FIRSTNAME : Michael;
LASTNAME : Truong;
UTEID : mkt532;
CSACCOUNT : mtruong;
EMAIL : mtruong92@utexas.edu;

CS361 Questions: Week 5

Lecture 66

1. What is PGP?
an email encryption system

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

4. If PGP is freeware, why would anyone bother to purchase support?
a lot of companies don't like to use freeware, they want parties that are available, that they can actually call on to get maintenence

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 geneates 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;
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?
save bandwidth

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;
versions of the compression algorithm behave slightly differently, though all versions are interoperable;
encryption after compression strengthens the encryption, since compression reduces redundancy in the message

4. Explain radix-64 conversion and why it's needed?
a transformation that maps groups of three octets into four ascii characters; many email systems would choke on certain bit strings they'd interpret as control commands

5. Why is PGP segmentation needed?
email systems often restrict message length

Lecture 69

1. What are the four kinds of keys used by PGP?
one-time session symmetric keys, public keys, private keys, passphrase-based symmetric keys

2. What special properties are needed of session keys?
unpredictable session keys must be generated; high entropy

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/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?
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?
the user selects a passphrase for encrypting private keys;
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;
the private key is encrypted using cast-128 with 128 bits of the hash code as key. the key is then discarded;
the entire security of the system depends upon your private key being kept private, and so you don't want to just store it on your disk, because then an attack who can subvert the protections on your disk can get your 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?
send the public key along with the message;
associate a unique id with each pair and send that with the message;
generate an id likely to be unique for a given user

2. What's on a user's private key ring?
a table of rows containing timestamp, key id, public key, private key, user id

3. What's on a user's public key ring?
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?
indicates the extent to which pgp trusts that this is a valid public key for this user

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?
the consumer problem: the attacker gets logically between the client and service and somehow disrupts the communcation;
the producer problem: the attack produces, offers or requests so many services that the server is overwhelmed;
the producer problem

2. Explain syn flooding.
an attacker forges the return address on a number of syn packets. the server fills its table with these half-open connections. all legitimate accesses are denied until the connections time-out

3. Why are the first three solutions to syn flooding not ideal?
increase the server's queue size: could consume considerable resources, the attacker can just send more requests;
shorten the time-out period: might disallow connections by slower clients;
filter suspcious packets: may be hard to determine

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 that pattern

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 hte 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.
over-provisioning the network: have too many servers to be overwhelmed (expensive and unworkable);
filtering attack packets: somehow distinguish the attack packets from regular packets (may not be possible);
slow down processing: disadvantages all requestors, but perhaps disproportionately disadvantages attackers;
"speak-up" solution (mike walfish): request additional traffic from all requestors

Lecture 73

1. Explain false positive and false negatives. Which is worse?
false positive: a genuine attack is not detected;
false negative: harmless behavior is mis-classified as an attack;
false positives

2. Explain what “accurate” and “precise” mean in the IDS context.
accurate: if an intrusion detection system detects all genuine attacks;
precise: if an intrusion detection system never reports legitimate behavior as an attack;

3. Explain the statement: “It’s easy to build an IDS that is either accurate or precise?
accurate: report everything as an attack
precise: report nothing as an attack

4. What is the base rate fallacy? Why is it relevant to an IDS?
since the attacks are relatively rare in the population, you get a lot of false positives;
an ids must be very accurate or suffer from the base rate fallacy, an ids with too many errors becomes useless

Lecture 74

1. What did Code Red version 1 attempt to do?
if date is between 1st and 19th of hte month, 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.
a machine can be disinfected by simply rebooting it

4. Why was Code Red version 2 much more effective than version 1?
code red version 2 uses a random seed in the random number generator

Lecture 75

1. How was Code Red II related to Code Red (versions 1 and 2)?
the code contains the string "coderedii" which became the name

2. Why do you suppose Code Red II incorporated its elaborate propogation scheme?
probably to set up a botnet later on

3. What did Code Red II attempt to do?
when the worm infects a new host, it first determines if the system has already been infected;
if not, the worm initiates its propagation mechanism, sets up a "backdoor" into the infected machine, becomes dormant for a day, and then reboots the machine;
begins a process of propogating itself

4. Comment on the implications of a large population of unpatched machines.
there's this huge population of unpatched machines out there which are vulnerable to these worms and so that means that they're going to keep circulating because they have a vulnerable population in which to circulate

5. Comment on the report from Verizon cited on slide 6. What are the lessons of their study?
we're really lousy about patching our machines and we should do better because the result is that it makes internet much more vulnerable because we got all these machinese out there that are susceptible to attack

Lecture 76

1. Why is a certification regime for secure products necessary and useful?
certification standards for security products would help the consumer understand what they need and what they're buying

2. Explain the components of an evaluation standard.
a set of requirements defining secruity 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?
different levels of confidentiality require different levels of certification

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?
a common set of standards for evaluation

2. What's "common" about it?
adopted by some 26 countries, including the u.s.

3. Why would there be any need for "National Schemes"?
different countries have different needs

4. Explain the difference between a protection profile and a security target.
protection profile: a set of implementation-independent security requirements for a category of products or systems
security target: set of security requirements to be used as the basis of evaluation

Lecture 78

1. Explain the overall goal of the protection profile as exemplified by theWBIS example.
detect invalid id tags;
detect invalid bin-cleared messages;
fault tolerance

2. What is the purpose of the various parts of the protection profile (as exemplified in the WBIS example)?
illustrates the components of a protection profile, it provides a systematic way of deciding whether threats and assumptions are being addressed by mechanisms and requirements

3. What is the purpose of the matrix on slide 7?
this gives you a systematic way of determining whether the mechanisms that you're proposing are adequate to solve the problems that are presented

Lecture 79

1. Explain the overall goal of the security target evaluation as exemplified by the Sun Identity Manager example.
to say that these are the kinds of requirements that you have to have for the system, a rationale and a summary of how their system actually counters the threats and guarantees that the assumptions are in fact satisfied; the idea is to specify what security means for this product and how the product enforces that notion of security

2. How do you think that a security target evaluation differs from a protection profile evaluation?
a security target evaluation specifies what security means for this product and how the product enforces that notion of security;
a protection profile evaluation doesn't relate to any specific product, but describes what security means for a particular class of systems

Lecture 80

1. What are the EALs and what are they used for?
evaluation under the common criteria; evaluation assurance levels (1-7) define the care with which the product was developed and the rigor of the evaluation process

2. Who performs the Common Criteria evaluations?
independent labs licensed by the national testing authority test up to eal4, in the u.s., only nsa performs testing for eal5 and higher

3. Speculate why the higher EALs are not necessarily mutually recognized by various countries.
higher EALs are difficult to verify by other countries to ensure trustworthiness

4. Can vendors certify their own products? Why or why not?
no; vendors could certify their own products with the highest eal to increase marketability

5. If you're performing a formal evaluation, why is it probably bad to reverse engineer the model from the code?
You want the model to reflect what the security policy should be, not just whatever the code happens to do.

Well done!