Christopher Morcom

Yousef Elmehdwi

CS 458

23 September 2018

**Problem 1**

**Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof.**

1. **John copies Mary’s homework.**

* CONFIDENTIALITY

1. **Paul crashes Linda’s system.**

* INTEGRITY, AVAILABILITY

1. **Carol changes the amount of Angelo’s check from $100 to $1,000.**

* INTEGRITY

1. **Gina forges Roger’s signature on a deed.**

* INTEGRITY

1. **Rhonda registers the domain name “AddisonWesley.com” and refuses to let the publishing house buy or use that domain name.**

* AVAILABILITY

1. **Jonah obtains Peter’s credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number.**

* CONFIDENTIALITY, INTEGRITY, AVAILABILITY

1. **Henry spoofs Julie’s IP address to gain access to her computer**

* INTEGRITY

**Problem 2**

**Computer viruses are programs that, among other actions, can delete files without a user’s permission. A U.S. legislator wrote a law banning the deletion of any files from computer disks. What was the problem with this law from a computer security point of view? Specifically, state which security service would have been affected if the law had been passed.**

Regarding the CIA in computer science, Confidentiality will be a problem if the system is breached successfully, secure or private data could be lost (potentially *en masse*). Regarding Data Integrity, some data may become unreliable over time or there could be a loss in source integrity. For Availability, the constant loss of storage space without deleting data would lead to spatial availability problems.

**Problem 3**

**Suppose that someone suggests the following way to confirm that the two of you are both in possession of the same secret key:**

1. **You create a random bit string the length of the key**
2. **XOR it with the key and send the result over the channel**
3. **Your partner XORs the incoming block with the key (which should be the same as your key) and sends it back.**
4. **You check, and if what you receive is your original random string, you have verified that your partner has the same secret key, yet neither of you has ever transmitted the key. Is there a flaw in this scheme?**

**Explain.**

Suppose the key *K* and a number *N*. The receiver can confirm *K* by sending *N*. If an attack like a MITM (Man-In-The Middle) Attack is used and both *K* ⊕ *N* (sent by sender) and *N* (sent by receiver) are recovered by the attacker, then by *K = (K* ⊕ *N)* ⊕ *N*, the attacker can retrieve *K*.

**Problem 4**

**Simplify the following XOR arithmetic expressions, where a , b , and c are bits such that a ⊕ b = c , where ⊕ is shorthand for XOR, and a ` stands for the complement of a (opposite bit value).**

**• a ⊕ a** = 0

**• a ⊕ a`** = 1

**• a ⊕ b`**  = a`b`+ab

**• a` ⊕ b`** = ab`+a`b

**• a ⊕ b ⊕ a** = (a ⊕ b) ⊕ a = a (similar to problem 3)

**• b ⊕ c** = b ⊕ (a ⊕ b) = (b ⊕ a) ⊕ b = b (similar to problem 3)

**Problem 5**

**Find the plaintext and the key, given the ciphertext** CSYEVIXIVQMREXIH. **Hint: The key is a shift of the alphabet *(CASEAR CIPHER)*.**

**KEY (Shift +4):**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **a** | **b** | **c** | **d** | **e** | **f** | **g** | **h** | **i** | **j** | **k** | **l** | **m** | **n** | **o** | **p** | **q** | **r** | **s** | **t** | **u** | **v** | **w** | **x** | **y** | **z** |
| E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |

**PLAINTEXT:**

you are terminated