Homework 5, David Rasoly.

Question 1.

Once clicking an “opt-out” or unsubscribe, one or more of the following can occur:

- The link can contain a redirect to a website that is infected with malware or contain a malware attachment file.
- The bulk could be sent to various emails, some active and some that are not. Once opt-out, the unsubscribe list could contain a link to an API that lets the sender know that the specific address is actually active, and someone who checks his or her email frequently is behind that address, this makes the email address worth more for spammers, as there is an advertising potential behind it.
- The sender could potentially know more about you - if the redirected unsubscription link leads to an external website, it can give the website personal data about you such as you browser type, your operating system, IP and geographic which derived from you ip address. This website can deliver you cookies and identify you personally, and identify you once you visit it, making your browsing less anonymous.

Question 2.

I chose to review HP A-MSR Router Series.

The ACL sets rules, such permit or deny for identifying traffic based on IP address and ports either from source and destination.

The ACL breaks down to several categories : WLAN, Basic, Advanced , Ethernet frame headers, User Defined and Simple ACLs. each category has numbers ranged from 100 to 42,767, and support either IPv4 and/or IPv6, depends on category. The range number for each ACL category is unique and a number must be assigned to identify the name of the ACL with exception of the WLAN category, in which a name cannot be assigned.

An ACL configuration example :
Suggests that Alice has access to Harvard’s Canvas device A, let these rules apply :

1. Let Alice connect to Canvas at any time, except between 2:00AM to 4:00AM.
2. Deny Bob’s access (also through device A) from Canvas at all times.

Matching Confguration :

```
[DeviceA-acl6-adv-3000] rule permit ipv6 source [Alice IP] destination [Harvard Canvas Server IP]
[DeviceA-acl6-adv-3000] rule deny ipv6 source [Alice IP] destination [Harvard Canvas Server IP] time-range 2:00AM - 4:00AM.
[DeviceA-acl6-adv-3000] rule deny ipv6 source [BOB IP] destination [Harvard Canvas Server IP]
```

Question 3.

An X.509 certificate is a digital format file that uses a Public Key Infrastructure to assert that a specific public key belongs to assert both the identity of the host or server, and to transfer data between the host and the owner of the certificate in a secure manner, and read the encrypted data transferred by the host.
A Certificate Authority is a server that responsible of managing and granting certificates and public keys. Generally, organizations such as banks, universities and other firms may support and handle a server that issues certificate, to allow secure connection between the certificate holders and the hosts that these certificates grants access to.
Public Key Infrastructure is an asymmetric encryption method, and as such, two keys are used, a private key and a public key, the certificate holds information about both the public key holder and the identity of the issuer. The sender encrypts the information data with the public key of the receiver's certificate, one the message arrives to the receiver, it will be decrypted using the private key. The Certificate Authority issuer will issue a certificate with a unique private key and a public key to the users, and these users will be able to conduct a secure connection over public connections with the trusted host ,that has the public key.

Question 4.

Continuing the explanation of how PKI works from question number 3 - Asymmetric Encryption methodology used by X.509 certificates could use not only to pass data confidentially through encryption, but also to verify a digital signature that was "signed" by the sender. A digital signature is produced by the sender to assure the identity of the sender. Suggest that Alice would like to submit her homework to Bob via email, the following steps will be taken to send the homework digitally signed :

1. Alice will generate a public and private key pair, and share the public key with Bob.
2. Then, alice will sign and encrypt her homework and send the encrypted homework to Bob via email attachment.
3. Bob will use the public key to decrypt and verify Alice's homework.

Question 5.

A SIP proxy server is a server that processes SIP requests between two SIP addresses, and facilitates communication between these entities. It is used to support Voice Over IP by calling the rules that arranges the sequence of actions that take place in order to allow the communication between the two peers, in such a way that the client's device that initiated the call, will be unconcerned with the proxy processes.
To better understand what happened when two entities communicate via SIP proxy, let's assume that Alice calls Bob through a sip proxy server.

1. Alice will send an INVITE to the SIP Proxy Server
2. The SIP Proxy Server will return TRYING to Alice and INVITE Bob.

3. Bob will return RINGING to the Proxy Server, which will be followed with RINGING to Alice.
4. Bob will then return OK to the Proxy Server, which will be followed with OK to Alice.
5. Alice will send ACK to the Proxy Server, which will be followed by ACK to BOB.
6. A media session, that could also contain VOIP will occur between Alice and Bob.
7. Once decided on terminating the session, Alice will send BYE to the Proxy Server, followed by BYE to BOB.
8. BOB will send BYE to the Proxy server, followed by BYE to Alice.

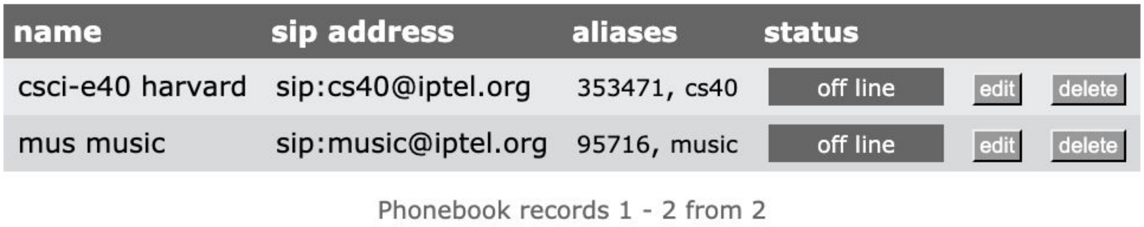
There are different types of SIP Server proxies :

- Stateless proxy - as its name suggests, this Proxy Server is not aware to the state of the call, and simply process commands and packets between the peers, and in case of packet loss they won't be reliable. The advantage of this Proxy Server type is its processing speed and volume.
- Stateful proxy - this Proxy Server store and maintain state. A Transaction Stateful Proxy holds the state of each pending request, and retransmission packets that were lost or timed out. In my opinion, Stateful Proxy servers will be more ideal for VOIP, since it could prevent voice data loss, and maintain quality of voice chat.

Question 6.

I was able to connect and hear music by calling sip:music@iptel.org , by doing the following steps:

- Register myself to iptel.org, and add both cs40 and music address to my account :

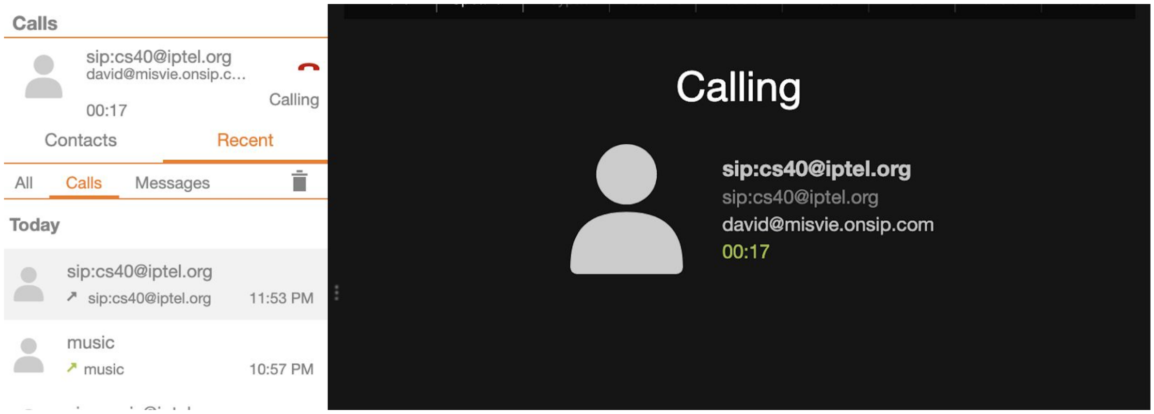


name	sip address	aliases	status		
csci-e40 harvard	sip:cs40@iptel.org	353471, cs40	off line	edit	delete
mus music	sip:music@iptel.org	95716, music	off line	edit	delete

Phonebook records 1 - 2 from 2

- Few hours after I set the account, I saw that the address are constantly offline, hence I opened a new account at onsip.com, the account name is david@misvie.onsip.com.
- I Downloaded, installed and configured a client software called Zoiper5, and logged to with my Onsip account.

- I tried calling cs40 using its sip address several times, it seems that the call goes through but I hear nothing when it answers, I tried to leave some messages, but I have no indication whether you can hear them or not, below is a screenshot of the connection.



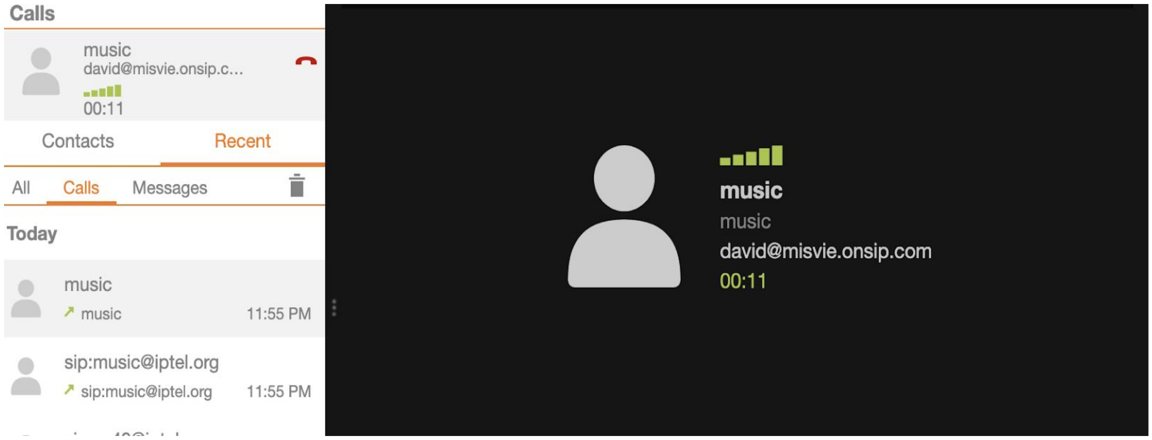
sip:cs40@iptel.org
david@misvie.onsip.c...
00:17
Calling

sip:cs40@iptel.org
sip:cs40@iptel.org 11:53 PM

music
music 10:57 PM

Calling
sip:cs40@iptel.org
sip:cs40@iptel.org
david@misvie.onsip.com
00:17

- After reading the comments at the canvas webpage at the class, I tried calling music, and was able to hear a nice song by The Turtles - “Happy Together”.



music
david@misvie.onsip.c...
00:11

music
music 11:55 PM

sip:music@iptel.org
sip:music@iptel.org 11:55 PM

music
music
david@misvie.onsip.com
00:11

References :

Krishnamurthy, R. (2016). A Framework for Evaluating Server Performance : Application to SIP Proxy Servers.

N.d. . (2016, August, 16).Understanding the different types of SIP servers
Retrieved from : https://www.orbtalk.co.uk

H.P. Documentation (n.d.). HP A-MSR Router Series Configuration Guide.