**CS 5601 Exam 2 Modules 8 through 12**

**Adam Hoffmeister**

1. **What is the one symmetric encryption algorithm that is theoretically unbreakable? What are at least two problems with using this algorithm for all encryption purposes?**

One-time pad is theoretically unbreakable. Two problems of this algorithm is that you cannot exchange keys securely, and if encoding/decoding isn’t synchronized, the encrypted message is useless.

1. **You’ve recommended to your organization that the building needs external security cameras at all entrances and emergency exits. However, the board is concerned with costs and only wants you to put one external camera per door. As the security person you know this isn’t a good idea. What are some arguments against a single camera per entrance? (feel free to think outside of what we discussed in class)**

Having more than one camera mitigates greater risk. When you use two cameras, every camera is in view by another camera. This prevents against attacks against the camera, itself, as the attacker would be seen by another view.

1. **What is the best detection tool for dealing with social engineering and how to do make it work for your organization?**

The best way to deal with social engineering is to train and educate employees. Organizations need to have policies and procedures that need to be followed. This prevents attackers from tricking or influencing employees into doing something out of the ordinary. With that, employees should have clear roles and responsibilities.

1. **What are some of the “human attacks” we see in information security? What controls would help reduce or even mitigate EACH of these attacks?**

* Shoulder surfing – Automatic screen saver lock after a short period.
* Dumpster diving – Train employees to not write down their credentials. Ensure procedure covers disposal of manuals.
* Installing malicious software – Have restrictions on user accounts and a policy on what may be installed.
* Installing unauthorized hardware – Have systems secured from being opened, or physically secure them behind closed doors.
* Access by non-employees – Have employees wear ID badges and visitors wear nametags.
* Social engineering – Train and educate employees. Have policies and procedures for employees to follow.

1. **Why are electronic emanations such a security concern in a high security environment? What controls would reduce the risks?**

Electronic emanations are a high security concern because they cannot be seen, thus they are not easily detectable. Wireless networks should be placed so they are hard to access from public areas. Sensitive equipment should be deep within a building. Other equipment, itself, can be shielded.

1. **Which fire detection device is responsible for more false positives than other fire detection devices?**

Rate-of-rise sensors provide more false positives than other detection devices.

1. **Of all the fire suppression choices, describe the best recommended class of fire suppression to use for a data center which is not occupied by staff?**

Electrical fires are of class C which requires CO2 or a dry chemical to suppress the fire.

1. **What is the paradox of social engineering attacks?**

People the biggest problem and security risk, but also the best to defend against those attacks.

1. **If you are required to use a key escrow through a third party, how can you ensure that the vendor cannot use the private keys without your knowledge? (Think separation of duties).**

The key can be broken into 2 or more parts. This allows you to use more than one key escrow to store the key. If one is compromised, you are still safe until you can update your key.

1. **Describe one condition of non-repudiation that can never be proven through digital analysis of the message sent and all logs involved. (taken from a lecture)**

People can deny that they were the sender behind the message. They could claim that others had access to their key or sent the message on their behalf.

1. **Why is opening a secure https in a new frame from a non-https frame a poor design practice?**

Accessing a secure page from an insecure page is inherently insecure. The SSL lock on the browser grantees that all the content is being served over HTTPS. If you have HTTP involved, the connection is not going to encrypted.

1. **What are the security goals of cryptography?**

Confidentiality and integrity are the two security goals of cryptography. This means that only authorized members can decode the message if it wasn’t tampered with.

1. **You have been requested by your organization to establish a new physical access control for the main office complex with multiple entrance and exit doors. One particular executive read an article of the strength of biometrics and is insisting that all external doors be outfitted with only a fingerprint scanner. As the Security Officer, what should you explain to the executive about this proposed security solution? (several answers come to my mind, but one will do)**

As biometrics are not 100% accurate, I would advise him to accompany it with another access control. In this case, I would recommend pairing it with a proximity device. As the employees already scan their finger, entering another PIN or swiping a card would be tedious.

1. **When dealing with a large environment of users and systems needing unique encryption keys each, why would the use of purely symmetric encryption be a problem?**

Symmetric encryption requires both parties to have the same key. This means that you wouldn’t be able to security trade keys between users, if you are only using symmetric encryption. The key needs to be sent and stored through an asymmetric encryption first.

1. **Why is not advisable for a programmer to create their own cryptographic algorithm for a product they are developing?**

A new cryptographic algorithm could have a minor bug that compromises its strength. There needs to be tests performed to see how easily the algorithm can be cracked and brute forced.

1. **What type of Symmetric Ciphers are the fastest and easiest to implement in hardware?**

Stream ciphers are the fastest and easiest to implement in hardware.

1. **Why is a large open space a good physical security feature?**

An open space is a good security feature because it provides a lot of time to respond to attacks. It makes the objective harder to reach without being seen.

1. **Why, when implementing a block cipher, is Electronic Codebook (ECB) using the same key on each block a bad design choice?**

When you use ECB with the same key on each block, information will be leaked. The message doesn’t get entirely scrambled, only portions of it do. This allows attackers to gain insight on what is encrypted.

1. **You are in charge of a design team and have been tasked with generating a cryptographic solution for a larger software project. The requirements for your team are:**

* **Must be able to exchange the cryptographic keys on the fly yet keep them secure**
* **Must able transfer huge amounts of data in reasonable time so the encryption algorithm speed is important.**
* **Must be mobile computing compatible.**

**Clearly PKI is the solution for the first requirement, but several members on your team feel that once each side has exchanged their public keys, using asymmetric algorithms only will be sufficient because CPU’s are plenty fast these days. As the team leader you need to decide if this is acceptable or convince your team that PKI only will fail in meeting the requirements. Please give examples to justify your decisions.**

PKI should be used to securely transfer keys between two parties. However, symmetric algorithms should be used to encrypt as they are faster and have less computational requirements. This process is called electronic key exchange. It uses the slow algorithm to transfer the keys, and the fast algorithm to transfer the data. This should allow the team to fulfill their tasks, while keeping the solution mobile compatible.

1. **You have been asked for design elements of a highly secured data center. Think of all the different types of physical security as well as access controls we have discussed to date. Will grade based on thoroughness.**

The building should be built in the open, not against other buildings. The walls should be concrete or brick to prevent break-ins and to increase wireless signal degradation outside. Floors should be elevated to prevent flooding and to allow cable runs. The ceiling should have cable conduits implemented to future proof. No drop ceiling should be used.

The entry and exit doors should have two cameras protecting each one; one in sight of the other. The doors should be metal with a smart card and pin lock. Also, access logs should be used to dissuade employees from abusing their access. No windows are needed.

Power should be provided through uninterruptible power supplies and surge protectors. The HVAC system needs to be secured and constantly monitored for outages. The whole building needs backup power in case of an outage.

For fire suppression, use CO2 or a dry chemical in conjunction with a fire detection device. Hand-held CO2 fire extinguishers should be abundant.

Wireless networks and sensitive equipment should be placed towards the center of the facility. This will prevent most electromagnetic emanations.

If they want to take it to the extreme: Have multiple cameras around the property, a fence around the building, a human security guard, shielding on all the walls, multiple rooms/doors inside the facility to restrict access, a long driveway/road with a locked gate, and two power and Internet companies.