EEC 765: Introduction to Cryptography and Computer Security
The University of Kansas

Homework 1 - Fall 2023

Due: Thursday October 12, 2023 in class

Name:

Please sign the following honor pledge.

On my honor, as a student, I have neither given nor received unauthorized aid on this academic work.

Signature:

Problem 1 (3 pts)

Public-key cryptography is often used to establish a shared secret key, so that the subsequent communication can be conducted using the more efficient symmetric encryption approach. Consider the following protocol.

1. Alice sends Bob her public key PK_1
2. Bob sends Alice his public key PK_2
3. Alice randomly generates K_1 and sends Bob $\{K_1\}_{PK_2}$
4. Bob randomly generates K_2 and sends Alice $\{K_2\}_{PK_1}$
5. Both Alice and Bob concatenate K_1 and K_2, and start communicating using the shared secret key K_1K_2

Describe a potential attack for this protocol.

We assume:

- the attacker has complete control over the communication channel and
- Dolev-Yao model applies (everything BUT the cryptographic primitives may be manipulated)

Problem 2 (4 pts)

The SSH protocol uses Diffie-Hellman key agreement protocol to establish a shared master secret between the server and the client, and uses the master secret to derive two keys for encryption/decryption and message authentication. Assumption: Cryptographic primitives hold (Dolev-Yao model applies).

a. (2 pts) Diffie-Hellman key agreement protocol is vulnerable to man-in-the-middle (MitM) attacks. Describe the attack in the context of SSH and how this would impact the security of the user's login credentials: 1) if the user uses password authentication; 2) if the user uses public key-based authentication.

b. (2 pts) To address the MitM problem, the SSH protocol allows the client to verify the server's identity by checking the digital signature produced by the server on the server's DH transcript – the client knows the server's public key. Explain why this will thwart the MitM attack on the SSH protocol. What does the client need to do in order to verify that the shared secret is established with the server that possesses the private key corresponding to the server's public key?

Problem 3 (3 pts)

Below is the message format for a browser response to access a password-protected web page using HTTP digest authentication.

```
GET URI HTTP/1.1
Host:  URL
...
Authorization:  Digest username="UserName", realm="Realm", nonce="Nonce",
uri="URI", algorithm=SHA-512, response="Response", qop=QoP, nc=NonceCount,
cnonce="ClientNonce"
```

Upon receiving the response from the client's browser, the web server will extract the fields `UserName, Realm, Nonce, URI`, etc. from the message and perform the following validation:

1. Use `UserName` and `Realm` to retrieve D_1 = SHA-512sum(`UserName:Realm`:Password) from the server's password file
2. Compute D_2 = SHA-512sum(`GET:URI`)
3. Compute r = SHA-512sum(D_1`:Nonce:NonceCount:ClientNonce:QoP:`D_2)
4. If r == **Response**, authentication succeeds and the content of `URI` is returned; otherwise authentication fails and an error code is returned to the client.

Point out a severe flaw in the above server implementation, and explain how to fix this implementation.
Assumptions: Cryptographic primitives hold i.e., Dolev-Yao model applies. The way the server stores the clients' passwords in its password file is out-of-scope (in other words, we assume it's secure).