Name: Yun Wen Chen
EID: dc27863
CS Login: dchen
Email: dianachen@utexas.edu

Lecture 66

1. What is PGP?

PGP stands for "Pretty Good Privacy". It is a collection of strong, high-power cryptographic algorithms, packaged together conveniently in a way that is easy to use for an average, everyday user.

2. What motivated Phil Zimmerman to develop it?

Zimmerman had a strong distrust for the government. The government discouraged the use of strong cryptographic algorithms because they didn't want people to encrypt their incriminating files. In addition, if someone were to encrypt their files, the government wanted to be able to decrypt it.

3. Does PGP provide effective security?

It would seem so, as with the cases of the FBI, United States Government, and the Italian Police not being able to decrypt some of the files encrypted with PGP.

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

There are many ways to tamper with freeware, and the version that a person downloads may not be a legitimate PGP. People buy support so they don't need extensive knowledge of the software, and are still able to get assistance maintaining their system.

Lecture 67

1. Explain the PGP authentication protocol.

The sender creates a message M.
The sender generates a hash of M, h(M).
The sender signs the has using its private key, adds it before the message. $\{h(M)\}_{Ks}^{-1}$, M
The receiver receives $\{h(M)\}_{Ks}^{-1}$, M
The receiver uses the sender's public key to verify its signature and get the hash code h(M).
The receiver generates a new hash code for M and compares it with the decrypted hash code.

In summary, the sender sends the intended message M as is, as well as the hash value of M signed with its private key. The receiver will know it is that particular sender because when it decrypts the hash value using the sender's public key, the hash value will be the same as the receivers calculated hash value on M.

2. Explain the PGP confidentiality protocol.

The sender generates a message M and a random session key K.
M is encrypted using key K. $\{M\}_K$
K is encrypted using the receiver's public key, and is added before the message. $\{K\}_{Kr}^{-1}$, $\{M\}_k$.
The receiver will use its private key to recover the session key. $\{\{K\}_{Kr}^{-1}\}_{Kr} = K$
The session key K is used to decrypt the message M.

In summary, a message is encrypted by a random session key. That session key is encrypted by the receivers public key, so that only the receiver may decrypt the session key, and use the session key to decrypt the message.

3. How do you get both authentication and confidentiality?

The authentication protocol contains the digital signature of the sender, but also contains the plaintext in the clear. However, the confidentiality protocol encrypts the message with a key, and encrypts the key with the receiver's public key so that only the receiver can decrypt. When you encapsulate the authentication protocol within the confidentiality protocol, you get both authentication and confidentiality.

Lecture 68

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

Compression, email compatibility, and segmentation.

What is compression needed?

Compression is needed to save bandwidth. You want to make your message as small as possible when sent over the internet.

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

You don't want your digital signature to depend on the compression algorithm.

Though different versions of compression algorithms may produce the same result, they may behave differently. Thus you don't want to accidentally tamper with your digital signature by first compressing your message, then signing the value in which the receiver's decryption algorithms may not understand.

Explain radix-64 conversion and why it's needed?

Encrypted text contains arbitrary 8-bit octets that email systems would interpret as control commands. The radix-64 conversion maps a group of 3 octets to 4 ASCII characters so that email servers don't experience this confusion.

Why is PGP segmentation needed?

Some emails are too large, and thus need to be sent in segments. The PGP breaks a message into pieces that mail servers can handle, and then reconstructs them when they arrive to the receiver.

Lecture 69

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

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

2. What special properties are needed of session keys?

Session keys are associated with a single message and can only be used once.

3. How are session keys generated?

Given an encryption algorithm E, E generates a new n-bit session key using a previous session key and two n/2-bit blocks generated from user keystrokes. User keystrokes and user keystroke timing are used to generate two n/2-bit blocks. These two blocks are encrypted with a previous session key, then with the encryption algorithm E, and combined to form the new key.

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

An odd number of sufficient size (> 200 bits) is generated. If the number is prime, then it is the key. If the number is not prime, this step is repeated until a prime number is found.

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

Private keys are encrypted by the hash value of a user-supplied passphrase. The entire security of the system depends on the private key. As a result, a user shouldn't store their private key on their computer in plaintext because if the computer becomes compromised, an attacker would easily retrieve the plaintext private key.

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?

Along with the message, the sender may generate an ID likely to be unique for a given user. The key ID for the PGP is the least significant 64-bits of the public key. Though there may be some collisions, it will be much more effective than looking through all of a user's public keys.

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

Timestamp - when the key pair was generated.
Key ID - least significant 64-bits of public key.
Public key - public portion of the key.
Private key - private portion of the key encrypted with a passphrase.
User ID - typically a user's email address.

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

Timestamp - when the entry was generated.
Key ID - least significant 64-bits of the 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?

Given that a user R receives a message encrypted with K_R:

- PGP retrieves R's encrypted private key from the private-key ring, using the key ID in the session key component of the message.
- PGP prompts user for passphrase to retrieve unencrypted private key.
- PGP retrieves session key to decrypt message.

5. What is the key legitimacy field for?

A key legitimacy field is a value that is associated with the level of trust PGP has for the particular key as a valid public key for the user.

6. How is a key revoked?

The owner of the key signs a key revocation certificate and distributes it to its desired recipients. The recipients, in turn, are expected to update their public-key rings.

Lecture 71

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

The consumer problem is when the attacker gets logically between the client and the service and disrupts communication whereas the producer problem is when the attacker is trying to impersonate many clients to overwhelm the server with requests or offers.

2. Explain syn flooding?

Syn flooding occurs when an attacker intentionally does not respond to a server request, keeping an open connection and overwhelming the server with these half-open connections. Suppose an attacker sends a SYN packet to a server, which allocates space in an internal table and sends an ACK back to the attacker saying that it has received the SYN packet. Suppose then, that the attacker does not respond to the server with an ACK. As a result, the connection between the server and thee attacker will stay half open until the connection times out, or the server finally receives and ACK from the attacker. With enough of these attacks, the server will fill its internal table with half-open connections, denying access to all the legitimate users until the forged connections time out.

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

The first idea is not ideal because it would take significantly more resources, and the attacker can just send more requests.

The second idea is not ideal because there might be legitimately slower clients.

The third idea is not ideal because it may be hard to determine whether a packet is suspicious and it would impede commerce between the server and legitimate users.

Lecture 72

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

If you can filter out the packets that are malicious or illegal, then they never establish connection with the server, and would not be able to consume any of the server's resources.

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

In an intrusion detection, the system analyzes traffic patterns and reacts to anomalous ones. However, at that point, the attack has already begun. In intrusion prevention, the system aggressively attempts to block malicious traffic. However, at this point, the system would have to know which requests are malicious.

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

Over-provision the network. That is, to have too many servers for an attack to overwhelm. This is expensive and unworkable.

Filter attack packets. That is, to distinguish between attack packets and regular packets. However, the attacker would definitely try their hardest to make sure that attacks are indistinguishable from normal packets.

Slow down processing. However, it disadvantages everyone, including legitimate clients.

"Speak-up" solution. Request additional traffic from all requestors. This is because the people sending you packets from botnet probably can't send you anymore packets because they are maxed out. However, legitimate packets belong to legitimate users who can probably send you additional packets.

Lecture 73

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

A false positive is when a legitimate behavior is mis-classified as an attack. A false negative is when malicious behavior is not detected.

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

Accurate means it detects all genuine attacks with no false negatives. Precise means it never reports legitimate behaviors, meaning no false positives.

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

It is easy to build an intrusion detection system that is accurate, meaning it detects all genuine attacks without any false negatives, or precise, meaning it never reports legitimate behaviors, meaning no false positives. However, the difficulty comes in building a system that is both accurate and precise, meaning that there are no false positives or false negatives. In other words, it is difficult to build a system that will not only detect all attacks, but also not mis-classify legitimate behavior as malicious.

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

The base-rate fallacy is having an IDS system having too many false positives. That is, because the detection rate is so high, it is constantly identifying legitimate behavior as malicious. This is relevant to an IDS because if there are too many false positives, the system becomes useless and ineffective.

Lecture 74

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

Code Red version 1 attempted to take control of Microsoft's IIS web servers. That is, it tried to use its buffer-overflow vulnerability to allow system-level exception of code, something that applications should not have the privileges for.

2. Why was Code Red version 1 ineffective?

The worm used a static seed, meaning that the generated IP lists used to infect machines were identical across infected machines.

The worm spread slowly because the infected machines had the same generated IP lists, thus they all attacked the same list of machines.

The DoS attack failed when the IP address for www1.whitehouse.gov was changed.

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

Memory resident means that a machine can be disinfected by rebooting it. That is, the worm lies in volatile memory, which is not preserved when the machine shuts off or is rebooted. However, this means that the machine is vulnerable to be infected multiple times, which is more than likely because the list generated by the worm was identical across all infected machines.

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

Code Red version 2 used a random seed in the random number generator. This means that the generated list of IP address between infected computers were not identical. Therefore, it was able to infect many more computers and proliferate vastly. In addition, the Code Red worm crashed or rebooted multiple web interfaces during it's attempt to send a copy of the worm. Even if the worm wasn't sent, it disrupted the hardware of many computers, indirectly causing a DoS attack.

Lecture 75

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

Code Red II was still trying to exploit the buffer-overflow vulnerability in Microsoft's IIS webservers. The writer of Code Red II used the string "CodeRedII", which later became its name.

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

Some of the time, Code Red II generated random IP addresses to direct their attack. However, most of the time, Code Red II used part of the current IP address, with added additional bits. This was because machines with the same prefix typically belonged to the same subnet or part of the internet and it was more likely that the machines on that subnet were running the same software. Therefore, if a machine on the subnet is infected, there is a better chance of infecting other machines on the subnet. As a result, Code Red II could reach out to a new internet area with its random IP generator, as well as infect that particular subnet with it's prefix-generated IP addresses.

3. What did Code Red II attempt to do?

Code Red II attempted to install a backdoor on the machines it has infected. Because Code Red II was not memory resident, rebooting a machine would not get rid of Code Red II. The backdoor allows for any code to be executed, which would allow for future attacks.

4. Comment on the implications of a large population of un-patched machines.

Un-patched machines make the internet a much more dangerous place, because they allow for these worms to propagate. Though it may seem like patched machines are safe, it may be that these patched machines may communicate with un-patched machines and become infected or infiltrated in a different way.

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

Verizon's study indicated that 9 out of 10 attacks took advantage of a vulnerability that could have been fixed by a patch six months prior.

Lecture 76

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

Because a customer trying to acquire security does not necessarily have the expertise to determine what their security goals are, what security products would meet those requirements, and how to properly purchase and deploy the security products.

2. Explain the components of an evaluation standard.

A set of requirements defining security functionality lays out the set of requirements that you would like a system to have in various contexts.

A set of assurance requirements are the policies for these functionality requirements.

A methodology is a systematic way to evaluate a security system for these functionality and assurance requirements.

A measure of the evaluation is basically a grade that reflects the trustworthiness of the system in question.

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

Crypto devices have a separation evaluation mechanism because there are not that many experts in that area. Because of the mathematical theories involved in cryptography, it is a sensitive area that needs additional expertise.

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

Level 1 is basic security, requiring only one approved cryptographic algorithm, and can be typically found in everyday home use.
Level 2 is improved physical security, with temper-evident packaging so that the owner can see if someone broke into the box.
Level 3 has counter measures in addition to an already strong tamper-resistance.
Level 4 is a complete envelope of protection, typically embedded in a packing that zeros out the keys once someone tries to tamper with it. This belongs more with government security needs.

Lecture 77

1. What is the Common Criteria?

The Common Criteria is a set of documents and a methodology for applying the criteria in a secure system evaluation for non-cryptographic security systems.

2. What's "common" about it?

It is shared between 26 countries, including the US. These countries agreed on a standardized criteria because often security systems have to take into account communication with other countries.

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

National Schemes are country specific, and may comply on a more specific level with the country's laws that it may not share with other countries.

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

A security target is a set of security requirements to be used for an evaluation. This is what you would test your product on to see how well the product fulfills these set of requirements. A protection profile is almost like a proposed set of security requirements, that can be evaluated and given a grade based on how well it fulfills security policies. Therefore, a developer or a company trying to implement a security system for a particular context can use the protection profile as a guideline for his implementation.

Lecture 78

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

The overall goal of the protection profile by the WBIS example is to protect the weight information of trash bins from being tampered with.

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

Assets - this describes what a security system is supposed to be trying to protect. In WBIS, this means the ID of the trans bin, the timestamp in which it was dumped, and the weight of the trash that was dumped.

Environmental assumptions - lay out some of the assumptions of this particular context of the protection profile. In WBIS, the environmental assumptions include that there is a tag attacked to all the waste bins, the crew is trustworthy, and the system is protected and backed up regularly.

Threats - threats lay out potential attacks on the system. In WBIS, it could be that an attacker destroys the tag or corrupts/interferes with the transmission of weight data from the scale into the information storage system.

Security Objectives - are some of the policies of the security system that could help uphold its goals. In WBIS, detection of invalid ID tags or invalid bin-cleared messages would make sure that the correct weight is being recorded with the correct bin ID. Fault tolerance would keep the records of these weights from being lost or destroyed.

Security Requirements - are the general mechanism requirements that would satisfy the goals of the security system. In WBIS, FDP_ITT.1 or, internal transfer integrity protection, is a requirement that upholds the goal of protecting the weight data from an attacker trying to tamper with it as it travels from the scale to the information storage device.

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

The purpose of the matrix on slide 7 is to systematically ensure that for this protection profile, all the proposed threats have a mechanism (in the form of security objectives and requirements) that can counter than and all the proposed assumptions in the security context have a mechanism that can validate the system. In general, the goal is to make sure that all your assumptions are justified and all the threats can be dealt with or eliminated with the security objectives and or requirements.

Lecture 79

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

The overall goal of the security target evaluation is to decide if Sun's Java System Identity Manager can properly manage user access privileges. In other words, Sun's system aims to make sure that the correct user can execute their privileged instructions and nothing else.

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

Protection profile evaluation typically pass when they are logically sound. In other word, if a protection profile makes sense in theory, then it will pass. A security target evaluation has to actually satisfy a set of requirements. Therefore, if a security product is supposed to work in theory, but has technical vulnerabilities, whether it be with the implementation, the messages that that attacker can see, or how its functionality affects any state that can be observed, it does not pass. An example would be that for authentication, a user would enclose their private key in a message encrypted by the receivers public key. Though in theory, that is a great way to let the receiver know the sender's identity, we have discovered that there are many ways that an attacker can derive the sender's private key from simply observing the messages passed between users, depending on the type of implementation of this idea.

Lecture 80

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

EALs are the levels of intensity that a product is evaluated. EAL1 checks to see if the product is functionally effective, whereas EAL7, the highest rigor, checks to see if the design of the product, as well as the functionality of the product is effective and upholds the policies.

2. Who performs the Common Criteria evaluations?

For lower levels, Common Criteria evaluations are done by independent labs certified by NIST (National Institute of Standards and Technology). For higher levels, Common Criteria evaluations are done by the NSA.

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

A reason why some security systems would want to be more evaluated more rigorously could be because they need to cater to a highly sensitive asset. Typically, these assets are government associated. Therefore, a country wouldn't trust another country to verify a security system used on its own assets. For example, if Country A evaluated a secure system with EAL7 and found a backdoor, it could approve the EAL7 evaluation, distribute the product to other countries, and be able to gain access to their systems.

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

No. Malicious vendors could "say" their product has passed an EAL evaluation, and infect machines. Regular vendors may not have enough perspective to thoroughly test their products, or they may lie as well in order to gain market advantage.

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

Because you have to use formal mathematical methods, and the model might not be very representative.