CS.201P: Introduction to Computer Security 1/11/2019

Homework 1

Due Monday 1/21/2019, 11:59pm, by upload to gradescope.com

Solve the following problems from the [GT] textbook:

1. Exercise R-1.17

Problem R-1.17

The English language has an information content of about 1.25 bits per character. Thus, when using the standard 8-bit ASCII encoding, about 6.75 bits per character are redundant. Compute the probability that a random array of t bytes corresponds to English text.

Solution:

1st) Since each byte has 8 bit, so the t bytes random array has the number of T = (2^8)^t = 2^(8t).

2nd) Given that the information content of English text is 1.25 bits per character, the number of t-byte arrays corresponding to English text is E = (2^1.25)^t = 2^(1.25*t).

3rd) Thus, the probability that a random array of t bytes corresponds to English text is E/T = 2^(-6.75t)

2. Exercise R-1.18

Problem R-1.18

Suppose that a symmetric cryptosystem with 32-bit key length is used to encrypt messages written in English and encoded in ASCII. Given that keys are short, an attacker is using a brute-force exhaustive search method to decrypt a ciphertext of t bytes. Estimate the probability of uniquely recovering the plaintext corresponding to the ciphertext for the following values of t: 8, 64, and 512.

Solution:

1st) Brute-force decryption generates 2^32 candidate plaintexts, one for each possible key value.

2nd) Each plaintext has probability 2^(–6.75t) of being English text.

3rd) Thus, the attack is expected to produce 2^(32–6.75t) candidate English plaintexts.

4th) Since the number of plaintext to be found (unicity distance) is less than 1 for the given values of t = 8, 64, 256, the attack is expected to always recover the plaintext.

3. Exercise R-1.19

Suppose you could use all 128 characters in the ASCII character set in a password. What is the number of 8-character passwords that could be constructed from such a character set? How long, on average, would it take an attacker to guess such a password if he could test a password every nanosecond?

Solution:

1st) There are 128^8 possible passwords with 8 ASCII characters.

2nd) It will take on average (expected on probability):

$$1 * \frac{1}{128^8} + 2 * \frac{128^8-1}{128^8} * \frac{1}{128^8-1} + 3 * \frac{128^8-1}{128^8} * \frac{128^8-2}{128^8-1} * \frac{1}{128^8-2} + \cdots$$

$$= \frac{1}{128^8} * (1 + 2 + \cdots + 128^8)$$

$$= \frac{(1+128^8)}{2} \text{ (times)}$$

guesses to get the right password.

3rd) When guessing a password takes 10^{-9} seconds; the total time is the product result

$$= \frac{(1+128^8)}{2} \text{ (times) * 1e-9 (seconds/times)}$$

$$= 36,028,797 \text{ seconds} \sim\sim \text{ about 417 days.}$$

4. Exercise R-1.22

R-22 The HF Corporation has a new refrigerator, the Monitator, which has a camera that takes a picture of the contents of the refrigerator and uploads it to the HF Corporation's web site. The Monitator's owner can then access this web

site to see what is inside their refrigerator without opening the door. For security reasons, the HF Corporation encrypts this picture using a proprietary algorithm and gives the 4-digit PIN to decrypt this picture to the Monitator's owner, so he or she can get access to the pictures of their Monitator's interior. What are the security concerns and principles that this solution does and doesn't support?

Solution:

There are 10 principles of the security concern, let's analysis them:

1st) *Economy of mechanism*. For the refrigerator, it has simplicity process for the picture and check. So support.

2nd) *Fail-safe defaults*. For the refrigerator, it was not mentioned about the default configuration. So we don't know.

3rd) *Complete mediation*. Every access to a resource is checked for compliance with a protection scheme. So support.

4th) *Open design*. The security architecture and design of a system should be made publicly available, since it use proprietary algorithm, so not support.

5th) *Separation of privilege*. Requirement to achieve access to restricted resources or have a program perform some action. So support.

6th) *Least privilege*. Each program and user of a computer system should operate with the bare minimum privileges necessary to function properly. Since the owner can get access to the pictures of their Monitator's interior, so not support.

7th) *Least common mechanism*. In systems with multiple users, mecha- nisms allowing resources to be shared by more than one user should be minimized. Since no multiple users, so support.

8th) *Psychological acceptability*. This principle states that user interfaces should be well designed and intuitive, and all security-related set- tings should adhere to what an ordinary user might expect. It seems support, at least for me to hear of this process.

9th) *Work factor*. According to this principle, the cost of circumventing a security mechanism should be compared with the resources of an attacker when designing a security scheme. It is low cost, since the refrigerator isn't important, so support.

10th) *Compromise recording*.This principle states that sometimes it is more desirable to record the details of an intrusion than to adopt more sophisticated measures to prevent it. For the refrigerator, it was not mentioned about the default configuration. So we don't know.

5. Exercise R-1.23

R-23 During the 2008 U.S. Presidential campaign, hackers were able to gain access to an email account of Vice Presidential candidate, Sarah Palin. Their attack is said to have involved tricking the mail system to reset Governor Palin's password, claiming they were really Palin and had forgotten this password. The system asked the hackers a number of personal questions regarding Palin's identity, including her birthday, zip code, and a personal security question—"Where did you meet your spouse?"—all of which the hackers were able to answer using data available on the Internet. What kind of attack is this an example of? Also, what degree of security is provided by a password reset feature such as this?

Solution:

Pretexting, where hackers request the new password, while pretending to be someone else by claiming that they are the real users. Then the security system will ask different questions about that user to find out whether or not the person who is asking for a new password is the same or not to reset the user's password. Hackers can easily find the answers to these questions by using internet and different social networking sites.

In this case there are some security concerns as it violates confidentiality and assurance that is provided by the service that is being used by Palin. They have provided a confidential way and assurance to use their service, but this approach is not secure nor effective. And there are some privacy concerns as well as the owner's personal information can be exposed and then it could be used for the wrong reasons.

6. Exercise C-1.1

C-1 Describe an architecture for an email password reset system that is more secure than the one described in Exercise R-23, but is still highly usable.

Solution:

The key is to again make sure it is the user itself. So I can raise up two solution as example:

The first solution is to send the reset code to the user's related phone

number, it has more probability that the phone is with the real user.

Another solution may be based on some authenticity, like the use of digital signatures, etc.

7. Exercise C-1.10. In your attack assume that the public key encryption scheme E is deterministic!

C-10 As soon as Barack took office, he decided to embrace modern technology by communicating with cabinet members over the Internet using a device that supports cryptographic protocols. In a first attempt, Barack exchanges with Tim brief text messages, encrypted with public-key cryptography, to decide the exact amounts of bailout money to give to the largest 10 banks in the country. Let p_B and p_T be the public keys of Barack and Tim, respectively. A message m sent by Barack to Tim is transmitted as $E_{p_T}(m)$ and the reply r from Tim to Barack is transmitted as $E_{p_B}(r)$. The attacker

can eavesdrop the communication and knows the following information:

- Public keys p_B and p_T and the encryption algorithm
- The total amount of bailout money authorized by congress is $900B
- The names of the largest 10 banks
- The amount each bank will get is a multiple of $1B
- Messages and replies are terse exchanges of the following form:

  Barack: How much to Citibank?
  Tim: $144B.
  Barack: How much to Bank of America?
  Tim: $201B.
  . . .

Describe how the attacker can learn the bailout amount for each bank even if he cannot derive the private keys.

Solution:

The attacker performs a dictionary attack. Since the message format is fixed and there are 10 possible banks and 900 possible bailout amounts, the attacker encrypts the 10 candidate messages from Barack (one for each bank) using public key p_B, and the 900 candidate responses from Tim (one for each bailout amount), using public key p_T . The attacker then matches the ciphertexts exchanged by Barack and Tim with the precomputed ones and determines the corresponding plaintexts. Note that the attacker does not need access to the private keys used by Barack and Tim.

8. Exercise C-1.11

As a result of the above attack, Barack decides to modify the protocol of Exercise C-1.10 for exchanging messages. Describe two simple modifications of the protocol that are not subject to the above attack. The first one should use random numbers and the second one should use symmetric encryption.

Solution:

In the first case, Barack can add a random value with b bits to his message, which increases the number of possible messages by a factor of 2^b. Or he can use a hash function.

In the second case, Barack can first encrypt a (random) key K for a symmetric encryption scheme, and then send the encrypted version of K along with an encryption of his actual message using key K and the symmetric cryptosystem.

9. Exercise C-1.16.

C-16 Consider the following method that establishes a secret session key k for use by Alice and Bob. Alice and Bob already share a secret key K_{AB} for a symmetric cryptosystem.

a. Alice sends a random value N_A to Bob along with her id, A.
b. Bob sends encrypted message $E_{K_{AB}}(N_A), N_B$ to Alice, where N_B is a random value chosen by Bob.
c. Alice sends back $E_{K_{AB}}(N_B)$.
d. Bob generates session key k and sends $E_{K_{AB}}(k)$ to Alice.
e. Now Alice and Bob exchange messages encrypted with the new session key k.

Suppose that the random values and the keys have the same number of bits. Describe a possible attack for this authentication method.

Can we make the method more secure by lifting the assumption that the random values and the keys have the same number of bits? Explain.

Assume that each party verifies the encrypted message sent by its counterparty. I.e., when Alice receives Bob's ciphertext C_B which Bob sends in step (b), she decrypts $m_B = D_{K_{AB}}(C_B)$ and drops the protocol unless $m_B = N_A$. Likewise, when Bob receives Alice's ciphertext C_A which Alice sends in step (c), he decrypts $m_A = D_{K_{AB}}(C_A)$ and drops the protocol unless $m_A = N_B$.

Solution:

In the first three steps, the attacker, Eve, observes random values N_A and N_B and their ciphertexts, $E_{K_{AB}}(N_A)$ and $E_{K_{AB}}(N_B)$, computed by Alice and Bob. In the fourth step, Eve replaces message $E_{K_{AB}}(k)$ sent by Bob to Alice with $E_{K_{AB}}(N_A)$ (or $E_{K_{AB}}(N_B)$). Thus, Eve induces Alice to use N_A (or N_B) as the session key, which is known to Eve. When Alice sends a message to Bob using session key N_A (or N_B), Eve can decrypt it.

This attack does not work when the key has length different from the random values as Alice can check the length of the key.

10. Exercise C-1.17

C-17 Alice and Bob shared an n-bit secret key some time ago. Now they are no longer sure they still have the same key. Thus, they use the following method to communicate with each other over an insecure channel to verify that the key K_A held by Alice is the same as the key K_B held by Bob. Their goal is to prevent an attacker from learning the secret key.

a. Alice generates a random n-bit value R.
b. Alice computes $X = K_A \oplus R$, where $\oplus$ denotes the exclusive-or boolean function, and sends X to Bob.
c. Bob computes $Y = K_B \oplus X$ and sends Y to Alice.
d. Alice compares X and Y. If $X = Y$, she concludes that $K_A = K_B$, that is, she and Bob have indeed the same secret key.

Show how an attacker eavesdropping the channel can gain possession of the shared secret key.

Solution:

The attacker eavesdrops X and Y. The attacker recovers key K_B by computing $X \oplus Y = X \oplus (K_B \oplus X) = (X \oplus X) \oplus K_B = K_B$.