INF140-Introducation to Cybersecurity, Mandatory Assignment 1

Overview of Cybersecurity (20 pts)

Question 1:

*Explain the meanings of the following security attributes in computer systems: conﬁdentiality, integrity, authenticity, accountability, availability.*

*For each attribute, describe an example in which the attribute of an asset in an information system can be potentially violated and the security techniques/controls that can be used to protect the attribute of the asset.*

**Confidentiality:** Confidentiality deals with the private and confidential information such as unauthorized entities cannot access the system.

* Violation:  
  Its common to use password protection to keep your unwanted individuals away, however there is a lot of different approaches an attacker can take to gain access anyways. E.g. the use of software to guess the password, and unfortunately its common to use weak passwords and use it to multiple accounts, which makes it way easier for the unauthorized individual.
* Protection:  
  To protect against these attacks you can choose a much stronger password, or even better, the use of two factor authentication. Some examples on this is biometrical confirmations or the use of your phone for confirmation.

**Integrity:** Integrity assures that information isn’t tampered by the program it’s using or along the destination of the information.

* Violation:  
  Even if most of the information traveling through the internet is encrypted, there exists exploits that can give an unauthorized person the ability to modify information between sender and receiver.
* Protection  
  To protect yourself from integrity attacks the sender and receiver must be assure that their software doesn’t contain any form for malware and be connected to a secure network.

**Authenticity:** Authenticity is about being able to confirm and verify the user is who they say they are, and that they are being trustworthy.

* Violation:  
  A party within a transaction may have left behind by an unauthorized entity.
* Protection:  
  Have a second form for authentication to confirm the authenticity.

**Accountability:** Accountability is the term involving the tracing and identification of every entity connected to the internet. The reason why, is in the instance of a security breach, the breach needs to be traced back to the origin of the attacker.

* Violation:  
  The use of shared user IDs and passwords render accountability useless.
* Protection:  
  Ensure that every user has its own identity on the network.

**Availability:** Ensuring minimal delay and reliable access to and use of information, such as authorized users aren’t denied.

* Violation:  
  Overwhelming security can cause antivirus and firewalls to interfere with the availability of the system
* Protection:  
  Making sure only necessary protection software are installed and wont interfere with the main system that’s trying to run.

Question 2:

*Consider a company whose operations are housed in two buildings on the same property:*

* *one building is headquarters*
* *the other building contains network and computer services.*

*The property is physically protected by a fence around the perimeter. The only entrance to the property is through a guarded front gate. The local networks are split between the Headquarters’ LAN and the Network Services’ LAN. Internet users connect to the Web server through a ﬁrewall. Dial-up users get access to a particular server on the Network Services’ LAN.*

*Read Section 1.5 in Chapter 1 and develop an attack tree in which*

* *the root node represents disclosure of proprietary secrets;*
* *there are at least 10 nodes;*
* *attacks include physical, social engineering, and technical attacks;*
* *both AND and OR nodes may be contained.*

**Disclosure of proprietary secrets:**

* Snaking into the property
  + Using tools to get past the fence
  + Help from man on the inside
    - Smuggling
    - Patrol routes, and potential cameras
  + Parachuting onto the roof
  + Entering through the sewers
* Identity theft
  + Copying/Stealing RFID from authorized worker
  + Taking the place of a look alike
  + Surgery to change biometrics
* Social engineering
  + Vishing
  + Phishing
  + Tailgating
* Software attack
  + Exploiting weakness in the firewall
  + Trojan horse

Network attack

Software attack

Human attack

Cryptographic Tools (60 pts)

Question 3:

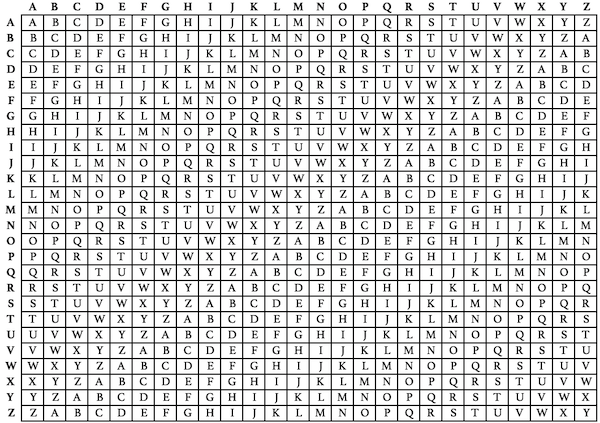
*Encrypt the following sentence*

*Cybersecurity is an evolving process and is determined by the weakest link*

*by*

* *the Vigenère cipher with key k = human; and*
* *the column transposition cipher 34681752*

The Vigenère Cipher:

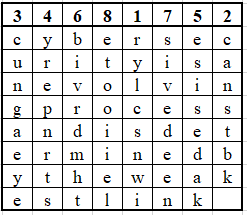


* Plain text: cybersecurity is an evolving process and is determined by the weakest link
* Key: human
* Cipher: jsneezyouepnk if hh qvbspunt wlacrzm mnq pm pegllyialx ny goy ienryet yphw

The Column transposition cipher:

* Plain text: cybersecurity is an evolving process and is determined by the weakest link
* Key: 34681752

Using the column transposition cipher:



* + Line 1: rylcsnwi
  + Line 2: canstbk
  + Line 3: cungaeye
  + Line 4: yrepnrts
  + Line 5: esisedak
  + Line 6: bivrdmht
  + Line 7: sivedeen
  + Line 8: etooiiel
* Cipher: rylcsnwicanstbkcungaeyeyrepnrtsesisedakbivrdmhtsivedeenetooiiel

Question 4:

Question 5:

1. Perform encryption and decryption using the RSA algorithm, as in the slides, for the following examples (10 pts: 2 pts for each):
   1. p = 13; q = 31, e = 19; M = 2
   2. p = 11; q = 31, e = 7; M = 4
   3. p = 3; q = 17, e = 5; M = 5
   4. p = 5; q = 17, e = 7; M = 6
   5. p = 7; q = 17, e = 29; M = 3
2. Encryption:  
   C = Me mod n = 219 mod 403 = 388  
   n = p \* q = 13 \* 31 = 403  
   Decryption:  
   M = Cd mod n = 3881/19 mod 403  
   φ(n) = (p-1) \* (q-1) = 12 \* 30 = 360  
   d = e-1 = 1/19
3. In a public-key system using RSA, suppose you intercepted a cipher text C =61 sent to a user whose public key is e =11, n =91. What is the plaintext M? Explain the steps that you ﬁnd the plaintext. (5 pts)

Question 6:

Consider a Diﬃe-Hellman scheme with a common prime q =23 and a generator g =5.

1. Alice has public key PUBA =10, what is Alice’s private key PRIA? (2 pts)

Function:

gPRIA mod q = PUBA  
5PRIA mod 23 = 10

1. Bob has public key PUBB =8, what is the shared secret key K? (3 pts)

Question 7:

After taking some courses on cryptography, Alice and Bob decide to try it out in their communication. They agree that they will use Vigenere cipher for data encryption/decryption, and RSA for sharing secrete key, where the key of Vigenere cipher only uses letters A,B,··· ,J and letters in a key are encoded as digits 0,1,...,9 for RSA. For instance, the key BAJ is 109.

Alice chooses a RSA public key (n, e) = (341,7). Bob uses the Vigenere cipher to encrypt a sentence and encrypt the Vigenere key by Alice’s RSA public key. Then Bob sends the following message to Alice:

61, Tfsgnhgs zq tadnov zuws gutoiosgoz dﬂqsk vik ﬀgfmopf. Ov jy uuxkdz. Answer the following questions:

* What is the Vigenere key used by Bob? (6 pts)
* What is the original message from Bob? (4 pts)