Lucas Harrison
LMH2538
lucash
harrisonlucas@utexas.edu

CS361 Questions: Week 5

Lecture 66

1. What is PGP?

It's a pretty good privacy cryptographic protocol designed to allow average people to take advantage of known cryptographic protocols.

2. What motivated Phil Zimmerman to develop it?

His distrust in giving the government an all access pass to every email from every person in a country. He wanted an easily accessible, strong cryptographic solution that would protect people's data.

3. Does PGP provide effective security?

Yes it does. It provides the very important aspects of confidentiality and integrity.

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

Companies purchase a cheap commercial version in order to have uniformity accross their network and when something goes wrong, they have someone to call and be accountable other than themselves. That way they don't have to staff a technician to deal with that kind of stuff.

Lecture 67

1. Explain the PGP authentication protocol.

The sender creates a message and a hash of the message. The sender encrypts the hash using thier private key and prepends the message to that encrypted part. Then they send it. The reciever has the message then and uses the sender's public key to decrypt the hash and compare the messages.

2. Explain the PGP confidentiality protocol.

The sender generates a random key. Then he encrypts the message using this key. Then he encrypts the key with the reciever's public key. Then when the reciever gets the message he can use his private key to unlock the session key which can then be used to decrypt the message.

3. How do you get both authentication and confidentiality?

You can achieve both by combining the two previous steps.

Lecture 68

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

Compression, email compatibility, and segmentation are also provided.

2. Why is compression needed?

To save bandwidth when sending messages.

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

Because you don't want the signature to depend on the compression algorithm.

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

Because some of the random binary strings that came in 8bit octets were being interpreted as commands by the email software. By converting it to 4 ascii characters, you avoid this problem.

5. Why is PGP segmentation needed?

In order to break up messages that might be too large for typical email providers to handle or interpret correctly.

Lecture 69

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

Session, public, private, and passphrase.

2. What special properties are needed of session keys?

They should have a high entropy and be unpredicatable. Randomness is good.

3. How are session keys generated?

Take the previous session key and generate a new key to encrypt that with using keystroke timing and movements of the mouse to provide enough randomness.

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

By generating two large primes that aren't easily guessable.

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

They're protected via the passphrase keys. It's necessary because if the private key is comprimised, the whole goal of PGP is wasted. By making the passphrase key be needed everytime you want to access the private key, you add an extra security layer making the system more reliable on the whole.

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?

They send an ID that is likely to be unique. They use the last 64 bits of the public key as an identifier so the reciever knows who sent it.

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

It stores thier own public/private key pairs. Each entry has a timestamp, key ID, public key, private key, and user ID.

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

The keys of people you want to communicate with. Each entry has a timestamp, key ID, public key, and user ID.

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

You type in your passphrase key, that's hashed and then used to decrypt your private key.

5. What is the key legitimacy field for?

It represents how strongly PGP trusts that this is a valid public key for that user.

6. How is a key revoked?

The user who owns a public key issues a signed key revocation certificate that advises people to discontinue use of that public key. Then, users are expected to update their public key rings.

Lecture 71

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

For consumer attacks, the attacker gets in between consumer and producer and disrupts the communication. For producer attacks, the attacker overwhelms the producer by requesting so many services, the producer can't keep up and can't handle legitimate requests. The producer problem is far more prevalent because you don't have to know

anything about the consumer.
2. Explain syn flooding.

An attacker issues connection requests to a server with fake return addresses. The server addresses these requests as it would any other connection. However, since they are fake return addresses, there is never going to be a connection established. So the server has many half open connections that time out eventually when no connection can be made but in the meantime, the server is filled with these and cannot accept real legitimate connection requests.
3. Why are the first three solutions to syn flooding not ideal?

The first solution creates more overhead by consuming resources, but the attacker could just issue more connections. The second, discriminates legitimate, but slow users. The third may not be strict enough to have an impact or may be too strict that you throw away legitimate requests.

Lecture 72

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

It works by noticing patterns in packets and discarding them. This works because in order to DDoS, the attacker has to send a lot of requests to overwhelm the server. These packets could be filtered and prevent the attack.
2. What are the differences between intrusion detection and intrusion prevention systems?

IDS analyzes the traffic patterns and notices anomalys. Once identified, the IDS can react. However, this reaction can only occur after the attack has begun. IPS, attempts to prevent intrusion by aggresively analyzing incoming packets in order to block the attack completely.
3. Explain the four different solutions mentioned to DDoS attacks.

Over-provisioning is having too many servers to be taken down. This is too expensive to be useful. Filtering attack packets is difficult because its very hard to distinguish malicious packets. Slow down processing disadvantages all requestors uniformly. Speak up solution operates under the assumption that attackers are already maxed out in sending requests. By increasing the legitimate user's requests, the percentage of non malicious packets goes up.

Lecture 73

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

False positive is when a legitimate behavior is classified as an attack. False negative is when an attack is undetected. I think false negatives are worse because then an attack goes unnoticed and when you expect everything to be working normally, it may not be.
2. Explain what “accurate” and “precise” mean in the IDS context.

Accurate means there are no false negatives. Precise means there are no false positives.
3. Explain the statement: “It’s easy to build an IDS that is either accurate or precise?

You can make overreaching protocols to have either accuracy or precision. You could assume everything is an attack and never miss one and be accurate. Or you could assume nothing is an attack and never mistake a legitimate behavior as an attack and be precise.
4. What is the base rate fallacy? Why is it relevant to an IDS?

There is math out there that shows that since the attacks are relatively rare, you

get a lot of false positives. This is relevant because even at a high detection accuracy of 90%, an IDS system could have 92% false positve rate which isn't very helpful.

Lecture 74

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

It attempted to infect other machines via random IP's or DDoS'd whitehouse.gov.

2. Why was Code Red version 1 ineffective?

The worm's "random" list of IP's to attempt to infect used a static seed in the random number generator and actually generated identical lists of IP addresses on each infected machine. Also, once the IP of whitehouse.gov was changed, the DDoS was ineffective.

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

Since it resided in the volitile memory of your machine, you just had to reboot and it would go away.

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

Because it actually had a random seed for the random number generator so it's random list of IP's to attempt to infect was generated, it was different each time.

Lecture 75

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

Only in that the writer of code red two knew about the first two versions and used the string Code Red II in it.

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

Because it realized that by copying part of the prefix of the current IP, you would be looking to infect computers on the same subnet of the internet (perhaps the same company or school) and would have more success since it is likely they would be running the same software.

3. What did Code Red II attempt to do?

It installed a mechanism for root level access that could be used for later attacks.

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

The evolution of Code Red demonstrates the implications. The first attack was relatively harmless, the second one a little more advanced, and the third one even still more advanced. They all used the same vulnerability. If the attacks had been even more malicious, a lot of things could have gone wrong. If they had simply patched, none of the evolving code would have been possible.

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

Same as above. If the patches take so long, you open the door for very sophisticated and harmful attacks to be devoloped and propogated.

Lecture 76

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

It allows the ignorant consumer to make a more educated decision on which security product they should buy for their desired purposes.

2. Explain the components of an evaluation standard.

A set of requirements defining security functionality, a set of assurances needed to

esablish functional requirements, a method for demonstrating these functional requirements are met, and a way to measure the end result which indicates the trustworthiness of a system.

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

Because they have more requirements that need to be met in order to considered trustworthy.

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

Level 1 is simple, basic security. Level 2 is this plus physical tamper-evident packaging. Level 3 has strong tamper resistance and measures to counter potential tampering. Level 4 has complete bubble of protection and immediate zeroing of keys upon tampering.

Lecture 77

1. What is the Common Criteria?

Its an agreed upon criteria that is used for evaluating secure systems.

2. What's "common" about it?

The common criteria documents and evaluation methodology for applying that criteria.

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

To add an increased level of evaluation or maybe to test functionality that is more specific to how that country runs.

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

Protection profiles are a description of a family of products in terms or threats, security objectives, etc. These are used to help classify what is expected of a firewall, for example, based on the common criteria. Once certain things are provided, you can call your product a firewall. Security targets are documents that contain the security requrirements of a product to be evaluated.

Lecture 78

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

The overall goal is to make sure the WBIS operates as intended. By stating assumptions, possible threats, security objectives, and security requirements, the PP allows the this class of products to eventually be implemented in a secure fashion.

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

The purpose is to identify all aspects of the problem. By assessing threats, and demanding certain aspects of security be in place, the PP allows the eventual creation of a product that is certified via the common criteria as being able to securely accomplish the original goal.

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

It gives a systemmatic way to determine if the mechanisms your're proposing is adequate enough to address all the potential threats out there and if the assumptions you're making are reasonable in the sense that they have a security mechanism validating that assumption.

Lecture 79

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

The overall goal is to demonstrate how no unauthorized users would be on your system. Threats, such as user's having weak passwords, were assessed and countered by security mechanisms from the common criteria such as requireing passwords to be a certain length and contain non alpha characters.

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

The ST evaluation differs in that the actual implementation details of how to deal with threats are included and only attempting to reach a certain EAL level of security. The PP evaluation simply assesses the risks and potential threats and assumptions that need to be addressed in order for the class of systems to operate securely.

Lecture 80

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

They are used to demonstrate how rigorously a system has been evaluated and can be confidently called secure to a certain degree.

2. Who performs the Common Criteria evaluations?

NIST manages this process in the USA. The product vendors themselves can't be trusted to do this and instead need independent organizations to do this.

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

Because the verification is very difficult and there is mutual distrust between various countries. Enough so that there is no reason to be careless enough to agree that they have a security system of EAL 7.

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

No they cannot because that would be a conflict of interest and doesn't establish a trustworthy evaluation.

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

Because you need to be able to formally prove the final product performs as intended.