Name:Tehreem Syed
EID:tfs385
CS Login:fatima
Email:tehreemsyed@utexas.edy

Lecture 66
1.
What is PGP?
PGP stands for pretty good privact. It was a program designed by Phil Zimmerman to encrypt email traffic using the best encryption algoithms out there and package them nicely in such a way that they can be easily accessible to general people.
2.
What motivated Phil Zimmerman to develop it?
Zimmerman has a strong distrust of the government and strongly believed that everyone had absolute right to privacy.
3.
Does PGP provide effective security?
Yes, it does.

4.
If PGP is freeware, why would anyone bother to purchase support?
For companies that want to use PGP, they want something reliable to use. Buying the software enables them to have a track record and for legal purposes they can use it when needed.

Lecture 67
1.
Explain the PGP authentication protocol.
This is a digital signature function.
Sender creates a message.
SHA-1 (or DSS/SHA-1) is used to generate a 160-bit hash code of the message.
The hash code is encrypted with RSA using the sender's private key and the result is prepended to the message.
The receiver uses RSA with the sender's public key to decrypt and recover the hash code.
The receiver generates a new hash code for the message and compares it with the decrypted hash code.

2.
Explain the PGP conÞdentiality protocol.
PGP provides encryption for messages sent or stored as files.The protocol is as follows:
The sender generates a message and a random 128-bit session key (used for this message only).
The message is encrypted using CAST-128 (or IDEA or 3DES) with the session key.

The session key is encrypted with RSA, using the recipient's public key, and prepended to the message.
The receiver uses RSA with his private key to decrypt and recover the session key.
The session key is used to decrypt the message.
3.
How do you get both authentication and conÞdentiality?

Both authentication and confidentiality may be combined for a given message aas follows:
Sender generates a signature for the plaintext message and prepends it to the message.
The plaintext message plus signature is encrypted.
The session key is encrypted using RSA and prepended to the message.

Lecture 68
1. Besides authentication and conÞdentiality, what other ÒservicesÓ does PGP provide?
It provides compression, email compatibility and segmentation. These are not "really" services and more so provide efficiiency and robustness.

2. Why is compression needed?
Compression is needed to save bandwidth on a large message.

3. Why sign a message and then compress, rather than the other way around?
It is done in this order because:

1.It is preferable to sign an uncompressed message so that the signature does not depend on the compression algorithm.
2.Versions of the compression algorithm behave slightly differently, though all version are interoperable.
3.Encryption after compression strengthens the encryption, since compression reduces redundancy in the message.

4. Explain radix-64 conversion and why itÕs needed?
PGP always involves encryption. Encrypted text contains ar
bitrary 8-bit octets. However, many email systems would choke on certain
bit strings they'd interpret as control commands.PGP uses radix-64 conversion to map groups of three octets into four ASCII characters. Also appends a CRC for data error
checking. By default, even ASCII is converted.Use of radix-64 expands the message by 33%. This is usually more than offset by the compression.

5. Why is PGP segmentation needed?
Email systems often restrict message length. Longer messag
es must be broken into segments, which are mailed separately.

Lecture 69

1.

What are the four kinds of keys used by PGP?

They are:

1.session keys
2. Public keys
3.private keys
4. Pass-Phrase base keys for storing 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?

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?

For new RSA keys, an odd number n of sufficient size (usually>
200 bits) is generated and tested for primality. If it is not p
rime,then repeat with another randomly generated number, until a
prime is found.Primes appear in the neighborhood of n about every
ln(n) =lge(n) numbers. Since we can exclude even numbers, to find a prime of around 200 bits, it takes about ln(2200)/2 = 70 tries.

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

The private keys are protected using pass-phrases.The private key is stored encrypted with a user-supplied passphrase in order to make it more secure. The entire security depends on you keeping your private key protected.

CS361 Questions: Week 5

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?

Given that a user may have multiple public/private key pairs, he could know by the following:

1.Send the public key along with the message.Inefficient, since the key might be thousands of bits.

2.Associate a unique ID with each key pair and send that with the message.Would require that all senders know thatmapping of keys to ID's for all recipients.

3.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.This is used by the receiver to verify that he has such a key on his "key ring." The associated private key is used for the decryption.

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

It has a timestamp, key ID , public key, priavte key, user ID.

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

It has key ID , public key , User ID

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

5. What is the key legitimacy field for?

Associated with each public key in the user's public key ring is a key legitimacy field that indicates the extent to which PGP trusts that this is a valid public key for this user.

Legitimacy is determined from certificates and chains of certificates, the user's assessment of the trust to be assigned to the key, and various heuristics for computing trust.

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?

David Gresty at Liverpool John Moore's University decomposes DoS attacks into two groups:

1.the consumer problem: (also known as the ``man-in-the-middle'' attack) the attacker gets logically between the client and service and somehow disrupts the communication.\\[1ex]

2.the producer problem: the attacker produces, offers or requests so many services that the server is overwhelmed.

Producer problem is more prevalent.

2. Explain syn ßooding.

A SYN Flooding attack happens when an attacker forges the return address on a number of SYN packets. The server fills its table with these half-open connections.

3. Why are the Þrst three solutions to syn ßooding not ideal?

Th first one is not deal because for increasing sevrer's queue size we will have more half open connections which are pretty huge liek around 66 bytes of stroage. So it still consumes considerable resources.

The second one has a problem because it could involve in denial of service to slower clients.

Teh third one is problematic because how do we determine which packet is suspicious and which is not. The criteria determination is pretty hard.

Lecture 72

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

I think it does not.

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

Intrusion detection assumes that the attack is in side the wall and something needs to be done about it. Intrusion prevention assumes that the attack should neever get in the wall at all.

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.

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

1.over-provisioning the network—have too many servers to be overwhelmed (expensive and unworkable);

2.filtering attack packets—somehow distinguish the attack packets from regular packets (may not be possible);

3.slow down processing—disadvantages all requestors, but perhaps disproportionately disadvantages attackers;

4.“Speak-up” solution(Mike Walfish)—request additional traffic from all requestors.

Lecture 73

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

There are two types of errors when considering any intrusion detection system.

False negatives:a genuine attack is not detected.False positives:harmless behavior is mis-classified as an attack.

It depends on what you are protecting and what you want to keep secure.

2. Explain what ÒaccurateÓ and ÒpreciseÓ mean in the IDS context.

An intrusion detection system is:
accurate:if it detects all genuine attacks
precise:if it never reports legitimate behavior as an attack.

3. Explain the statement: ÒItÕs easy to build an IDS that is either accurate or precise?

Either report aeverything as an attack or reports nothing is an attack and that sis easy, They difficult part is having both in a blend.

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

The issue is that on a typical system you have lots of traffic coming in on the network and they are all not malicious. They are rare events. Since the attack are relatively rare you get lots of false positoves.

If you have an IDS in place, it must be very accurate or you'll soon turn it off because almost all of your alarms will be false alarms.

If you have a fairly right result there are still chances of false postives.

Lecture 74

CS361 Questions: Week 5

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

On July 12, 2001, the CodeRed virus began attacking machines running unpatched versions of Microsoft's IIS webserver. Works as follows:

If date is between 1st and 19th of the 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?

It was not effective because:

Because of flaws in the design, especially the "static seed", CodeRed did very little damage.The CodeRed worm is memory resident. A machine can be disinfected by simply rebooting it.Once-rebooted, the machine remains vulnerable to repeatinfection, likely since each newly infected machine probes thesame list of IP addresses.

3. What does it mean to say that a worm is Òmemory residentÓ? What are the implications.

It means the it resided in the volatile memory of teh machine and you just had to r eboot but then yous tood the chance of reinfected because you were likely to be on that list which was generated over and over again,

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.

Lecture 75

1.How was Code Red II related to Code Red (versions 1 and 2)?
It had the string codered in it.

2.Why do you suppose Code Red II incorporated its elaborate propogation scheme?
To overwhlem the servers.

3.What did Code Red II attempt to do?

4.Comment on the implications of a large population of unpatched machines.
People did the study found that depending on the country the number of machines were patched. So there is ahuge ppulation of unmatched machines out there who are vulnerable to these worms.

5.Comment on the report from Verizon cited on slide 6. What are the lessons of their study?
We are really lousy about patching out machines because it makes our internet vulnerable to these worms.

Lecture 76

1. Why is a certiÞcation regime for secure products necessary and useful?
It is necessary and useful for most customers dont have the xpertise to perform these steps effectively.

2. Explain the components of an evaluation standard.
Security functionality that you would llike it to have.An evaluation standard provides the following:
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?
Because they are more important than other devices.

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

These are levels of certification for cryptographic 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?
Set of dicmuments and methodology for applying the criteria and implementing it. So they have national schedmes and evaluation schemes which are country specific. Evaluations by one country should be acceptable by another country at a certain level.

2. WhatÕs ÒcommonÓ about it?
The commonality is having being common in all countroies.

3. Why would there be any need for ÒNational SchemesÓ?
In order to take care of danger f attacks in that country.
4. Explain the difference between a protection proÞle and a security target.

Security target plicy that is set of security requirement ti be ysed as the basis of evaluation.
There are two types of evaluations under the CC.
1.evaluations of protection profiles (PP), a set of implementation-independent security requirements for a category of products or systems;
2.evaluations of products or systems against a security target (ST).

Lecture 78

1. Explain the overall goal of the protection profile as exempliÞed by the WBIS example.
OT.Inv1: detect invalid ID tags
OT.Inv2: detect invalid bin-cleared messages
OT.Safe: fault tolerance

This is just a definition for a class of security systems.

2. What is the purpose of the various parts of the protection proÞle (as exem.pliÞed in the WBIS example)?

You are nto saying what particular mechanism are tehre but what systems youneeed in order to do it.

3. What is the purpose of the matrix on slide 7?
If you fill in teh matrix with security objective to counter a threat or fill in a n objective and there is an x then you know that all of the threats have some counter mechanism for them and some assumptions have validation with the .

Lecture 79
1. Explain the overall goal of the security target evaluation as exempliÞed by the Sun Identity Manager example.
SUn enumerated the set of theats and now have to say how they might havehbene counterede.

2. How do you think that a security target evaluation differs from a protection proÞle evaluation?
A Security Target is a specific system or class of systems
submitted for evaluation.
The policy may be specified "fresh" or as previously evaluated
protection profiles.
The idea is to specify what security means for this product
and how the product enforces that notion of security.

Lecture 80
1. What are the EALs and what are they used for?
Evaluation Assurance Level is the person submits either the protection profile or security target and specifies how much evidence they put forward tht the evalation is actually taken care of.

2. Who performs the Common Criteria evaluations?
All the countries recoginize common criteria upto a certain level but then beyond that level it may not recognize it. The governmetn.
3. Speculate why the higher EALs are not necessarily mutually recognized by various countries.
Its highly secure information and NSA or other authorities dont recognize that much information from other countries.

4. Can vendors certify their own products? Why or why not?
It can be done by the vendors. But it mor eleft on good faith.
There are cases of overmarketing.
5. If ouÕre performing a formal evaluation, why is it probably bad to reverse engineer the model from the code?
If you build a system , you claim that I will make it secure by reverse engineering the product then it is not a good approach to security.

Well done!