Name: Aaron Dishman
UTID: adishman
UTCS: adishman
email: aaron.dishman@utexas.edu

CS361 Questions: Week 5

Lecture 66

1. What is PGP?

   PGP stands for Pretty Good Privacy. It was an attempt by Phil Zimmerman extremely strong encryption system, using state of the art cryptographic algorithms that was easy to use and accessible to all.

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?

   yes it does…even the government has found it difficult to encrypt

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

   maybe because they don't trust a free source that may or may not have included malicious code

Lecture 67

1. Explain the PGP authentication protocol.

   1) Sender creates a message M.
   2) Sender generates a hash of M.
   3) Sender signs the hash using his private key and prepends the result to the message.
   4) Receiver uses the sender's public key to verify the signature and recover the hash code.
   5) Receiver generates a new hash code for M and compares it with the decrypted hash code.
   or:
   S→R : {h(M)}Ks−1, M

2. Explain the PGP confidentiality protocol.

   1) Sender generates a message M and a random session key K.
   2) M is encrypted using key K.
   3) K is encrypted using the recipient's public key, and prepended to the message.
   4) Receiver uses his private key to recover the session key.
   5) The session key is used to decrypt the message.

3. How do you get both authentication and confidentiality?

    Both authentication and confidentiality may be combined for a given message.
    1) Apply the authentication step to the original message.
    2) Apply the confidentiality step to the resulting message.

Lecture 68

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

    only authentication and confidentiality are “services” but it also offers compression, email compatibility, and segmentation

2. Why is compression needed?

    for efficiency and robustness

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

    so that the signature does not depend on the compression algorithm

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

    Encrypted text contains arbitrary 8-bit octets. However, many email systems would choke on certain bit strings they’d interpret as control commands. PGP uses radix-64 conversion to map groups of three octets in to four ASCII characters. Also appends a CRC for data error checking. By default, even ASCII is converted. Use of radix-64 expands the message by 33%. This is usually more than offset by the compression.

5. Why is PGP segmentation needed?

    Email systems often restrict message length. Longer messages must be broken into segments, which are mailed separately. PGP automatically segments messages that are too large. This is done after all of the other steps, including radix-64 conversion.Thus, signature and session key appear only once.

Lecture 69

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

    Session, public, private, passphrase-based

2. What special properties are needed of session keys?

    used once and generated for each new message

3. How are session keys generated?

    Each session key is associated with a single message and used only once. The encryption algorithm E is used to generate a new n-bit key from a previous session key and two n/2-bit blocks generated based on user keystrokes, including keystroke timing. The two blocks are encrypted using E 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?

For new RSA keys, an odd number n of sufficient size (usually > 200 bits) is generated and tested for primality. 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?

1) The user selects a passphrase for encrypting private keys.
2) When a new public/private key pair is generated, the system asks for the passphrase. Using SHA-1, a 160-bit hash code is generated from the passphrase, which is discarded.
3) The private key is encrypted using CAST-128 with 128 bits of the hash code as key. The key is then discarded.

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?

Generate an ID likely to be unique for a given user. Uses the least significant 64-bits of the key as the ID.

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

his own public/private key pairs

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

public keys of correspondents

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

1) 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.
2) PGP prompts the user for the passphrase to recover the unencrypted private key.
3) PGP recovers the session key and decrypts the message.

5. What is the key legitimacy field for?

key legitimacy field indicates the extent to which PGP trusts that this is a valid public key for this user.

6. How is a key revoked?

A user may wish to revoke a public key because:

compromise is suspected, or
to limit the period of use of the key.

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?

    1) the consumer problem : (also called “man-in-the-middle” attack) the attacker gets logically between the client and service and somehow disrupts the communication.

    2) the producer problem : the attacker produces, offers or requests so many services that the server is overwhelmed.

2. Explain syn flooding.

    A SYN Flooding 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.

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

    could consume considerable resources
    might disallow connections by slower clients
    May be hard to determine if the return address does not match the apparent source

Lecture 72

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

    Because you might be able to distinguish the attack packets from regular packets and block the attack packets before they can attack

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

    An intrusion detection system (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.
    An intrusion prevention system (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.

    1) over-provisioning the network—have too many servers to be overwhelmed (expensive and unworkable);
    2) filtering attack packets—somehow distinguish the attack packets from regular packets (may not be possible);
    3) slow down processing—disadvantages all requestors, but perhaps disproportionately disadvantages attackers;
    4) “Speak-up” solution (Mike Walfish)—request additional traffic from all requestors.

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.

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

   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?

   It’s easy because entirely accurate could mean denying everyone, therefore detecting all genuine attacks, as well as legitimate.

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

   The base rate fallacy describes how people do not take the base rate of an event into account when solving probability problems. A 90% accurate IDS would result in many false positives.

Lecture 74

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

   Generate a random list of IP addresses and attempt to infect those machines.
   On 20th to 28th of the month, launch a DoS flooding attack on www1.whitehouse.gov.
   The worm also defaces some webpages with the words “Hacked by Chinese.”

2. Why was Code Red version 1 ineffective?

   The worm uses a static seed in its random number generator and thus generates identical lists of IP addresses on each infected machine.
   Each infected machine probed the same list of machines, so the worm spread slowly.
   The IP address for www1.whitehouse.gov was changed so the DoS attack failed.

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

   Worm resides in RAM. A machine can be disinfected by simply rebooting it.

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

   Because it used a random seed in the random number generator.
   Spread faster, probes sent to different hosts, affected routers, switches, DSL modems, and printers

Lecture 75

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

Also exploits the buffer-overflow vulnerability in Microsoft’s IIS webservers.

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

In order to go undetected for longer period of time

3. What did Code Red II attempt to do?

Installs a mechanism for remote, root-level access to the infected machine. This backdoor allows any code to be executed, so the machines could be used as zombies for future attacks.

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

Could be used as zombies or botnet in a major DDoS attack in the future

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

If people were to update their software regularly, it would be harder for hackers to create large zombie/botnets

Lecture 76

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

provides 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 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.
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 federal government might use them, and they have the highest standards

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, tamper-evident packaging.
Level 3: strong tamper-resistance and countermeasures.
Level 4: complete envelope of protection including immediate zeroing of keys upon tampering.

Lecture 77

1. What is the Common Criteria?

    The need for secure systems evaluation criteria led numerous countries to develop their own. This has largely been replaced by, The Common Criteria , adopted by some 26 countries, including the U.S.

2. What's "common" about it?

    common methods of evaluating the secure-ness of a system

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

    because different countries have different evaluation criteria

4. Explain the difference between a protection profile and a security 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 Security Target is a document that contains the security requirements of a product to be evaluated (TOE), and specifies the measures offered by the product to meet those requirements. It may match a protection profile.

Lecture 78

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

    Protect information that may not be confidential but are still unique such as records that a waste bin was cleared out consisting of bin ID, timestamp, and weight.

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

    Detect invalid ID tags, invalid bin-cleared messages, and fault tolerance.

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

    Illustrates the components of a protection profile.

Lecture 79

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

    Store the properties of users, to support automatic generation of passwords, and to specify password quality parameters.

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.

Lecture 80

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

   There are 7 EALs and are for functionally tested, structurally tested, methodologically tested and checked, methodologically designed, tested and reviewed, semi formally verified design and tested, and formally verified design and tested.

2. Who performs the Common Criteria evaluations?

   The government of the country where the evaluation is performed.

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

   Because to be tested at EAL5/EAL6/EAL7 must have been designed using formal methods. Only NSA performs testing for EAL5 and higher.

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

   If they can it won’t be respected as much as the CC.

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

   It will mess with the process.