CS4355 Assignment 1

October 31, 2019

Avery Briggs

3471065

1. Please answer the following questions.
    a) List and briefly define categories of passive and active security attacks.

    Passive – An attack that silently waits and listens for a trigger. It does not perform any actions until it is prompted or activated. A significant portion of passive malware is traffic monitoring software that listens and reports network traffic. Spyware is a common passive malware. The main challenge concerning passive attacks is detection, since they are silent, and it is not immediately obvious that it exists or what it is doing.

    Active – An attack that immediately and continuously attempts to breach. Can perform malicious operations on files or through browsers or email applications masquerading as the device owner. Active malware would include viruses that delete or encrypt files, once they infect a computer it immediately causes damage. Ransomware and denial of service are common types of active malware attacks. The main challenge concerning active attacks is prevention, since the effects of the malware are so damaging, we never want to subject our data or systems to it's actions.

    b) List and briefly define the basic security requirements in computer and network security.

    The main components of network security are comprised of concepts relating to confidentiality, integrity, and availability. These are also known as the CIA triad of network security. Combined with elements of non-repudiation and authenticity, we can encapsulate all aspects of software assurance.

    Confidentiality – Only the specified users are allowed access to the data.

    Integrity – Only authorized parties are allowed to edit the data.

    Availability – Data must be readily available to relevant parties.

    Non-repudiation – Assurance that someone cannot deny something.

    Authenticity – Assurance that all parties are who they claim to be.

    Accountability – Actions of an entity must be able to be traced uniquely back to that entity.

    c) Describe the Kerckhoff's Principles.

    There are 6 main design specifications and requirements outlined in the Kerckhoff's principles for a system to be considered secure:

    1. The system must be substantially, if not mathematically, undecipherable (unconditionally secure or at the minimum computationally secure).
    2. The system must not require secrecy and can be stolen by the enemy without causing trouble. (The security of the system is not dependent on the secrecy of its processes and artifacts).
    3. Keys should be easy to remember and easy to communicate without requiring written notes. The keys must also be easy to change or modify the keys with different participants.
    4. The system ought to be compatible with telegraph communication. (Most common communication medium, and easily accessible using physical wires).
    5. The system must be portable, and its use must not require more than one person;
    6. Regarding the circumstances in which such system is applied, it must be easy to use and must neither require stress of mind nor the knowledge of a long series of rules.

Several of these principles are written in a war, or attack context. This explains why it must be portable, and not stressful to use. In the event of an attack, a tedious system to secure your data, would be a big weakness in the security system. Kerckhoff's principles outline why a cryptologist should not rely on secrecy and obscurity to protect their system from attackers and their malware.

d) Describe the functions of confusion and diffusion in symmetric ciphers.
Confusion – Is the process of substituting letters during encryption, in an effort to make the statistical relationship between the key and the cipher text as complex as possible. This helps to deter attackers from recognizing a found key and increasing their computation time to reassure their predictions.
Diffusion – The process of spreading the effect of the key or cipher text as widely as possible. This increases computation time for attackers by obscuring the effects of the key as much as possible. It makes searching for the key a much more difficult task. Diffusions goal is to ensure that each ciphertext digit is affected by many plaintext digits, which further increases complexity.

e) Describe the Strict Avalanche Conditions in symmetric ciphers.
The avalanche effect is a property of any encryption algorithm such that a small change in either the plaintext or the key produces a significant change in the ciphertext. The condition that enables a symmetric cipher to be able to avalanche is that on average half of the output bits should change for every bit in the cipher text. This leads to widespread "garbling" of the bits.

f) Describe the key management problem in conventional cryptosystems.
The Key management problem is an issue pertaining to several modern cryptosystems. Since cryptosystems use keys to encrypt and decrypt data, a large vulnerability opens regarding secure access to the keys. Depending on the risk associated with the data, some systems opt for computationally secure encryption techniques, and therefore are the most susceptible to known-key attacks. An attacker with a user's key can decrypt all information that was encrypted using that key. This is why it is critical for a user to never share their private keys with anyone, for risk of it being intercepted.

2. A fundamental cryptographic principle states that all messages must have redundancy. But we also know that redundancy helps an intruder tell if a guessed key is correct. Consider two forms of redundancy.
    - First, the initial n bits of the plaintext contain a known pattern.
    - Second, the final n bits of the message contain a hash over the message.

    From a security point of view, are these two equivalent? Discuss your answer.

    No, these are not equivalent. That is because in the first case if there is a known pattern, attackers can use this pattern to increase their certainty of a guessed key being correct. With a pattern, the redundancy will repeat producing a cipher text with patterns. A has over the message, however, will obscure any obvious patterns making the hacking process much more difficult by increasing confusion. The pattern approach provides confusion; however, the hash approach provides confusion and diffusion, making it the better choice for redundancy.

3. Suppose that a message has been encrypted using DES in ciphertext block chaining mode. One bit of ciphertext in block Ci is accidentally transformed from a 0 to a 1 during transmission. How much plaintext will be garbled as a result?

    ON PAPER

4. The following is a ciphertext with Caesar Cipher, please analyze it, and give the corresponding plaintext and the used key.

   DRO MSDI LBSWC GSDR CEWWOB'C NOVSQRDC, GSDR MYVYBPEV ZBYNEMO SX DRO WKBUOD CDKXNC KXN RKGKSSKX WECSM CZSVVSXQ YXDY LOKMROC.

   - Looking at the cipher text I notice an apostrophe, which is indicates that an 's' will immediately follow. This is a trait of the English language where the vast majority of words that contain an apostrophe end in an 's'. However, it may also be a 't' for example, so this is not a definitive clue.
   - Also considering that the message was only encrypted using a Caesar-cipher, the search space for a shift value is only 26, since there are 26 letters in the English alphabet. This opens the possibility of a brute force attack. The attack can be quickly executed since the message is short and the search space is relatively small.

   Using a brute force attack, starting at 'a', I recovered the plain text to be:

   "THE CITY BRIMS WITH SUMMER'S DELIGHTS, WITH COLORFUL PRODUCE IN THE MARKET STANDS AND HAWAIIAN MUSIC SPILLING ONTO BEACHES."

   Which is uncovered using a shift value of 16.

5. Please complete the following two tables and describe why Z11 and Z ∗ 11 [6] are abelian groups. abelian groups.

Z = x + y mod 11	X											
Y		0	1	2	3	4	5	6	7	8	9	10
	0	0	1	2	3	4	5	6	7	8	9	10
	1	1	2	3	4	5	6	7	8	9	10	0
	2	2	3	4	5	6	7	8	9	10	0	1
	3	3	4	5	6	7	8	9	10	0	1	2
	4	4	5	6	7	8	9	10	0	1	2	3
	5	5	6	7	8	9	10	0	1	2	3	4
	6	6	7	8	9	10	0	1	2	3	4	5
	7	7	8	9	10	0	1	2	3	4	5	6
	8	8	9	10	0	1	2	3	4	5	6	7
	9	9	10	0	1	2	3	4	5	6	7	8
	10	10	0	1	2	3	4	5	6	7	8	9

Z = x * y mod 11	X											
Y		0	1	2	3	4	5	6	7	8	9	10
	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	1	2	3	4	5	6	7	8	9	10
	2	0	2	4	6	8	10	1	3	5	7	9
	3	0	3	6	9	1	4	7	10	2	6	8
	4	0	4	8	1	5	9	3	6	9	3	7
	5	0	5	10	4	9	3	8	2	7	1	6
	6	0	6	1	7	2	8	3	9	4	10	5
	7	0	7	3	10	6	2	9	5	1	8	4
	8	0	8	5	2	10	7	4	1	9	6	3
	9	0	9	7	5	3	1	10	8	6	4	2
	10	0	10	9	8	7	6	5	4	3	2	1

Both Z_{11} and Z^*_{11} are abelian groups because they both follow the four axioms that define an abelian group. Closure, associativity, existence of identity, existence of inverse, and commutativity. This is because both groups produce elements within the group, it is cyclical in nature, and only supports or performs addition or multiplication operations which are closed under associativity, and commutativity.

6. Prove the following:
   a) [(a mod n) + (b mod n)] mod n = (a + b) mod n
      ON PAPER
   b) [(a mod n) × (b mod n)] mod n = (a × b) mod n
      ON PAPER

7. Prove the following:
   a) Prove the One-time padding is provably secure.
      One-time-padding depends on the randomness of the key. However, random is a difficult concept to define. In the field of cryptography we define an event as random if has two distinct traits, unpredictability and balanced. These mean that the probability of predicting the event (next bit) is no greater than 0.5, and that the distribution of all outcomes is about equal.
      ON PAPER

   b) Prove the Fermat's Little Theorem a ^ (p−1) ≡ 1 mod p, where p is prime and gcd(a, p) = 1.
      ON PAPER

   c) Prove that there are infinitely many primes.
      ON PAPER

8. Using the extended Euclidean algorithm, find the multiplicative inverse of:
   i) 1234 mod 4321
      ON PAPER

   ii) 550 mod 1769
      ON PAPER

9. Suppose Alice and Bob share the common modulus n = p × q = 35263, but have different public private key pairs (e1 = 17, d1) and (e2 = 23, d2). If David wants to send a message M to Alice and Bob, he first computes the cipher text C1 = Me1 mod n for Alice, the value of C1 is 28657, and also computes the cipher text C2 = Me2 mod n for Bob, the value of C2 is 22520. Finally, David sends (C1, C2) to Alice and Bob, respectively. Now, suppose a passive adversary A eavesdrops the ciphertexts (C1, C2). Can the adversary A recover message M just from (C1, C2) and the public keys (n, e1, e2)? If the adversary A can, please show what strategy that the adversary A would apply, and give the value of message M as well.
   ON PAPER