Name: Amanda Liem
EID: al34232
CS Login: aliem
Email: amandaliem94@yahoo.com

Lecture 66
1. What is PGP?

PGP is a cryptographic algorithm developed by Phil Zimmermann, with the goal of providing strong encryption to everyone. It is easy to use and freely available to everyone.

2. What motivated Phil Zimmerman to develop it?

He wanted to give everyone strong encryption, and make it easily accessible.

3. Does PGP provide effective security?

Yes, it is quoted as “the closest you’re likely to get to military-grade encryption.

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

Commercial businesses can use the vendor support.

Lecture 67
1. Explain the PGP authentication protocol.

First, the message is hashed. That hash is then signed with the sender’s private key. This is sent to the receiver with the actual message in plaintext. This way, the receiver can make sure that the sender’s public key can decrypt the hashed message, and then hash the plaintext message to make sure that the message was not tampered with in any way.

2. Explain the PGP confidentiality protocol.

The sender can generate a random session key to encrypt a message with. To send this random session key to the receiver, they encrypt it with

the receiver’s public key. The receiver can then receive the encrypted
message and the encrypted session key, then decrypt the session key
with their private key, and then decrypt the message itself.

3. How do you get both authentication and confidentiality?

Apply the authentication step to the original message, and then
apply the confidentiality step to the resulting message.

Lecture 68
1. Besides authentication and confidentiality, what other “services” does PGP provide?

Compression, Email compatibility, and Segmentation.

2. Why is compression needed?

It’s not needed, it’s used to make the system more robust and efficient.
It also make the encryption more secure by reducing 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, Versions of the compression
algorithm behave slightly differently, though all versions are interoperable.
Also, encryption after compression strengthens the encryption, since
compression reduced redundancy in the message.

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

radix-64 maps groups of three octets into 3 ascii characters. It also
appends a CRC for data error checking. This is so that email systems
don’t accidentally misinterpret an encrypted 8-bit octet as a control
command.

5. Why is PGP segmentation needed?

Because Email systems often restrict message length.

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?

It must be a symmetric key, which is n bits long based on the previous session key.

3. How are session keys generated?

It's generated using the previous session key and then 2 n/2-bit blocks that are generated based on user keystrokes (like timing). An encryption algorithm is used on the 2 blocks using the previous key.

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

A prime number of > 200 bits is generated. It takes around 70 tries to find a prime in this range.

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

It is protected with a passphrase. The actual key is not stored, and must be generated every time using the 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?

There are several methods that could be used, but one used for PGP is to generate an ID likely to be unique for a given user. They use the least significant 64 bits of the key as the ID.

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

A timestamp (when the key ring pair was generated), a Key ID (64 least

significant digits of the public key), the Public key (public portion
of the key), private key (the private portion of the key, encrypted
using a passphrase), and the User ID – usually the user's email
address.

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

A table of other people's public keys and key IDs – whom they are sending
messages to, or receiving messages from.
A timestamp, Key ID (least significant digits of this public key), the
public key, and User ID

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

It uses the Key ID in the session key component of the message as an index,
then asks the user for the passphrase to decrypt the private key.

5. 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.

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 is more prevalent?

The consumer problem has to do with the consumer not being able to communicate
with the server, while the producer problem has to do with the server not
being able to handle as many requests as it is given. Server attacks are more
prevalent.

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. Consequently, all
legitimate accesses are denied until the connections time-out.

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

1) It would consume considerable resources
2) It would disallow connections by slower clients

Lecture 72
1. Why does packet filtering work very well to prevent attacks?

Because the filter 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?

IDS reacts after the attack has begun, while the intrusion prevention system
attempts to block attempted attacks.

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

over-provisioning the network: you have too many servers to be overwhelmed
filtering attack packets - somehow distinguish the attack packets from
regular packets
slow down processing - disadvantage attackers
“Speak-up” solution - request additional traffic from all requestors

Lecture 73
1. Explain false positive and false negatives. Which is worse?

A false negative - not being able to catch the attack.

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

accurate: the intrusion detection system detects all genuine attacks
precise: 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?

Well if you classify everything as an attack (which is easy), you are accurate.

But if you never classify anything, you are precise. Both are not very impressive
by themselves.

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

You focus on the first presented information, and over/ underestimate a
scenario. In IDS, you overestimate the effectiveness of a system that claims
a certain percentage of accuracy.

Lecture 74
CS361 Questions: Week 5 3
1. What did Code Red version 1 attempt to do?

bring down service of the website www1.whitehouse.gov

2. Why was Code Red version 1 ineffective?

It used a static seed, so once you changed the ip address of the machine/
website, it no longer worked.

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

The virus lives in virtual memory, so cannot survive a reboot.

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

It used a random seed for its random number generator for ip addresses.

Lecture 75
1. How was Code Red II related to Code Red (versions 1 and 2)?

It exploited the same buffer-overflow vulnerability in Microsoft’s IIS
webservers.

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

To spread itself to as many machines as possible.

3. What did Code Red II attempt to do?

install a mechanism for remote, root level access to the infected machine.

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

They will largely get infected, and it will spread quickly.

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

That preventing viruses is very doable, if people were proactive about protecting their machines.

Lecture 76

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

Because people sometimes can’t assess for themselves what type and level of security they need.

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?

Crypto needs a specific requirement set.

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 secure systems evaluation criteria used by 26 countries, which contains
CC documents, CC Evaluation Methodology, and an evaluation scheme.

2. What's "common" about it?

It is shared by many countries, and they agree on certain evaluations
together.

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

Nations could have different requirements for evaluations.

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

protection profiles are a set description of a family of products in terms
of threats, environmental issues and assumptions, security objectives, and
requirements of the Common Criteria. A security target is a document that
contains the security requirements of a product to be evaluated.

Lecture 78
1. Explain the overall goal of the protection profile as exemplified by the WBIS example.

A protection file seeks to outline what the goals of a particular type
of security product should be.

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

To cover various aspects of the security product.

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

To make sure that each threat/ assumption is covered by a corresponding
objective/requirement.

Lecture 79
1. Explain the overall goal of the security target evaluation as exemplified by the Sun Identity Manager example.

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?

There are different kinds of requirements.

Lecture 80
1. What are the EALs and what are they used for?

They are levels used to specify the level of rigor the product was tested
under.

2. Who performs the Common Criteria evaluations?

The government of the country giving out the certification.

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

Countries could have different ideas of security, or are developed to
different levels.

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

No – that would be potentially biased, or plain out used for corruption.

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

It’s much easier to miss a fatal feature if you write the model based
on what you already have.

Well done!