Adan Cortez

AC42886

Lecture 66

1. What is PGP?

Pretty good privacy or "the closest you're likely to get

military-grade encryption."

2. What motivated Phil Zimmerman to develop it?

Zimmerman has a strong distrust of the government and believed

that everyone had an absolute right to privacy.

3. Does PGP provide effective security?

Yes. In several incidents, the government had significant trouble

trying to decrypt any PGP-encrypted files.

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

Freeware doesn't have the personel support and maintenance that

paid support has.

Lecture 67

1. Explain the PGP authentication protocol.

The sender creates a message M and generates a hash of M and

signs the hash with his private key and prepends it the result

to the message. The receiver can use the public key to verify

and recover the hash and can verify that the hash is correct

by hashing M.

2. Explain the PGP confidentiality protocol.

Sender generates a message M and a random session key K. M is

encrypted using K and K is encrypted using the recipient's

public key and prepended to the message. Receiver uses his

private key to recover the session key K and uses K to decrypt

the message.

3. How do you get both authentication and confidentiality?

You can apply the confidentiality step to the result of the

authentication step with the original message.

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?

Signing the message first is preferable so that the signature

does not depend on the compression algorithm.

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

The radix-64 maps groups of three octets into four ascii characters

in order to prevent any mail systems to interpret bit strings as

control commands.

5. Why is PGP segmentation needed?

Email systems often restrict message length so segmentation allows

for messages that are too long to be broken into smaller pieces.

Lecture 69

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

Session keys, public keys, private keys, and passphrase-based keys.

2. What special properties are needed of session keys?

The session keys should be random appearing and not guessable.

3. How are session keys generated?

The session keys are generated by using a previous session key

and teo n/2-bit blocks generated based on user keystrokes, including

keystroke timing. The blocks are encrypted using an encryption

algorithm and the previous key to form a new key.

4. Assuming RSA is used for PGP asymmetric encryption, how are the

keys generated?

The keys are generated by finding an odd number n and testing n

for primality. If n is not prime then repeat with another randomly

generated number until one is found.

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

The private keys are protected by having the user select a passphrase

for encrypting private keys. The passphrase is hashed and used as

the key for encrypting the private key. The private key protection

is necessary to prevent attackers from being able to directly

access the keys from just accessing the storage.

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?

PGP generates an ID that uses the least significant 64-bits of

the key as the ID and sends the ID along with the message.

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

Timestamp, Key ID, public key, private key, and User ID.

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

Timestamp, Key ID, public key and User ID.

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

PGP retrieves the 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. It then prompts the user

for a passphrase to recover the unencrypted private key and

recovers the session key and decrypts the message.

5. What is the key legitimacy field for?

The key legitimacy field indicates the extent to which PGP trusts

that the user's public key ring is a valid public key.

6. 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 do you think would be more prevalent?

The consumer problem is where the client is not able to contact

the server for services because the attacker is intercepting

all messages between the two and halting communication.

The producer problem is where the server is overwhelmed by

requests to where legitimate clients cannot access the service

given by the server.

The producer problem is more prevalent.

2. Explain syn flooding.

The attacker floods the server by sending many forged SYN packets

with fake return address. This causes the server to fill up its

table with half-open connections which denies legitimate accesses

until the connections time out.

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

The first solution takes up more resources and doesn't solve the

issue of receiving fake SYN packets as the attacker could just

send more.

The second solution could time out slower clients and lock out

legitimate users.

The third solution is hard to implement as gauging whether an

address is legitimate based on the return address is difficult.

Lecture 72

1. How well does packet filtering work to prevent attacks?

Not well. Hard to discriminate patterns of attacks from patterns

of usage.

2. What are the differences between intrusion detection and intrusion

prevention systems?

Intrusion detection reacts after the start of an attack by analyzing

your traffic pattern and reacting to anomalous patterns. Intrusion

prevention attempts to block attempted attacks.

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

Over-provisioning the network attempted to solve DDoS by having

more servers than possible to be overwhelmed by the attacker.

Filtering packets attempts to stop DDoS by distinguishing attack

packets from regular packets and discarding the attack packets.

Slow down processing to disadvantages everyone and hopefully

disproportionately disadvantages attackers more.

The speak up solution has the server request more information

from all requesters in the hopes that the attacker is already

maxed out and can't respond.

Lecture 73

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

A false positive is when it reports legitimate behavior as an

attack. A false negative is when a genuine attack is not detected.

A false negative is far worse in comparison in my opinion.

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

An accurate system means it detects all genuine attacks while a

precise system means 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 to report everything as an attack or nothing as an

attack but it's hard to find the spot where only an actual

attack is reported as an attack.

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

Base rate fallacy is where the user begins to ignore alarms

when many attacks are raised as a false positive.

An IDS can become useless if it succumbs to base rate fallacy

and reports too many false positives.

Lecture 74

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

Attempt to infect as many machines as possible during a time

period and after that period, launch a DoS flooding attack

on www1.whitehouse.gov.

2. Why was Code Red version 1 ineffective?

The worm used a static seed for the IP address generator and thus

infected the same machines constantly which made spreading it

slow. The IP address for www1.whitehouse.gov was also changed so

the DoS attack failed.

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

are the implications.

The worm only stays in memory and not on permanent storage.

The machine can be disinfected just by simply rebooting it.

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

The static seed issue was replaced with a random seed which allowed

for a far wider spread of infection.

Lecture 75

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

Both code reds exploit the same buffer overflow vulnerability

in Microsoft's IIS webservers.

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

propogation scheme?

Machines on the same network or subnet are likely to be running

similar software so it targets most of the time, an IP address

that is similar to the infected machine.

3. What did Code Red II attempt to do?

Code Red II installed a mechanism for remote, root-level access

to the infected machine that allowed 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 worm will continue to circulate since there are so many

machines that are unpatched.

5. Comment on the report from Verizon cited on slide 6. What are

the lessons of their study?

People are really bad at keeping their machine up to date.

Lecture 76

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

useful?

Most customers don't have the expertise to assess needs to

determine requirement, identify the product that will meet

those requirements and purchase the product to deploy it.

2. Explain the components of an evaluation standard.

A set of requirements defining security functionality for its

purpose. A set of assurance requirements needed for establishing

the functional requirements to determine level of assurance from

the product. A methodology for determining that functionality

requirements are met. A measure of the evaulation result

to indicate the truthworthiness of the evaluated system.

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

Cryptology is a fairly sensitive area and there aren't as many

crypto experts as the other security areas so there are special

documents that describe the evaluation of crypto modules.

4. Explain the four levels of certification for crypto devices.

Level one provides basic security that uses at least one

approved algorithm. Level two has improved physical security

with tamper-evident packaging. Level 3 has strong tamper-

resistance and countermeasures. Level 4 has a complete

envelope of protection including immediate zeroing of keys

upon tampering.

Lecture 77

1. What is the Common Criteria?

A set of documents and evaluation methodology for applying the

criteria with some country specific evaluation methodology.

2. What’s “common” about it?

Evaluations graded to a certain level by one signing country

should be accepted and respected by all the other countries.

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

At a certain level, countries may have additional requirements

they deem necessary for their use case.

4. Explain the difference between a protection profile and a

security target.

A protection profile is formal descriptions of security for a class

of systems. The security target is a specific system or family

of systems.

Lecture 78

1. Explain the overall goal of the protection profile as exemplified

by the WBIS example.

Record that a waste bin was cleared and the correct information

was recorded for that waste bin.

2. What is the purpose of the various parts of the protection profile

(as exemplified in the WBIS example)?

The various parts identify the assets, envrionmental assumptions,

threats, and security policy.

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

The matrix is used to map threats and assumptions to requirements

and objectives.

Lecture 79

1. Explain the overall goal of the security target evaluation as

exemplified by the Sun Identity Manager example.

The goal is to manage user access privleges stored in directory

services.

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

a protection profile evaluation?

Protection profile is an abstract set of goals a system has to

meet, and the security target is an evaluation of how an

implementation of that system meets those abstract goals.

Lecture 80

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

EALs are evaluation assurance levels and they are meant to

identify how rigorously a vendor provided assurance for

their product.

2. Who performs the Common Criteria evaluations?

The governement or a certifying agency.

3. Speculate why the higher EALs are not necessarily mutually

recognized by various countries.

Different countries can't trust their highly classified

information based on another country's assurance evaluation.

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

Vendors cannot self certify their own product due to a

conflict of interest.

5. If you’re performing a formal evaluation, why is it probably

bad to reverse engineer the model from the code?

Reverse engineering the model from the code may also reverse

engineer a bug into the model if the code has a bug.