Mingu Chang (mc35926)
CS ID: mchang
mc-kpmg@hotmail.com

CS361 Questions: Week 5

Lecture 66

1. What is PGP?
   -"Pretty Good Privacy": strong encryption, using state of the art cryptographic
2. What motivated Phil Zimmerman to develop it?
   - Zimmermann had a strong distrust of the government, and believed strongly that everyone had an absolute right to privacy.
3. Does PGP provide effective security?
   -PGP is very widely used and extremely secure.
4. If PGP is freeware, why would anyone bother to purchase support?
   -a lot of companies do not like to use freeware. they want parties that are available that they can actually call on to get maintenance and that sort of stuff.

Lecture 67

1. Explain the PGP authentication protocol.
   -sender creates a message M, sender generates a hash of M, sender signs the hash using his private key and prepends the result to the message, receiver uses the sender's public key to verify the signature and recover the hash code, receiver generates a new hash code for M and compares it with the decrypted hash code.
2. Explain the PGP confidentiality protocol.
   -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, receiver uses his private key to recover the session key, the session key is used to decrypt the message.
3. How do you get both authentication and confidentiality?
   -apply the authentication step to the original message, and apply the confidentiality step to the resulting message.

Lecture 68

1. Besides authentication and confidentiality, what other " services" does PGP provide?
   - compression, email compatibility, segmentation
2. Why is compression needed?
   -PGP compresses the message, using the ZIP compression algorithm, after applying the signature and before encryption.
3. Why sign a message and then compress, rather than the other way around?

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

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

   -PGP uses radix-64 conversion to map groups of three octets into four ASCII characters. Also appends a CRC for data error checking. Use of radix-64 expands the message by 33%.
5. Why is PGP segmentation needed?

   -PGP automatically segments messages that are too large. This is done after all of the other steps, including radix-64 conversion.

Lecture 69

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

   -Session keys, Public keys, Private keys, Passphrase-based keys
2. What special properties are needed of session keys?

   -Each session key is associated with a single message and used only once. Key size depends on the chosen encryption algorithm E.
3. How are session keys generated?

   -The encryption algorithm E is used to generate a new n-bit key from a previous session key and two n/2bit blocks generated based on user keystrokes including keystroke timing.
4. Assuming RSA is used for PGP asymmetric encryption, how are the keys generated?

   -For new RSA keys, an odd number n of sufficient size is generated and tested for primarily. If it is not prime, then repeat with another randomly generated number until a prime is found.
5. How are the private keys protected? Why is this necessary?

   -The private key is stored encrypted with a user-supplied passphrase. The private key is encrypted using CAST-128 with 128bits of the hash code as key.

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?
   -Send the public key along with the message. Inefficient, since the key might be thousands of bits. Associate a unique ID with each key pair and send that with the message. Would require that all senders know that mapping of keys to ID's for all recipients. Generate an ID likely to be unique for a given user. This is PGP's solution. Use the least significant 64-bits of the key as the ID.
2. What's on a user's private key ring?
   -The private key ring is a table of rows containing: Timestamp, Key ID, public key, private key, User ID
3. What's on a user's public key ring?
   -Public key ring is a table of rows containing: Timestamp, Key ID, Public key, User ID
4. What are the steps in retrieving a private key from the key ring?
   -PGP retrieves receiver's encrypted private key from the private-key ring, using the key ID field in the session key component of the message as an index, PGP prompts the user for the passphrase to recover the unencrypted private key, PGP recovers the session key and decrypts the message.
5. What is the key legitimacy field for?
   -it indicated the extent to which PGP trusts that this is a valid public key for this user.
6. How is a key revoked?
   -can be revoked because compromise is suspected or to limit the period of use of the key

Lecture 71

1. Explain the difference between the consumer and producer problems. Which is more prevalent?
   -the consumer problem: the attacker gets logically between the client and service and somehow disrupts the communication
   -the producer problem: the attacker produces, offers or requests so many services that the server is overwhelmed.
2. Explain syn flooding.
   -example of syn flooding: the transaction may involve some handshake(protocol); the attacker does not respond and the server ties up resources waiting for a response
3. Why are the first three solutions to syn flooding not ideal?

-the problem with increase the size is that each one of these happens connections takes maybe six hundred bites a storage and so there is a limit to how much you can do this; the problem with shorten time is there and that itself is a denial of service attack because slower clients maybe disadvantage because it will timeout before they can ever complete the handshake; filter suspicious is hard thing to do because how do you know when a packet is really legitimate or not.

Lecture 72

1. Why does packet filtering work very well to prevent attacks ?
   -A filter or packet sniffer can detect patterns of identifiers in the request stream and block messages in the pattern.
2. What are the differences between intrusion detection and intrusion prevention systems?
   -IDS can analyze traffic patterns and react to anomalous patterns. However, often there is nothing apparently wrong but the volume of requests. An IDS reacts after the attack has begun.
   -IPS attempts to prevent intrusions by more aggressively blocking attempted attacks. This assumes that the attacking traffic can be identified.
3. Explain the four different solutions mentioned to DDoS attacks.
   -over-provisioning the network, filtering attack packets, slow down processing, "speak-up" solution

Lecture 73

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

-False negatives: a genuine attack is not detected, False positives: harmless behavior is mis-classified as an attack. Which is worse is depend upon the scenario that what you are protecting.

2. Explain what “accurate” and “precise” mean in the IDS cont ext.

-accurate: if it detects all genuine attacks;
-precise: 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?
   -either report everything is an attacker or report nothing is an attack.
4. What is the base rate fallacy? Why is it relevant to an IDS?
   - A perfect IDS would be both accurate and precise: Most intrusion detection systems suffer from the base-rate fallacy.
   -IDS classifies an attack as an attack with probability 90%.
   -IDS classifies a valid connection as attack with probability 10%.

Mingu Chang
(mc35926)
CS ID: mchang
mc-kpmg@hotmail.com

Lecture 74

1. What did Code Red version 1 attempt to do?
   -CodeRed virus began attacking unpatched machines
2. Why was Code Red version 1 ineffective?
   -because of flaws in the design, especially the static seed, CodeRed did very little damage.
3. What does it mean to say that a worm is "memory resident"? What are the implications.
   -The CodeRed worm is memory resident. A machine can be disinfected by simply rebooting it.
4. Why was Code Red version 2 much more effective than version 1?
   -Version 2 had a much greater impact due to the sheer volume of hosts infected and probes sent to infect new hosts.

Lecture 75

1. How was Code Red II related to Code Red (versions 1 and 2)?
   -CodeRED ll is a different worm, exploiting the same vulnerability as CodeRed
2. Why do you suppose Code Red II incorporated its elaborate propogation scheme?
   -CodeRed ll uses a much more sophiscated propagation strategy.
3. What did Code Red II attempt to do?
   -CodeRed ll generates a random IP address and then applies a mask to produce the addresses to probe.
4. Comment on the implications of a large population of unpatched machines.
   -dangerous,
5. Comment on the report from Verizon cited on slide 6. What are the lessons of their study?
   -users often do not patch machines, leaving a population of vulnerable hosts.

Lecture 76

1. Why is a certification regime for secure products necessary and useful?
   -provide a standardized process of independent evaluation by expert teams to provide a certified level of confidence for security products.
2. Explain the components of an evaluation standard.
   -A set for requirements defining security functionality, A set of assurance requirements needed for establishing the functional requirements. A methodology for determining that the funcional requirements are met. A measure of the evaluation result indicating the trustworhiness of the evaluated system.

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

4. Explain the four levels of certification for crypto devices.
   -level 1: basic security; at least one approved algorithm or function
   -level 2: improved physical security;
   -level 3: strong tamper-resistance and countermeasures
   -level 4: complete envelope of protection including immediate zeroing keys upon tampering.

Lecture 77

1. What is the Common Criteria?
   -The Common criteria comprises the CC documents, the CC Evaluation Methodology, country-specific evaluation methodologies called an Evaluation Scheme or National Scheme.
2. What's “common” about it?
   -Evaluation
3. Why would there be any need for “National Schemes”?
   -Evaluation to a certain level by one signing country are respected by all of the others.
4. Explain the difference between a protection profile and a s ecurity target.
   - A PP is a description of a family of products in terms of threats, environmental issues and assumptions, security objectives and requirements of the COmmon Criteria.

   -THE SECUITY TARGET is a document that contains the secuirty requirements of a product to be evaluated and specifies the measures offered by the product to meet those requirements.

Lecture 78

1. Explain the overall goal of the protection profile as exemplified by the WBIS example.
   -The WBIS illustrates the components of a protection profile.
2. What is the purpose of the various parts of the protection profile (as exem-plified in the WBIS example)?
   -Detect invalid ID tags, Detect invalid bin-cleared messages, fault tolerance
3. What is the purpose of the matrix on slide 7?
   -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.
   -O.managedData: store properties of users, O.PasswordGEn: support automatic generation of passwords, O.PasswordQual: specify password quality parameters, OE.Time: the underlying OS provides reliable time.
2. How do you think that a security target evaluation differs from a protection profile evaluation?
   -A security Target is a specific system or class of systems submitted for evaluation. The policy may be specified "fresh" or as previously evaluated protection profiles.

Lecture 80

1. What are the EALs and what are they used for?
   -EAL1: functionally tested, EAL2: structionally tested, EAL3: methodologically Tested and checked, EAL4: methodologically designed , tested and reviewed, EAL5L semiformally designed and tested, EAL6: semiformally verified Design and tested, EAL7: formally verified Designed and tested.
2. Who performs the Common Criteria evaluations?
   -Issuing a CC certification means that the government of the country where the evaluation is performed believes the evaluation was conducted properly. The governments of 26 countries now formally recognize the Common Criteria.
3. Speculate why the higher EALs are not necessarily mutually recognized by various countries.

-In the U.S., only NSA performs testing for EAL5 and higher. A U.S. agency would not accept a certification for EAL5 or above issued by another country.

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

   -Evaluations are performed by independent labs for a fee. The labs 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?

   -because the Evaluation Assurance levels define the care with which the product was developed and the rigor of the evaluation process.

Well done!