National University of Computer & Emerging Sciences, Karachi
Spring 2020 CS-Department
Final Exam

1st Jul 2020, 9:00 am – 12:00 am

Course Code:CS-404	**Course Name:Information System Security**
Instructor Name :Engr-Shahbaz Akhtar Siddiqui	
Student Roll No:	**Section No**

Instructions:

Time: 60 minutes. **[50 Total Points]**

Rules:

---

1. Join For Exam following class link with your NU account
https://classroom.google.com/u/0/c/MTE5NTcwMDEwNTE5 Class Code **gsp45fe**
2. For any query join Whatsapp Group (https://chat.whatsapp.com/DxgY4B0YOLKAp7APXYC4zJ)
3. The script should be handwritten. Use plan-A4 size paper starting with roll Number in header and
4. Submit each answer in combine PDF format

Question 1: **[10 Points]**

Please See the Link (https://www.youtube.com/watch?v=X84FpLmMm7M) .Answer the following questions

1. What is a purpose secure software update mechanism?

The software update is an important mechanism by which security changes and improvements are made in software, but there is also an important point related to secure software update which means that your software is updated through the secure procedure
Some keys points (that should be expected from Students)
1. Update come from trusted websites
2. There will be a mechanism of authentication which enable the power to install the update of software
3. Prompt message continue regarding the update of the message
4.Log file maintain regarding the update of software

2.Explain the two use-cases of network forgery that explained in the video

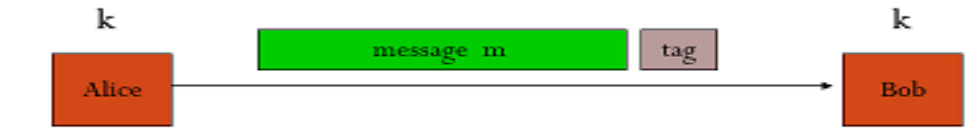
HTTP auth problems

- Hardly used in commercial sites
  - User cannot log out other than by closing browser
    - What if user has multiple accounts?
    - What if multiple users on same computer?
  - Site cannot customize password dialog
  - Confusing dialog to users
  - Easily spoofed
  - Defeated using a TRACE HTTP request (on old browsers)

Home network access through http Api so there will be chance of spoofing

3. Proposed a secure mechanism through which the defined use-case become secure

Message integrity: MACs



Generate tag: $tag \leftarrow S(k, m)$

Verify tag: $V(k, m, tag) \stackrel{?}{=} \text{`yes'}$

- MAC is short information
  - Provide integrity and authenticity assurances on the message.
  - Integrity assurances detects accidental and intentional message changes
  - Authenticity assurances affirms the message's origin

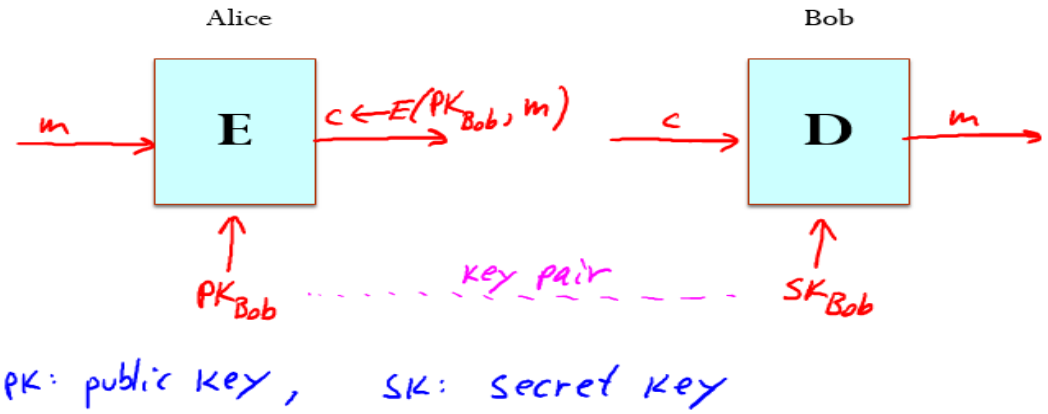
Def: **MAC** $I = (S,V)$ defined over (K,M,T) is a pair of algs:

- $S(k,m)$ outputs t in T
- $V(k,m,t)$ outputs `yes' or `no'

Question 2: **[10 Points]**

Please See the Link (https://www.youtube.com/watch?v=X84FpLmMm7M) .Answer the following questions

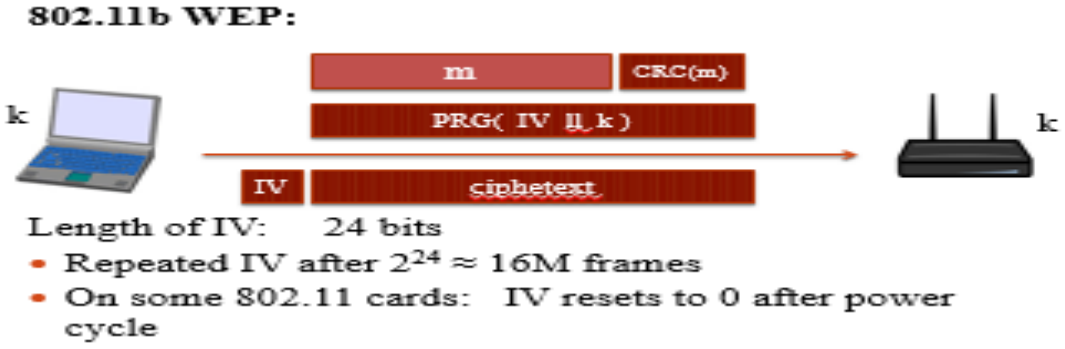
1. **Explain the use case of Single Use Key and Multi Use key** **[2 Points]**



2. Why Cryptography is not the solution of all security Problems

Cryptography is defined as a mathematical formulation to maintain perfect secrecy in communication which enables integrity, confidentiality, availability in the message, but cryptography is not a solution to all security problems, Suppose an organization store the cache of employees web browsing in a cache server . The normal user if access this server he/she able to find the user credential by putting this record to any penetration tools, this is not a cryptographic problem but a bad implementation of access-rights this is why we say Cryptography is not a solution of all security problem

3. Give Mathematical example of Cryptographic algorithm for wireless communication

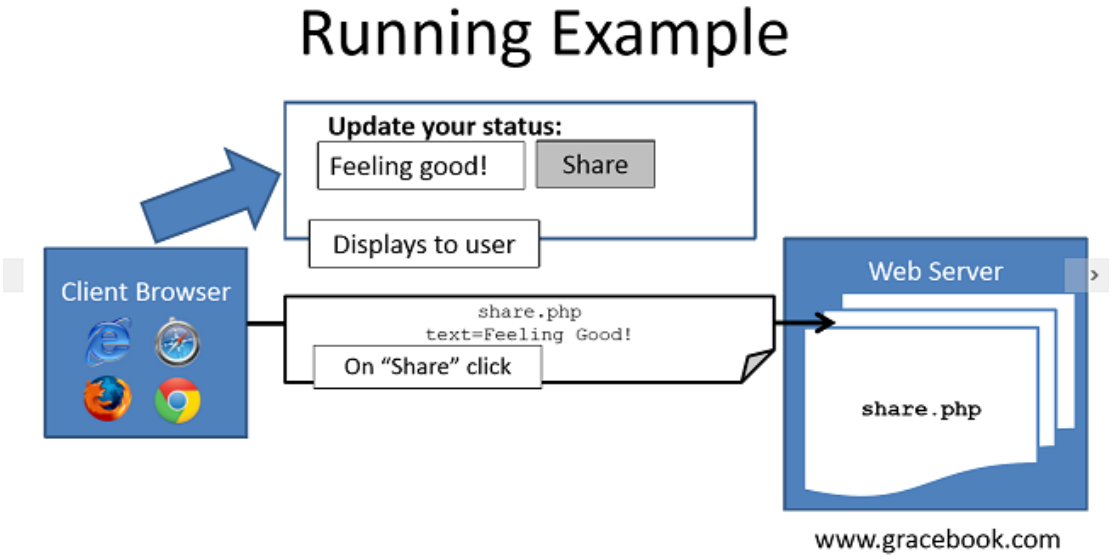


Explain this picture

Question 3: **[10 Points]**

Please See the Links (https://www.youtube.com/watch?v=dMwxIHIabeg) (https://www.youtube.com/watch?v=jPcdaCyUEVM&list=PLf0TFb7VbRljK7uX6MmVqpVarVb0tC8my&index=25&t=0s) .Answer the following questions

1. Explain Cross-Site request forgery mechanism through conceptual diagram. Mention each step involved in defined use-case in videos [2 Points]



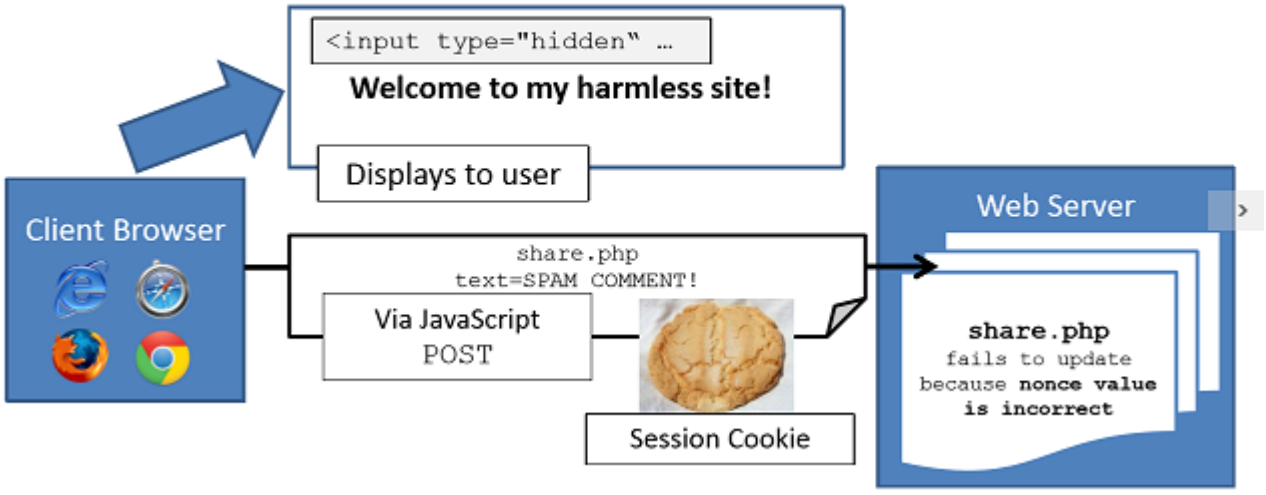
2. How session ids and cookies are sent automatically to the browser during cross site request forgery attack [3 Points]

- Alice logs in at **login.site.com**
  login.site.com sets session-id cookie for **.site.com**
- Alice visits **evil.site.com**
  overwrites .site.com session-id cookie with session-id of user "badguy"
- Alice visits **cs155.site.com** to submit homework.
  cs155.site.com thinks it is talking to "badguy"

Problem: cs155 expects session-id from login.site.com; cannot tell that session-id cookie was overwritten

3. Prosposed a mechanism that protect from Request forgery attack [5 Points]

Attack Case



Question 4: **[10 Points]**

1. The following SQL statement is sent to the database to add a new user to the database, where the content of the $name and $passwd variables are provided by the user, but the EID (Employ ID) and Salary fields are set by the system. How can a malicious employee set his/her salary to a value higher than 80000?

$sql = "INSERT INTO empoyee (Name, EID, Password, Salary)VALUES ('$name', 'EID6000', '$passwd', 80000)";

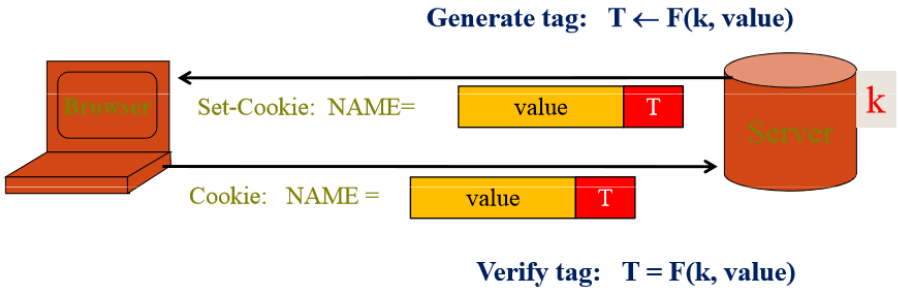
```
pg_query("SELECT * from users WHERE
            uid = 'admin'--'   AND  pwd = 'f';");

pg_query("SELECT * from users WHERE
            uid = 'admin';");

pg_query("SELECT * from users WHERE
            uid = 'admin'; DROP TABLE users;--' AND
            pwd = 'f';");
```

2. Explain the Cryptographic Checksum solution for cookies integrity

Solution: Cryptographic Checksums

Goal: Data Integrity

Requires secret key ***k*** unknown to browser



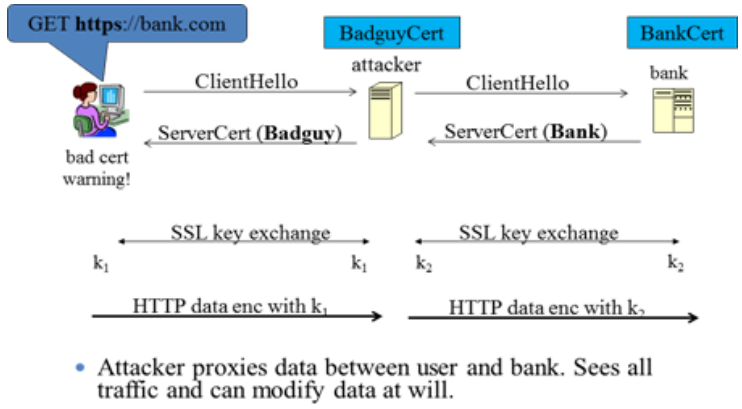
3. An application proxy firewall is able to scan all incoming application data for viruses. It would be more efficient to have each host scan the application data it receives for viruses, since this would effectively distribute the workload among the hosts. Why might it still be preferable to have the application proxy perform this function?

The primary advantage of an application proxy is that it has a complete view of connections and application data. Consequently, it can have as comprehensive of a view as the host itself could have. As a result, the application proxy is able to filter bad data at the application layer (such as viruses) while also filtering bad packets at the transport layer. The disadvantage of an application proxy is speed or, more precisely, the potential lack thereof. Since the firewall is processing packets to the application layer, examining the resulting data, maintaining state, etc., it is doing a great deal more work than packet filtering firewalls.

Question 5: **[10 Points]**

Please See the Links (https://www.youtube.com/watch?v=FC7SJXjbgyc) .Answer the following questions

1. The Facebook web server runs on a secure application layer protocol HTTPS. While running on a secure protocol, how the attacker able to forge the user's credentials? illustrate with the help of a diagram [2 Points]



Explain this picture in detail

2. Explain the 2-Factor authentication system deployed by Google. What are the limitations of this authentication mechanism? How an attacker can by-pass or compromise the 2-factor authentication? [8 Points]

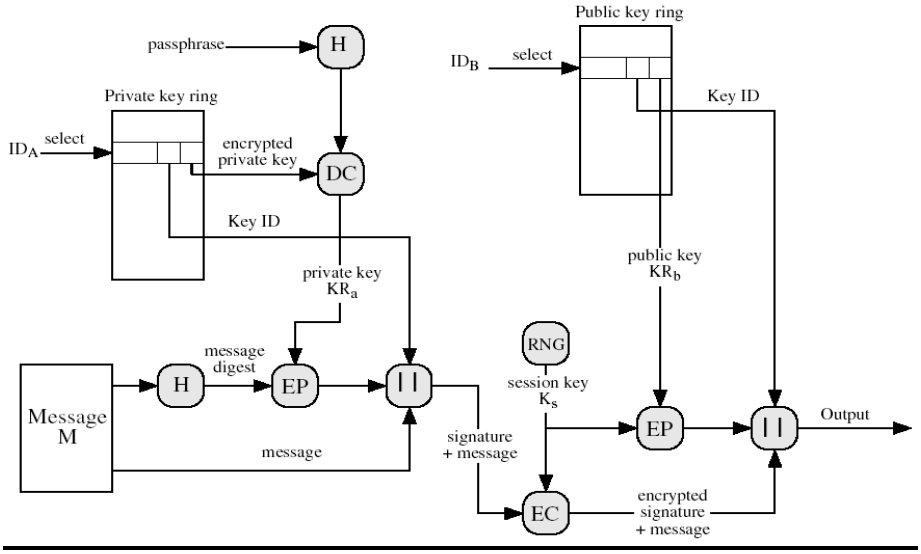
1. Delay in delivery of sms
2. SMS gateway compromise
3. Unavailability of Devices
4. weak SMS Encryption

Explain in detail

Question 6: **[10 Points]**

Please See the Links (https://www.youtube.com/watch?v=mf7x9IiJndY) .Answer the following questions

1. A military battalion requires an email to be sent to the Army Chief that needs to be securely transmitted over a public network. You, as an IT security specialist, are given this task to perform such operation using public-key cryptosystem. Explain your solution with the help of a diagram.



[5 Points]

2. In a public-key system RSA, you intercept the ciphertext C =10 sent to a user whose public key is e=5, n=35. What is the plaintext M? [5 Points]

We know that the ciphertext C = 10, and the public key PU = {e, n} = {5, 35}. Based on Euler's Totient function, φ (n) is defined as the number of positive integers less than n and relatively prime to n. We could find that φ (n) = 24.

Now, we guess two prime numbers p and q. Let p be 5 and q be 7. All the following conditions will be satisfied based on the guess: (1) n = p*q = 5*7=35 (2) φ (n) = (p-1)(q-1)=(5-1)(7-1)=4*6=24 (3) gcd(φ (n), e) = gcd(24, 5) =1, 1< e < φ (n)

We calculate d in the next step. Based on RSA key generation algorithm, d ≡ e-1 mod φ (n) which is equivalent to ed ≡ 1 mod φ (n) or ed mod φ (n) =1. (chapter 9.1 page 269)

We have e = 5, φ (n) = 24. So, 5d mod 24 =1, and d = 5.

Now, we find the private key PR = {d, n} = {5, 35}.

Based on RSA decryption algorithm, M = C^d mod n = 10^5 mod 35 = 5

We also can verify the correctness by the RSA encryption algorithm as the following: C = M^e mod n = 5^5 mod 35 = 10 Therefore, we conclude that the plaintext M is 5.