necessarily mutually recognized by various countries.

   Evaluations at EAL5 and above tend to involve the security requirements of the host nation's government, which might be different and confidential by each country.

4. Can vendors certify their own products? Why or why not?

   No. It contradicts with the definition of certification. Evaluation must be performed by independent organizations that are licensed by the national testing authority.

5. If you’re performing a formal evaluation, why is it probably bad to reverse engineer the model from the code?

   It will be too simple and not a good formal (mathematical method) model of security chosen for this evaluation.