CSE 345/545: Foundations to Computer Security

Assignment: 1

Maximum marks: 100

Deadline for submission: 23 Feb 2025, 11:59 PM

Instructions:

- Follow the name convention and submission instructions for every question carefully.
- Your file names should follow the convention qi.xx or qi_report.pdf where i is the question number from 1 to 5.
- Keep your code efficient, make sure output matches the requirements.
- Post your queries on Google Classroom.
- Strict plagiarism checks will be conducted for each question. The assignment must be done individually.

1. Cryptography [30 marks]

You might be familiar with symmetric and asymmetric key cryptography. Both methods have their advantages and limitations. People who want to correspond via symmetric key cryptography have to share the key. The process is faster compared to asymmetric cryptography since the keys are much shorter, but if the channel being used for key exchange gets compromised, the entire system becomes insecure.

A popular algorithm to achieve asymmetric cryptography is RSA. One method to facilitate secure symmetric key exchange is to share them via asymmetric cryptography. Thereafter, all communication between the two parties would be secured through symmetric key cryptography. Suppose, Bob and Alice want to communicate via this paradigm.

Consider that Salsa20 (with a 16 byte/128 bit key) will be used for symmetric encryption. You can use the PyCryptodome library for the same.

A. Alice generates the shared symmetric key: Generate random 16 byte string. This would be used as the key for Salsa20 encryption. Return this byte string. [3]
B. Bob generates his asymmetric keys: Use the GMP library to implement RSA. Take prime numbers ‘p’ and ‘q’ as inputs and generate ‘n’, ‘e’ and ‘d’ for Bob. (n, e) is the public key, (n, d) is the private key. Return Bob’s public key and private key. [7]
C. Alice uses Bob’s public key to encrypt K: Use the symmetric key generated in part 1.a. as the message and encrypt it using Bob’s public key. Return the ciphertext ‘c’. [5]
D. Bob obtains the shared symmetric key: Given the ciphertext ‘c’, use Bob’s private key to decrypt the message. Bob has now received the shared symmetric key K. Return K.[5]

E. Bob encrypts a message using shared symmetric key: Use the key K to encrypt a given message 'm' (byte string) on Bob's end and return the encrypted message.[5]
F. Alice decrypts Bob's message: Given the ciphertext, use the shared key K to decrypt Bob's message at Alice's end and return the decrypted message. [5]

Please note:

- Prime integers p, q are up to 1023 digits long and should be taken as inputs.
- The message m is a byte string.
- Avoid using loops to choose 'e'.
- You are free to create helper functions.
- In real world applications, Bob's private key would not be known to anyone except Bob. Here, you have been asked to return the private key for the sake of making the process clearer.

Submission: A single python file q1.py; q1_report.pdf - Report that explains the flow of your code with a sample Input/Output.

2. Authentication [25 marks]

A "JSON Web Token", or "JWT", is a stateless method of authentication that has recently grown in popularity. The JWT string contains the signature of its payload, signed using a private key/secret and following a chosen algorithm – this ensures the token's integrity. Read more about the structure, and other standards of the JWThere.

A. a. Define a Python function **verifyJwt(token, secret)** that takes in a JWT and a secret as arguments. Validate the token's signature against the supplied secret. If it is valid, return the decoded payload. Otherwise, throw an exception. The function should implement checks for at least two symmetric algorithms of your choice. Note: You are not allowed to use the "PyJWT" library, or any other library implementing JWT verification. [10]
B. Consider the following JWT:


```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJmY3MtYXNzaWdubWVudC0xIiwiaWF0IjoxNTE2MjM5MDIyLCJleHAiOjE2NzI1MTE0MDAsInJvbGUiOiJ1c2VyIiwiZW1haWwiOiJhcnVuQGlpaXRkLmFjLmluIiwiaGludCI6Imxvd2VyY2FzZS1hbHBoYW51bWVyaWMtbGVuZ3RoLTUifQ.LCIyPHqWAVNLT8BMXw8_69TPkvabp57ZELxpzom8FiI
```

Your task is to retrieve the secret used to sign the above JWT. Once retrieved, create a new JWT with the same secret, and change the role to “admin”. Document and explain your steps. [10]

C. If a single secret key is used to sign all JWTs for user authentication, and that key gets leaked, all user data in the application is at risk. What modification to the authentication architecture can you propose such that widespread damage can be prevented, if a JWT signing secret is cracked? [5]

Submission: A single python file q2.xx, a report for parts b and c, q2_report.pdf

3. Digital Certificates [20 marks]

This question would require you to get familiar with crt.sh and dnsdumpster. Your task here is to simply use dnsdumpster and crt.sh to fetch all the subdomains of iiitd.edu.in.

A. Once you have done that, fetch the private IP addresses of these subdomains and list them (subdomain:[PRIVATE_IP]). [7.5]
B. Explain your methodology and try automating this process as much as you can by writing a script in any language you are comfortable coding in. [7.5]
C. What according to you can be the security implications of private IP addresses being leaked to the public, i.e. if this list of subdomain and private IP addresses is given to an attacker outside the IIITD network, how can they leverage the same? [5]

Submission: q3.xx: single code file in any language you are comfortable with.; q3_report.pdf(a single report for parts a, b and c)

4. Port Knocking [15 marks]

Install and configure knockd on your VM such that by knocking a certain sequence of ports you are able to open and close port 22 SSH. The iptable rules should be made keeping all corner conditions in mind.

A. Explain as to how you went ahead and did all the above along with the choice of iptable rules and the sequence of ports. [10]
B. Why should one prefer doing this over TCP instead of UDP? [2.5]
C. What is the default choice of ports in the knockd configuration. Is it safe? [2.5]

Submission: A report q4_report.pdf

5. **Firewall [10 marks]**

You have been hired as a Security Engineer at a startup that recently faced a DDoS attack and data exfiltration attempt. Your task is to design and implement firewall rules to enhance security while maintaining business operations i.e IP filtering, logging and DDoS prevention.

Firewall requirements:

- Allow only admin IPs(lets say 192.168.1.3) to access SSH/RDP.
- Allow HTTP/HTTPS but block access from blacklisted IP range 103.25.231.0/24.
- Allow only internal IPs to access the database server(consider default port for databases).
- Enable logging for debugging and tracking unauthorized access.
- Configure rate limiting to prevent excessive HTTP requests from a single IP.
- Set a limit of 5 connections per second per IP to prevent overloading.

Write all commands and steps you have taken to achieve the final firewall for your server. You can reuse the same VM from question 3 but make sure you flush the firewall rules to remove any preset rules. [10]

Submission: A report q5.pdf showing the commands you have used and screenshot of your final firewall.