CS361 Intro to Computer Security Daniel Rosenwald
Young, Bill July 11th, 2014

EID: dpr447
CS login: randose
Email: danielrosenwald@gmail.com

Week 5

Lecture 66

1. A packaging of high powered cryptographic algorithms created by Phil Zimmerman that is easily usable by the general public.
2. Zimmerman had a distrust of the government and wanted to create e-mail encryption so the government couldn't intercept messages.
3. Yes, it is extremely hard to crack even by the FBI.
4. Companies would buy the package because a lot of the times they want the on-hands support that you can't get from freeware.

Lecture 67

1. The hash of the message is encoded and then at the receiving end it's compared to make sure the sender is who they say they are.
2. The sender encrypts the message with a random session key, encrypts the session key, and the receiver decrypts the session key and then decrypts the message with it.
3. To get both, you simply combine these two protocols.

Lecture 68

1. PGP also provides compression, compatibility, and segmentation.
2. It's done to reduce bandwidth.
3. Because you don't want the signing to depend on the compression algorithm.
4. Radix-64 turns every 24 bits into 4 ASCII characters, which eliminates the misinterpretation of octets by some email systems.
5. If messages are too long, it breaks them up, sends them separately, and then reassembles them on the other end.

Lecture 69

1. Session keys, public keys, private keys, and passphrase-based keys.
2. Session keys must be used only once and they must be random.
3. They are generated by using the previous key and manipulating it with data collected by movement of the mouse and keystroke timing.
4. They are generated by randomly guessing, excluding even numbers, until you find a prime.
5. The private key is encrypted with a passphrase that you generate. It's necessary to maintain the integrity of the system.

Lecture 70

1. Generate an ID likely to be unique for a given user.

2. Timestamp, Key ID, Public key, Private key, User ID.
3. Timestamp, Key ID, Public key, User ID.
4. You type in your passphrase, it's hashed, and then the private key gets used by PGP.
5. It's a measure of how strongly I believe the key belongs to who I think it is, similar to certificates.
6. The owner simply issues a signed key revocation certificate.

Lecture 71

1. The consumer problem comes about when the attacker gets in the middle of your transaction, while the producer problem happens when your server gets flooded.
2. Syn flooding attacks happen when an attacker forges the return address on a number of SYN packets. The server fills its table with these half-open connections.
3. First one is not good because it just means the attacker needs to send more requests, second one would disadvantage their slower clients, and the third one is not feasible because its hard to determine what's legit and what's not.

Lecture 72

1. Packet filtering works well to prevent attacks because it detects patterns that are anomalous to regular activity.
2. IDS would analyze traffic and react to bad requests while IPS assumes that attacks are identifiable and stops them before they happen.
3. Over-provisioning is just the idea of having too many servers to bog down, filtering attack packets tries to identify malicious packets and stop them, slow down just tries to slow down the flow of all information with an added disadvantage to attackers, and Speak-up requests additional traffic from all requestors, which would break the pattern of some attacks.

Lecture 73

1. False positives happen when regular traffic is identified as an attack; false negatives occur when malicious traffic is not detected. They can both be pretty bad.
2. Accuracy is a measure of detecting attacks while precision is a measure of how many false positives come up.
3. Because you can just flag all messages or not flag any, full precision or full accuracy is easy to achieve, just not both.
4. The base-rate fallacy is the idea that even with pretty high precision and accuracy, there can still be a pretty big chance that you get a false pos/neg.

Lecture 74

1. Use a vulnerability to overload servers (DoS attack) on the White House.
2. It didn't work well because they used a static seed, which means it generated the same IP addresses each time.

3. The memory resident idea is that the virus is only in memory and does not get stored on the hard drive. So, if you reboot you will be clear of the virus.
4. Code Red 2 was much more effective because it used a random seed.

Lecture 75

1. Not very related, however the writer knew about Code Red 1.
2. In order to set itself up undetected.
3. It attempted to infect other machines and spread, giving the creator remote access to those machines.
4. There is a huge population of vulnerable machines so these worms can still circulate.
5. The lesson is that we are lazy, and we should be patching to prevent these attacks from spreading.

Lecture 76

1. Because it allows the common man to evaluate various security systems for his needs.
2. It includes a set of requirements, a set of assurance requirements, a methodology, and a measure of the result.
3. Because they are different.
4. 1: Basic security gives one approved algorithm, 2: is tamper-evident as well, 3: has strong tamper-resistance and countermeasures, and 4: gives a complete envelope of protection that actively fights attacks on the fly.

Lecture 77

1. It's a set of criteria that most governments accept to be good for evaluating security.
2. It's common because it's accepted by many countries.
3. National schemes would be needed for different domains.
4. The ST describes the abstract policy while the PP is an evaluation of an existing system.

Lecture 78

1. The overall goal of the protection profile of WBIS is to make sure the correct weight of each trash bin gets to the government safely.
2. The various parts of the protection profile are there to account for each and every way that an attacker could disrupt the transfer of information.
3. If you fill in the matrix with security objectives and put an X somewhere in each row, you know that you're using a mechanism for each threat.

Lecture 79

1. The Sun Identity Manager security target evaluation has the main goal of countering threats.
2. A security target evaluation differs from a protection profile evaluation in that the target is a system or class of systems while the protection profile is a set of guidelines for securing of that system.

Lecture 80

1. They are Evaluation Assurance Levels and they are used to ascertain the confidence in the evaluation of the security system.
2. The Common Criteria evaluations are performed by the government of the country where the evaluation is performed.
3. The higher EALs might not be mutually recognized by various countries because they may have different belief systems on what assurance is.
4. No, because NIST says that it must be done by an independent organization that is certified to do so.
5. You don't want to reverse engineer the model from the code because that sucks and you just want to be provided with a model that you can check the code to see if it conforms to. That's the way things should be.