CSCI 4273 Fall 2014 **Vince Coghlan**

Homework #2

1: Do a literature survey to learn about SMS (Short Message Service). What are the different types of SMS? What kind of application architecture does SMS use? Explain your answer
There is only one kind of SMS, since it is a defined standard of communication in the GSM standard. There are many protocols, however, that either build on top of it, or extend its functionality. These include Nokia Smart Messaging, which adds functionality for pictures and other non-text data, Extended message service, which allows for text messages in various fonts and colors, and Multimedia messaging service, which supports even larger file formats than the other systems. SMS uses a client server architecture Each phone's SME sends the message to a centralized SMC server. This server then relays the data to the correct destination.

2: (Tools exercise) Telnet into a mailserver (telnet mailserver 25) and send an email to yourself and an email to your friend. Submit a print out of message exchanges between SMTP client and server.
You cant telnet to a mailserver anymore since almost no one uses unencrypted mail these days. Thats ok, we can use openssl's s_client to establish a connection the output looks like so (this is pretty much identical to what telnet would look like):

```
$openssl s_client -starttls smtp -connect smtp.colorado.edu:587 -crlf
CONNECTED(00000003)
verify return:0
---
Certificate chain
 0 s:/C=US/postalCode=80309/ST=CO/L=Boulder/street=455 UCB/O=University of Co
   i:/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO High
 1 s:/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO High
   i:/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust Externa
 2 s:/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust Externa
   i:/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust Externa
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIGGzCCBQOgAwIBAgIRAIhvS3txD4kc4cBuyjP4/XAwDQYJKoZIhvcNAQEFBQAw
```

gYkxCzAJBgNVBAYTAkdCMRswGQYDVQQIExJHcmVhdGVyIE1hbmNoZXN0ZXIxEDAO
BgNVBAcTB1NhbGZvcmQxGjAYBgNVBAoTEUNPTU9ETyBDQSBMaW1pdGVkMS8wLQYD
VQQDEyZDT01PRE8gSGlnaC1Bc3N1cmFuY2UgU2VjdXJlIFNlcnZlciBDQTAeFw0x
NDA2MTEwMDAwMDBaFw0xNzA2MTAyMzU5NTlaMIIBDzELMAkGA1UEBhMCVVMxDjAM
BgNVBBETBTgwMzA5MQswCQYDVQQIEwJDTzEQMA4GA1UEBxMHQm91bGRlcjEQMA4G
A1UECRMHNDU1IFVDQjEwMC4GA1UEChMnVW5pdmVyc2l0eSBvZiBDb2xvcmFkbyBh
dCBCb3VsZGVyIC0gT0lUMSkwJwYDVQQLEyBPZmZpY2Ugb2YgSW5mb3JtYXRpb24g
VGVjaG5vbG9neTE0MDIGA1UECxMrSG9zdGVkIGJ5IFVuaXZlcnNpdHkgb2YgQ29s
b3JhZG8gYXQgQm91bGRlcjEQMA4GA1UECxMHU0dDIFNTTDEaMBgGA1UEAxMRc210
cC5jb2xvcmFkby5lZHUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDC
P6LzY1ukt78bK/dEpmBaZpyOLDimpepMKX6PkpVIXQX8Q0mqeAA8pNmaVf0lPQ/m
gZXtaC6b9QFnGoLNcqdYR1hEOhWN7kEwiLq/Ou8cDt12DItF0VoFjVPbebgKm8ZD
CIuKsE4aaQHhbYw5kQ7xZS6F6/QzVoGWpxpfNxsD0e9GXEY4n6BNZV8m9oLgY/Bf
8w1QgIeP0SQP5+NxZtk0yE331FfszrkJTSH7lIRYP0II/h8q1tBkXTbMUYtfOcOe
pWTFQLW06u4wk31laIhsk6jpv+qtdMEx+kPBNkp3rOtb0OlkEkugcwWzo7StwM2a
zABy8GJ2C7V9WUHV8KNfAgMBAAGjggHzMIIB7zAfBgNVHSMEGDAWgBQ/1bXQ1kR5
UEoXo5uMSty4sCJkazAdBgNVHQ4EFgQUjrATxUR0Nrp65PDAnFK2epXp/n0wDgYD
VR0PAQH/BAQDAgWgMAwGA1UdEwEB/wQCMAAwNAYDVR0lBC0wKwYIKwYBBQUHAwEG
CCsGAQUFBwMCBgorBgEEAYI3CgMDBglghkgBhvhCBAEwUAYDVR0gBEkwRzA7Bgwr
BgEEAbIxAQIBAwQwKzApBggrBgEFBQcCARYdaHR0cHM6Ly9zZWN1cmUuY29tb2Rv
LmNvbS9DUFMwCAYGZ4EMAQICME8GA1UdHwRIMEYwRKBCoECGPmh0dHA6Ly9jcmwu
Y29tb2RvY2EuY29tL0NPTU9ET0hpZ2gtQXNzdXJhbmNlU2VjdXJlU2VydmVyQ0Eu
Y3JsMIGABggrBgEFBQcBAQR0MHIwSgYIKwYBBQUHMAKGPmh0dHA6Ly9jcnQuY29t
b2RvY2EuY29tL0NPTU9ET0hpZ2gtQXNzdXJhbmNlU2VjdXJlU2VydmVyQ0EuY3J0
MCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC5jb21vZG9jYS5jb20wMwYDVR0RBCww
KoIRc210cC5jb2xvcmFkby5lZHWCFXd3dy5zbXRwLmNvbG9yYWRvLmVkdTANBgkq
hkiG9w0BAQUFAAOCAQEAxL39tWFJGoTwfM30Z/QxZp22RJYpqRHnQJcF1MX5mNWK
XjQBeoHn73Kt8KVrqGwRT9dR5UdsiR/mXGg7WbpfxHTNJ9hQg7PF4/pX7N10muUN
9UAIYGcRCphOjWLIQpCHUth1FPZ8dCxLURNMEcBRtyThum3ICvU4MOgulx4boJaB
/213RnML9csGmifqiPav7QvFUcbeR1/tqrMnXCikmFEZO93kQwlpKtORdd7zbj5q
LHGaEAd2bCmbbBe48+bdnb2IhtVLE+9UJ3nmKBMSciHJbwwl6A+IHlOzGBhcOYn2
l9ZyodSKabQf3JqrCsfHmnKjzT8UcUiJQnyoDgW0/w==
-----END CERTIFICATE-----
subject=/C=US/postalCode=80309/ST=CO/L=Boulder/street=455 UCB/O=University of
issuer=/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO Hi
---

```
No client certificate CA names sent
---
SSL handshake has read 4756 bytes and written 363 bytes
---
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1
    Cipher    : DHE-RSA-AES256-SHA
    Session-ID: A25EE7C3A1A9DC258AA3B5C8555B13540C431C7C9392948F1B16523FCB38F
    Session-ID-ctx:
    Master-Key: 5C80ED1FCDCBB7457F539097AA0C5386C525D2872F98A5363D867AA54A6B4
    Key-Arg   : None
    Start Time: 1413171636
    Timeout   : 300 (sec)
    Verify return code: 0 (ok)
---
250 STARTTLS
EHLO test
250-smtp.colorado.edu
250-8BITMIME
250-SIZE 83886080
250-AUTH PLAIN LOGIN
250 AUTH=PLAIN LOGIN
AUTH LOGIN
334 VXNlcm5hbWU6
dmljbzQyOTk=
334 UGFzc3dvcmQ6
<Ive ommited my password here>
235 #2.0.0 OK Authenticated
MAIL FROM:<vince.coghlan@colorado.edu>
250 sender <vince.coghlan@colorado.edu> ok
RCPT TO:<vincecoghlan@gmail.com>
```

```
250 ok
DATA
354 Go ahead
SUBJECT: oh hai

wakawaka!
.
250 OK
QUIT
221 closing connection

$
```

Sending an email to a friend would require a simple change of the RCPT TO line, so I wont add that here (its all the same).

3: Suppose a webpage consists of five objects: base HTML file (Ob), another HTML object (Oa), and three jpeg objects (O1, O2 and O3). Draw a diagram to show message exchanges between a client and the server, when the client downloads this webpage, when (a) non-persistent HTTP is used; (b) a persistent HTTP with pipelining is used.

(a) This means that 5 different TCP conncections will occur. This makes more sense to explain then to draw out. The client initiates a TCP connection, sends an HTTP request, the server retrieves the requested object and sends a response to the client, the server then closes the connection. This is then repeated for each file. First the base file, then the object file, then whatever order the jpegs are loaded in.

(b) the client will send all requests and then the server will send back the data in the order it was asked for, all over the same TCP connection.

4: Do a literature survey to find out what is a whois database. Use various whois databases on the Internet to obtain the names of two DNS servers. Indicate which whois databases you used.

First, using who.is, we can look at google.com to find the nameserver they use. Apparently it is ns1.google.com. Using whois.net we can look at colorado.edu to find that the DNS they use is boulder.colorado.edu.

5: Visit `http://www.iana.org` and answer the following questions

(a) What are the well-known port numbers for network news transfer protocol (NNTP), NETBIOS session service, and ISO-IP?
The official TCP port for NNTP is 119, although 433 should be used if seperate servers for transmitting and reading are required, this is from `http://tools.ietf.org/html/rfc3977`. The port for NETBIOS session service is defined in `http://tools.ietf.org/html/rfc1002` as 139. The port for ISO-IP is 147 according to `http://tools.ietf.org/html/rfc1340`.

(b) What are the requests processed as a part of "Root Management" of IANA?
They are various root levels of domains. These can be seen at `http://www.iana.org/domains/root/db`. for instance, if i wanted to make a website called awesome.vince i could apply to get .vince as a root level domain.

6: Visit `http://www.root-servers.org`. Look at the monthly graph (2-hour average) of IPv4 bits/s and IPv6 bits/s in the root server managed by U.S. Army Research Laboratory.

(a) When did the maximum and minimum, incoming and outgoing data rate occured?
The maximum incoming and outgoing data rate was 91.5 kp/s and occured September 28, 2014. The minimum is hard to tell from the graph (im using the graph at `http://h.root-servers.org/128.63.2.53_3.html`), but it seems to have occured the night of September 21st.

(b) Approximately what is the difference between IPv4 data rate and IPv6 data rate?
For TCP we can know this data precisely, it is 51.131 kB/s. For UDP it is 1253.9 kB/s. This data was found at `http://h.root-servers.org/hlb1_v6_bps.html` and `http://h.root-servers.org/hlb1_v4_bps.html`

7: Do a literature survey of key escrow, mandatory key disclosure law and mandatory decryption law. Define them briefly and provide your views (about half page) about them.
Key escrow is an agreement for some organization to have access, under specific circumstances, to keys that another party may hold. For example, a company can hold keys on thier emplyees, and if one suddenly becomes under investigation, they may legally be able to use that key to examine encrypted messages that person may have sent. Mandatory key disclosure law and decryption laws force a person or organization, much like a sepina, to hand over their keys or data to a court or third party. Now for my opinion. All of these laws,

besides being unconstitutional and immoral, are completely and utterly inneffective. There is no way that you will not be able to transmit data that you want hidden, and destroying keys is fairly straightforward. Say I want to send an encrypted email once to someone, the process of creating a new PGP key takes minutes and can be simply destroyed after the data has been transfered. Forcing people to give up keys to data is a desperate attempt by prosecuters to pretend that they have any power in the matter of information. This is not the 1950's anymore. All of these laws were made by out-of-touch, old, white, male and shortsighted polititians who think the internet is a series of tubes and think that kids should stop skateboarding near thier porch. On top of all this, the illusion that the government doesnt already have a hold of your data is laughable. If they truely needed to know what you were doing (trust me, they dont care about you) then they could simply check one of thier massive data centers to find the specific key they needed. This is assuming they dont already have a backdoor in RSA, TLS, SSL, or any number of 0-days they have on linux, windows, and mac. The moral of the story is dont assume your data is safe unless you generated the keys yourself. Even then, you probably are not safe then. Just dont do anything legally questionable unless you know you wont be caught. Better yet, dont go near a computer.

8: Exercise 14 (Page 692) 5th Edition
My browser trusts the authorities that are in my mac keychain, which are all the authorities that apple installs by default. I trust these since if apple was scamming everyone they would lose a ton of money. if I disable trust, then chrome constantly asks me if I want to trust a certain website's authority.

9: Suppose a firewall is configured to allow outbound TCP connections but inbound TCP connections only to specified ports. What problem does this cause in using ftp to download a file from an outside server? How can you fix this problem?
An FTP server will sometimes connect back on a different port in order to send the file. This means that it will get blocked when trying to initiate a new TCP connection back on a different port. In order to fix this, you can either open that port, or forward all packets from that port, to a different one.

10: How is a digital signature different from user authentication? Explain with an example.
A digital signiture is the process of encrypting hashed data with your private key in a scheme where it can only be decrypted with that users public key, so as long as you trust his/her public key as being his/hers, than you can verify that it was his/her data. This is the theory, in practice the data is not encrypted, but just a hash of the data, and then that is attached with the original encrypted data. This way a recipient simply has to hash the data, and

decrypt the signature, if they match, then the signature is valid. User authentication is a completely different and mostly unrelated topic. This usually means prompting a user for thier identity and a passphrase, the passphrase is then hashed and checked agains a database to see if the hash matches what is on file. This can be done in many other ways besides this. Example: User A decides he want to log into a remote system, the remote system only allows users to log in if they provide the correct password, and are verified as being who they say they are. User A would send his username and password, encrypting the hash of these things with his private key. The remote server would then decrypt his/her hash using User A's public key. If there was a match, the server would then hash the password data with their own hashing function then match it against a list they have, thus completing user authentication.