Colin Murray
UTEID: cdm2697
UTCS-username: tashar
Email: murray.colin43@gmail.com

CS361 Questions: Week 5

Lecture 66

1. What is PGP?

It's a system developed that combines the best available cryptographic algorithms in order to provide a relatively simple way for people to strongly encrypt email messages.

2. What motivated Phil Zimmerman to develop it?

Zimmerman felt that the government shouldn't be able to snoop on the communications of its citizens. If the public had a very strong, relatively easy to use method of encryption they could avoid government eavesdropping.

3. Does PGP provide effective security?

It would seem so as there are reports of government agencies attempting to break PGP yet coming up short. The algorithms it relies on are extremely robust and have withstood the test of time.

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

Often times companies choose a proprietary software that offers extra support as opposed to freeware which can be flakey with support and might not offer as extensive of features.

Lecture 67

1. Explain the PGP authentication protocol.

PGP uses digital signatures by having the sender sign the hash of the message being sent using their own private asymmetric key. The resulting signed hash is appended to the message to provide integrity and authentication.

2. Explain the PGP confidentiality protocol.

The message is encrypted using a random session key using a high quality symmetric encryption algorithm. This session key is then encrypted with the recipient's public key and prepended to the message. The receiver decrypts the session key using his private key and subsequently uses the session key to decrypt the message.

3. How do you get both authentication and confidentiality?

The sent message would be the combination of the 2 steps mentioned above and would look something like this:
$S \rightarrow R : \{K\}_{Kr}, \{\{h(M)\}_{Ks}^{-1}, M\}_{K}$

Lecture 68

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

Compression, Email compatibility and Segmentation

2. Why is compression needed?

Compressing messages helps save bandwidth as networks (especially when PGP was developed) could be limited. It is generally done after applying the signature but before encryption. It also means there's less data to encrypt so generally the actual encryption process moves faster.

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

It'd be undesirable to have the digital signature depend on anything but the message itself. If it were the other way around it would also depend on the compression used.

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

A radix-64 transformation takes a standard set of 3 octets (24bits) and turns it into 4 ascii characters. Everything in the message after the transformation is now in ascii which is pretty standard across all email clients.

5. Why is PGP segmentation needed?

Certain mailers have limits on message length. PGP allows breaking up the message into segments which all mailers are able to support so PGP can encrypted any size message and still be supported by any email client.

Lecture 69

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

Session keys (used once and generated for each new message), Public keys (used in asymmetric encryption), Private keys (also used in asymmetric encryption) and passphrase-based keys (used to protect private keys)

2. What special properties are needed of session keys?

It should have high-entropy (random appearing and difficult to guess), it should be associated with a single message and it must only be used once.

3. How are session keys generated?

Session keys are generated by encrypting the previous session key as well as seemingly random events like user-keystroke timing.

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

2 large primes are generated by generating a very large number of a particular size, testing it for "primeness", tossing it if it fails and repeating the process until two numbers pass the "primeness" test.

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

Private keys are stored by asking the user for a pass-phrase which will be hashed and using this hash to encrypt the private key using CAST-128. Whenever the user wants to access the private key he must enter his password first. This prevents impersonation in the event that the user's device was compromised or stolen.

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?

The sender instead sends a unique ID that hopefully is unique to the recipient (e.g. the recipient doesn't have another public-key : ID pairings where the ID is the same). In PGP the least significant 64 bits of the public-key are used as the ID. The recipient ideally may just look up the ID in a table of public-key : ID mappings and retrieve the sender's correct public key.

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

Timestamp (when the key was generated), Key ID (last 64 bits of public key), public key (public key portion of the private key), private key (private portion encrypted with a passphrase), and user ID (some username to associate the private key with).

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

Timestamp (when the public key was generated), Key ID (last 64 bits of public key), public key (the key itself), and user ID (some username to associate this public key with).

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

PGP receives a message encrypted using the receiver's public key (K_R). PGP retrieves the private key from the private-key ring using the Key ID field provided in the received message. PGP prompts the user to validate themselves (enter username and passphrase), the passphrase being used to decrypt the private key. The private key is now used to decrypt the message.

5. What is the key legitimacy field for?

It specifies how strongly PGP believes the public key really belongs to the public key's owner. This field may store certificates that verify the legitimacy of the sender's public key.

6. How is a key revoked?

A revocation certificate is sent out signed by the user. Any recipients are expected to update their public-key rings with the user's new public key.

Lecture 71

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

The consumer problem is if the attacker logically gets between the client and the service, somehow disrupting communication. The producer problem occurs when the attacker targets the server itself, overwhelming it and preventing it from servicing legitimate users.

2. Explain syn flooding.

An attacker (or many distributed attackers) attempts to initiate many TCP handshake with a server. He does this by faking the source address on each message (or using the many bots) and sending the server SYN packets, which the server must respond to. The server responds with a SYN/ACK at the given source address. If the source address is spoofed the connection remains "half-open" which can be deadly if the server allocated resources for this fake connection. It is even more difficult if the source addresses are real but belong to the attacker's botnet, at which point the clients finish the connection sending an ACK back and remain stagnant, consuming server resources.

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

Increasing the storage size of the server's connection table is an impractical solution when the attacker can just send more SYN packets faster. A shorter timeout on half-open connections may deny service to legitimate clients who simply have a slower connection. Filtering suspicious packets can be very difficult since there's really no clear distinction between a fake SYN packet and a real one. Additionally, if the means of determining legitimate packets is too strict it may accidentally flag legitimate client SYN packets and block legitimate connections.

Lecture 72

1. Why doesn't packet filtering work very well to prevent attacks?

Often there is no tell-tale sign distinguishing a malicious packet from a legitimate one, at least none that wouldn't be computationally infeasible to check.

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

Intrusion detection systems check the behavior of the system itself to see if any anomalous patterns emerge. Intrusion prevention systems attempt to block attacks from gaining access to the system in the first place.

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

- Over-provisioning the network – possessing too many servers to be overwhelmed (expensive and unworkable)
- Filtering attack packets – somehow distinguish the attack packets from regular packets (very difficult often times)
- Slow down processing – disadvantages all requestors, but perhaps disproportionately disadvantages the attacker.
- "speak-up" solution – request additional traffic from all requestors.

Lecture 73

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

It depends on the case. For extremely sensitive systems, false positives may be acceptable compared to a false negative, but for less sensitive systems it might be more important to avoid throwing off false positives at this risk of annoying people or disrupting availability.

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

An accurate system detects all genuine attacks, a precise system never reports legitimate behavior as an attack.

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

A purely accurate system might report everything as an attack, a purely precise system might report nothing as an attack. It is very difficult to find a strong balance in between.

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

Even if an IDS has a reasonably high percentage chance to detect an attack, the fact that attacks are often vary rare compared to legitimate packets means that most "attacks" flagged by the IDS are going to be legitimate, even if it has a very high success rate at detecting attacks.

Lecture 74

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

If the date was between the 1st and 19th of the month, it generated a random list of IP addresses and had the infected system send out packets attempting to infect other machines. On the 20th to 28th of the month it would launch an attack flooding www.whitehouse.gov. It also defaced some web pages with the words "Hacked by Chinese".

2. Why was Code Red version 1 ineffective?

The worm used a static seed to randomly generate IP addresses, meaning infected machines would always generate the same list of IP addresses.

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

It resided in the volatile memory, and would be cleared from the machine after a reboot. It would be very likely though that the machine would be reinfected since the static seed managed to pick that IP in the first place.

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

Code Red 2 used a randomly generated seed allowing it to spread much faster and more widely. Many of the IP addresses corresponded to machines that were not prepared to handle heavy traffic. This resulted in heavy widespread internet traffic and incapable machines crashing under the strain.

Lecture 75

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

Code Red II made reference to Code Red in the body of it's code.

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

It uses parts of known IP addresses to find machines on the same network or subnet that are likely to be running similar software. It also has a higher guarantee packets will be sent to legitimate IP addresses.

3. What did Code Red II attempt to do?

It attempted to install a back-door on the machine which could allow remote-access.

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

Since there are huge populations of machines that remain unpatched, worms like Code Red can propagate on the Internet for a very long time, perhaps indefinitely.

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

9 out of 10 times, the vulnerability exploited was patched six-months prior to the attack. Basically people are bad at patching their machines.

Lecture 76

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

Certification agencies assess and standardize the process of validating the trustworthiness of products so the common consumer doesn't need to judge for themselves (especially since it can be a rigorous process requiring experts to certify the trustworthiness of a software product).

2. Explain the components of an evaluation standard.

An evaluation standard model provides a set of requirements for defining security functionality. It establishes a set of assurance requirements needed for establishing the functional requirements. It imposes a methodology for determining that the functional requirements are met and it serves as a measure of trustworthiness based on the evaluation result of the system.

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

The requirements (assurance and functional) would be very different when evaluating the reliability and trustworthiness of crypto devises as opposed to general programs that do not carry sensitive information (or at least aren't dedicated to that goal).

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

1. Basic security: at least one approved algorithm or function.
2. Improved physical security, tamper-evident packaging
3. Strong tamper-resistance and countermeasures.
4. Complete envelope of protection including immediate zeroing of keys upon tampering.

Lecture 77

1. What is the Common Criteria?

It is a standardized certification scheme that has been adopted by at least 26 countries including the US comprising of CC documents and CC Evaluation Methodology as well as country-specific evaluation methodologies called Evaluation Schemes or National Schemes. Evaluations then done by one country (at least up to a certain level) are respected by all other countries.

2. What's "common" about it?

It's standardized and accepted with only minor differences (National Schemes) between the countries who have adopted CC. Therefore its methodologies are common between countries and can be (for the most part) respected throughout all countries if a product is certified in one.

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

Certain countries may require software to undergo stricter evaluations based on national security or privacy laws within the country itself. Thus if the CC evaluation being sought after is high enough, the countries laws may require different or more thorough evaluation schemes.

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

The security target is the evaluation of a product which ideally is assessed to be secure up to a target security level based on some protection profile's requirements. It is a document which describes why the product may match the requirements of a particular protection profile. The protection profile is a set of implementation-independent security requirements for a category of products or systems which must be met, it is essentially a set of security policies for the category of system.

Lecture 78

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

The goal is to define the assumptions that must be made for the system in question to function properly and the threats that could subvert the system. Ideally by analyzing the threats and seeing if the system holds up in the face of threats, the protection profile will be met.

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

The assets involved list the information being sought after when the system is used (in this case the weight, timestamp and bin ID of a trash bin). The environmental assumptions enumerate the various normal requirements that must be met for normal operation of the system (like the waste bin must have an ID and the crew operating the system must be trustworthy). The threats against the system are enumerated, which the system should be able to counter or prevent. Finally it suggests a policy of backing up in case of system fault (which may not be the result of an attack). Considering all these conditions the system can be evaluated against them to see if it meets the security objectives (non-implementation specific mechanisms that achieve security objectives for this class of system) as well as security requirements (broad security goals that should be met for this category of system which are required in the Common Criteria).

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

The matrix enumerates the threats and assumptions on the left and the objectives and requirements on the top. Ideally each column (an objective or requirement) is met that either counters a threat or validates an assumption. If every row has an x in it somewhere than the system meets the requirements of its protection profile.

Lecture 79

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

Their security target evaluation is a document that Sun put together evidence that that was thoroughly thought out about what the security requirements of their system would be and how their system met these requirements.

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

Sun's security target evaluation addresses factors that exist within Sun's implementation of the system that addresses all the concerns laid out in Sun's proposed security policy or an existing protection profile (which has already been evaluated and deemed secure up to a certain level). The security target is implementation specific and is evaluated based on how the implementation fulfills all necessary security policies. Protection profiles are a set of policies and mechanisms that must be in place for a class of systems to be secure, and protection profiles are evaluated to make sure the policies they mandate are thorough and address the all issues that category of systems faces.

Lecture 80

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

EAL's specify the level of rigor underwent in validating the security of a system in question. EAL1 is the lowest and the least evidence must be provided to get this security assurance level whereas EAL7 must have very rigorous evidence provided.

2. Who performs the Common Criteria evaluations?

The government of the country where the evaluation is performed or a certification agency in the country evaluates the product's claims and the companies' own evaluation and evidence on these claims. A certificate is given if the Certification authority or government doing the evaluation deems the requirements are met by the proposed evidence by the company.

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

High ELA's for certain products may be subject to the laws of privacy and security within particular countries. Often times high ELAs are evaluated by government agencies (like the NSA) and these agencies may evaluate products differently based on the laws of the country.

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

No, otherwise the trustworthiness of these certifications would be subjective and possibly biased or incorrect. Vendors must evaluate and provide evidence for their product so that another certification agency who is trusted (their business model depends on the trustworthiness of their evaluations) can objectively evaluate it.

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

The model dictates the code, but it's difficult to see from the code what the model is.

Well done!