NAME: Ali Pasha
UTEID: aap2493
CSACCOUNT: alipasha
EMAIL: alipasha@utexas.edu

CS361 Questions: Week 5

Lecture 66

1. What is PGP?

   If you completed all of these steps and you still lose, let the computer go first and just ask for a hint every time. However, if you want the satisfaction of beating the computer by yourself, just keep practicing.

2. What motivated Phil Zimmerman to develop it?

   Don't ever risk your king, it's the most valuable piece on the board. Don't ever move backwards unless absolutely necessary.

3. Does PGP provide effective security?

   Just keep practicing and don't give any pieces away! Keep moving forward! Protect your pieces and invade the board!

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

   Play with confidence that you are going to win.

Lecture 67

1. Explain the PGP authentication protocol.

   In more recent Windows and Mac computers, a chess game is built in. Use this to practice!

2. Explain the PGP confidentiality protocol.

   You don't have to practice against other people. You can also buy a chess engine to install for your computer and/or laptop, to play against the CPU!

3. How do you get both authentication and confidentiality?

   Not only does it conflict with the touch-move rule, but it also makes you look like a bit of a dandy, and that you're not sure about where you're going to move the piece, if at all.

Lecture 68

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

A waste of 5 points! However, if you move it down to the center of the back of your side, it would be dominating and attacking one of the two most powerful files of the game board - the Center.

2. Why is compression needed?

A rook is worth 5 points, and is easily abandoned in the lonely corner of your side, all by itself, doing nothing.

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

Chess is like a medieval war. You need to push the opponent back and invade their territory, in hopes of getting closer and closer to their King. If you're in a war, and you're being pushed back while your opponent is moving in on you, is that good for you? No, it will help your opponent win.

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

Don't go complete aggression. Go about as a rule of thumb, 60% aggression and 40% defending.

5. Why is PGP segmentation needed?

Just look for isolated pawns that could be nicked by you. However, don't let your guard down

Lecture 69

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

Even if you're one pawn up, that could win you the game. That being said, even if you are down by, say, a knight, you could still win the game.

2. What special properties are needed of session keys?

The King, obviously, cannot be taken, and is worth the game, basically. Inspect every move you take. Make the move in your mind.

3. How are session keys generated?

Here are the relative value of pieces: Pawn = 1 Knight = 3 Bishop = 3 Rook = 5 Queen = 9.

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

Never give any pieces away for free, or give a bad trade.

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

Mastering Chess doesn't just happen. You need to learn to be more protective of your pieces, and more aggressive over the opponent. But you can never be sure you will definitely win a match.

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?

On the Internet, several groups serve as "root certification authorities".

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

Some entity may be designated as a certification authority (notary public, personnel office, security officer in a company, etc.).

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

There is also a need for trust in situations where there is not a single hierarchy, such as on the Internet. Two individuals may not have a common "superior."

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

Thus, an individual's certificate contains a chain of evidence rooted at some unimpeachable authority.

5. What is the key legitimacy field for?

Now Y can certify the identify of her subordinates in a similar manner. She appends her certificate to each of theirs.

6. How is a key revoked?

Y's certificate is X's affirmation of her identity. Anyone can decrypt it with X's public key and look at the contents.

Lecture 71

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

The following are possible steps. Suppose X is the president of the company and her immediate subordinate is Y. Each have a public key pair.

2. Explain syn flooding.

A public key and user's identity are bound together in a *certificate*. This is then signed by a *certification authority,* vouching for the accuracy of the binding.

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

Electronically, certification is accomplished with digital signatures and hash functions.

Lecture 72

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

The chain can begin at the top or from the bottom of the hierarchy.

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

If both trust their management, they can certify each other's authenticity via their common supervisor.

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

Presumably, they have a common supervisor (ancestor in the hierarchy tree of the company).

Lecture 73

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

Sometimes certification occurs through a *common respected individual*. For example, suppose Ann and Andrew work for different divisions within the same company.

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

However, it would be unmanageable to require all of these parties to be present for communication to occur. There is a need to securely store and pass around records of such certification.

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

His supervisor may vouch for him, and so on. A truly paranoid customer may require a chain of certifications leading back to some unimpeachable authority at the base

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

In a large company, your supervisor may vouch for or certify your employment.

Lecture 74

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

Establishing trust may involve "chains" of certification.

2. Why was Code Red version 1 ineffective?

That is, how do I know that the public key you present is really your public key and not someone else's?

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

The most common circumstance in which trust is needed in a distributed context is in *binding a key to an identity*.

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

Business Bureau, and credit reporting agencies all function in part as certification = authorities for such transactions.

Lecture 75

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

authorities for such transactions.

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

This threshold may depend on the size or nature of

3. What did Code Red II attempt to do?

Trust we're willing to confer without going further in the certification process.

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

In general, we have a "trust threshold," a degree of

5. Comment on the report from Verizon cited on slide 6. What are the lessons of their study?
We may believe a party's affiliation or ask for independent validation

Lecture 76

1. Why is a certification regime for secure products necessary and useful?
"vouches for" the trustworthiness of one

2. Explain the components of an evaluation standard.
relationship of trust. One way is to rely on a third party who

3. Why would crypto devices have a separate evaluation mechanism?
do two entities that are mutually suspici

4. Explain the four levels of certification for crypto devices.
Certification addresses the need for *trust* in computer system

Lecture 77

1. What is the Common Criteria?
Public key systems are well-suited for digital signatures. Recall that some algorithms, RS

2. What's "common" about it?
If P signs message M with signature $S(P,M)$, it must be impossible for anyone else to produce $S(P,M)$. Also ensures *no repudiation.*

3. Why would there be any need for "National Schemes"?
A check is a *tangible object* authorizing the transaction.
The signature on the check *confirms authenticity*.

4. Explain the difference between a protection profile and a security target.
According to Encyclopædia Britannica, polo was first played in Persia (Iran) at dates given from the 6th century BC to the 1st century AD.

Lecture 78

1. Explain the overall goal of the protection profile as exemplified by theWBIS example.
Other authors give dates as early as the 5th century BC (or earlier)[5] Its birthplace was Asia and authorities[who?] credit Persian Emperor Shapur II of the Sassanid dynasty of the 4th century who learned to play polo when he was seven years old. Naqsh-i Jahan Square in Isfahan is a polo field which was built by king Abbas I in the 17th century.

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

Sultan Qutb-ud-din Aybak, the Turkic slave from Northern Afghanistan who then became Emperor of North India, ruled as an emperor for only four years, from 1206 to 1210, but died accidentally in 1210. While he was playing a game of polo on horseback (also called chougan in Persia),

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

From Persia, in medieval times polo spread to the Byzantines (who called it tzykanion), and after the Muslim conquests to the Ayyubid and Mameluke dynasties of Egypt and the Levant, whose elites favoured it above all other sports.

Lecture 79

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

Notable sultans such as Saladin and Baybars were known to play it and encourage it in their court. Polo sticks were features on the Mameluke precursor to modern day playing cards.

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

Later on, polo was passed from Persia to other parts of Asia including theIndian subcontinent and China, where it was very popular during theTang Dynasty and frequently depicted in paintings and statues.

Lecture 80

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

Valuable for training cavalry, the game was played from Constantinople to Japan by the Middle Ages.

2. Who performs the Common Criteria evaluations?

It is known in the East as the Game of Kings. The name polo is said to have been derived from the Tibetan word "pulu", meaning ball.

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

The modern game of polo, though formalised and popularised by the British, is derived from Manipur (now a state in India) where the game was known as 'Sagol Kangjei', 'Kanjai-bazee', or 'Pulu'.

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

It was the anglicised form of the last, referring to the wooden ball that was used, which was adopted by the sport in its slow spread to the west. The first polo club was established in the town of Silchar in Assam, India, in 1834.

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

The origins of the game in Manipur are traced to early precursors of Sagol Kangjei. This was one of three forms of hockey in Manipur, the other ones being field hockey (called Khong Kangjei) and wrestling-hockey (called Mukna Kangjei).

Well done!