Name: Vincent Nguy

EID: vn2863

CS Login: vn2863

Email:nguyvincent@yahoo.com

**CS361 Questions: Week 5**

# Lecture 66

1. What is PGP?

PGP( Pretty Good Privacy) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication.

1. 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.

1. Does PGP provide effective security?

Yes. In 2003, an incident involving seized Psion PDAs

belonging to members of the Red Brigade indicated that

neither the Italian police nor the FBI were able to decode

PGP-encrypted ﬁles stored on them.

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

Companies would like the help of support for efficacy.

# 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.

S →R : {h(M)}Ks^(-1), M

1. Explain the PGP confidentiality protocol.

PGP provides encryption for messages sent or stored as files. Sender generate 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.

S->R : {K}kr, {M}k

1. 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.

1. Why is compression needed?

Encryption after compression strengthens the encryption, since compression reduces redundancy in the message.

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

So that the signature does not depend on the compression algorithm.

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

It map groups of three octets into four ASCII characters. Also a CRC for data error checking. It expands the message by 33%

1. Why is PGP segmentation needed?

For messages that are too large.

# Lecture 69

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

Session keys, Public keys, Private keys, Passphrase-based keys.

1. What special properties are needed of session keys?

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

1. 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.

1. 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 primarily. If it is not prime, then repeat with another randomly generated number, until a prime is found.

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

The private key is stored encrypted with a user-supplied passphrase.

# 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.

1. What’s on a user’s private key ring?

Timestamp: when the key pair was generated.

Public Key: public portion of the key.

Private Key: the private portion, encrypted using a passphrase.

Key ID: 64 least significant digits of the public key

User ID: usually the user’s email address.

1. What’s on a user’s public key ring?

Timestamp: when the entry was generated.

Key ID: 64 least significant digits of this entry.

Public key: the public key for the entry.

User ID: identifier for the owner of this key. Multiple IDs may be associated with a single public key.

1. 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.

1. What is the key legitimacy field for?

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

1. How is a key revoked?

The owner issues a signed key revocation certificate.

# Lecture 71

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

The consumer problem: ( also called “man-in-the-middle” attack) the attacker gets logically between the 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.

The consumer problem is more relavent.

1. Explain syn flooding.

The transaction may involve some handshake (protocol); the attacker does not respond and the server ties up resources waiting for a response.

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

Increase server queue size. Consumes considerable resources.

Shorten the time-out period. Might disallow connections by slower clients.

Filter suspicious packets. If the return address does not match the apparent source discard the packet. 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. Ingress filtering means sniffing incoming packets.

1. 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.

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

Over-provisioning the network – have too many servers to be overwhelmed.

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?

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.

False negatives: a genuine attack is not detected.

False positives: harmless behavior is miss-classified as an attack. Which do think is a bigger problem?

1. 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.

1. Explain the statement: “It’s easy to build an IDS that is either accurate or precise?

You would have to have really strict detection to catch every attack but never miss hit a legitimate behavior.

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

The IDS classifies an attack as an with probability 90%.

The IDS classifies a valid connection as attack with probability 10%.

# 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. Launch a DoS flooding attack on www1.whitehouse.gov The worm also defaces some webpages wih the words “Hacked by Chinese.”

1. Why was Code Red version 1 ineffective?

Each infected machine probed the same list of machines, so the worm spread slowly.

1. 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. Once-rebooted, the machine remains vulnerable to repeat infection.

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

It used a random seed in the random number generator. This had a major impact: more than 359,000 machines were infected with CodeRed (version 2) in just fourteen hours.

# Lecture 75

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

Code Red II had the string “CodeRedll” which became its name.

1. Why do you suppose Code Red II incorporated its elaborate propogation scheme?
2. What did Code Red II attempt to do?

It 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.

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

The virus will keep circulating since there is a large population of unpatched machines

1. Comment on the report from Verizon cited on slide 6. What are the lesson s of their study?

People are just lazy in not wanted to patch there machines.

# Lecture 76

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

Most customers are not experts in security so the certification regime evaluates products for you.

1. Explain the components of an evaluation standard.

A set of requirements define security functionality.

A set of assurance requirements needed for establishing the functional requirements.

A methodology for determining that the requirements are met.

A grading system.

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

It would help the consumer understand what they need and what they’re buying.

1. Explain the four levels of certification for crypto devices.
2. Basic security; at least one approved algorithm or function.
3. Improved physical security, tamper-evident packaging.
4. Strong tamper-resistance and countermeasures
5. Complete envelope of protection including immediate zeroing of keys upon tampering.

# Lecture 77

1. What is the Common Criteria?

A set of documents and methods of Evaluation.

1. What’s “common” about it?

It is adopted by some 26 countries.

1. Why would there be any need for “National Schemes”?

Each country has their own specific problems.

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

A protection profile is a formal descriptions of security for a class of systems; a security target is a specific system or family of systems.

# Lecture 78

1. Explain the overall goal of the protection profile as exemplifiedby the WBISexample.

Identify the threats, know your Assets, and develop Security Objectives and Requirements for the type.

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

The idea is to specify what security means for this product and how the product enforces that notion of security.

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

It has the threats on the Columns and Security objectives on rows. You can map out how many threats are being addressed in your system.

# Lecture 79

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

Specify what security means for this product and how the product enforces that notion of security.

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

Security target is an instance of a protection profile. i.e. windows fire wall to fire walls in general.

# Lecture 80

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

Evaluation under the Common Criteria targets a speciﬁed level of rigor. The vendor provides assurance that the corresponding rigor was applied during development and test.

1. Who performs the Common Criteria evaluations?

The government of the country where the evaluation is performed believes the evaluation was conducted properly.

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

The respect of the certificate is only in “good faith”

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

No. can’t trust them to do that ☺.

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

Attackers can decode and learn ways to hack your product.

Well done!