Norman E. Lopez
UTEID: nel349
CSACCOUNT: nel349
email: noell.lpz@utexas.edu

Lecture 66

1. What is PGP?

Is a type of encryption. Pretty Good Privacy. Uses the best available cryptographic algorithms as building blocks

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 Based on algorithms with extensive public review.
Public key encryption: RSA, DSS, Diffie-Hellman.
Symmetric encryption: CAST-128, IDEA, and 3DES.
Hash coding: SHA-1.

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

The commercial version satisfies businesses needing vendor support.

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.

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?

1.Apply the authentication step to the original message.
2 Apply the confidentiality step to the resulting message.

Norman E. Lopez
UTEID: nel349
CSACCOUNT: nel349
email: noell.lpz@utexas.edu

Lecture 68

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

- Compression
- Email compatibility
- Segmentation

2. Why is compression needed?

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

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?

using as digits "A–Z", "a–z", "0–9", plus two more characters, often "+" and "/". Use of radix-64 expands the message by 33%.

5. Why is PGP segmentation needed?

Email systems often restrict message length. Longer messages must be broken into segments, which are mailed separately.

Lecture 69

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

Session keys: used once and generated for each new message
Public keys: used in asymmetric encryption
Private keys: also used in asymmetric encryption
Passphrase-based keys: used to protect private 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?

Key size depends on the chosen encryption algorithm E. 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?

Norman E. Lopez
UTEID: nel349
CSACCOUNT: nel349
email: noell.lpz@utexas.edu

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?
Whenever the user wants to access the private key, he must supply the passphrase. Since the 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?

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?

Timestamp: when the key pair was generated.
Key ID: 64 least significant digits of the public key.
Public key: the public portion of the key.
Private key: the private portion, encrypted using a passphrase.
User ID: usually the user's email address. May be different for different key pairs.

3. 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.

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?

Indicates the extent to which PGP truststhat this is a valid public key for this user.

6. How is a key revoked?

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.

Norman E. Lopez
UTEID: nel349
CSACCOUNT: nel349
email: noell.lpz@utexas.edu

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. In producer problem the attacker producess, offers or request so many services that the server is overwhelmed.

2. Explain syn flooding.

The volume of requests may overwhelm the server. The transaction may involve some handshake or 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?

There will be no significant impact on solving the problem since the attacker will attempt to overflow the server's queue size. It will consume the servers resources.

If shortening the time-out period it is likely that legitimate clients might get disconnected from a server without good probable cause.

It might take longer to determine if to filter the suspicious packets, therefore will consume a high amount of resources.

Lecture 72

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

filtering out illegal requests or maybe not. The important thing is that you are reducing the chances of a typical DoS flooding attack.

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

The IDS(Intrusion Detection System) reacts after the attack has begun. Detects high volumes of requests or any unusual patterns.

Ths IPS(Intrusion Prevention System) reacts before the attack by being more aggressively blocking attempted attacks. Assumes that the 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 but may not be possible.

slow down processing - disadvantages all requestors. Server reputation may go bad. but also disadvantages attackers.

"speak up" -- request additional traffic from all requestors.Walfish's solution assumes that the attacker's bots are already maxed out.

Lecture 73

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

False negative: a genuine attack is not detected.

Norman E. Lopez
UTEID: nel349
CSACCOUNT: nel349
email: noell.lpz@utexas.edu

False positive: a legitimate behavior is classified as an attack but is not.
Depends on the scenario.

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

Accurate means that it detects all of the genuine attacks. Precise is responsible for never reporting legitimate behavior as an attack.

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

You can have a system which is accurate meaning that it will block everything including legitimate behavior but not precise. In the other case the IDS is precise but genuine attacks go through the filter.

4. What is the base rate fallacy? Why is it relevant to an IDS? From all the detected malicious packages a small percentage is really malicious. It is important to predict this base rate fallacy in order to know if your system is working correctly.

Lecture 74

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

Launch a DoS flooding attack on www1. whitehouse.gov by infecting computers with some ip addresses then make flooding attack to www1. whitehouse.gov.

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. the operating system is not permitted to swap them out to a storage device; they will always remain in memory.

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

Version 2 had a much greater impact on global infrastructure due to the sheer volume of hosts infected and probes sent to infect new hosts. Also infected additional devices with web interfaces: routers, switches, DSL modems, and printers.

Lecture 75

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

Exploits the same vulnerability.n Microsoft's IIS webservers.

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

Norman E. Lopez
UTEID: nel349
CSACCOUNT: nel349
email: noell.lpz@utexas.edu

The largest the number of infections it would be easier to propagate. Unlike the previous code Red I needed to avoid being memory resident so that it would not be eliminated by the machine.

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.

The chances of propagations are higher. The virus can survive longer.

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

People don't update the patches.

Lecture 76

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

Most customers don't have the expertise to perform these steps effectively.

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?

Approximately 150 vendors of cryptographic modules have had independent labs perform compliance/conformance testing of their modules.

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?

It is a security system evaluation criteria shared by some 26 countries. It comprises the CC documents, the CC Evaluation Methodology , and country-specific evaluation methodologies called and Evaluation Scheme or National Scheme.

Norman E. Lopez
UTEID: nel349
CSACCOUNT: nel349
email: noell.lpz@utexas.edu

2. What's "common" about it?

Evaluations (to a certain level) by one signing country are respected by all of the others.

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

Every nation handles security at different levels of suspicion.

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

evaluations of protection profiles (PP), a set of implementation-independent security requirements for a category of products or systems

evaluations of products or systems against a security target(ST).

Lecture 78

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

To protect assets from threats

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

OT.Inv1: detect invalid ID tags
OT.Inv2: detect invalid bin-cleared messages
OT.Safe: 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.

Managing user access privileges stored in directory services.

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

The Security Target is a document that contains the security requirements of a product to be evaluated.

Norman E. Lopez
UTEID: nel349
CSACCOUNT: nel349
email: noell.lpz@utexas.edu

Lecture 80

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

Evaluation under the Common Criteria that specifies the level of rigor.

2. Who performs the Common Criteria evaluations?

The governments of 26 countries.

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

Most of the countries have independent suspicions about particular threats. Not necessarily all the threats involve every country.

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

No, tests must be performed by an independent organization accredited to perform CC testing. It does not make sense for vendors to self-certify as they could ignore important threats that could hurt customers.

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

It uses mathematical methods such as prime number factorization which could become inefficient to decode or impossible.