CS 6823 Final Exam
December 2018
David Ho Dh2487

1a. [8 pts] Suppose a parent just purchased Circle with Disney and successfully connected it to their home Wi-Fi network. What will the device need to do once on the network to start performing it's functions.

The Circle with Disney is essentially acting as a proxy and firewall where all data must go through it in order to record data as well as filter / block some functions. As a result, all traffic must be rerouted through Circle. In order to do this, it could basically do a MITM attack where it tells the computers on the network that it is the router, and then all data going through the router would go through the Circle. With all the data, it can perform the functions of blocking websites as well as recording histories and time spent on websites.

1b. [4 pts] If a user is visiting a website via HTTPS (encrypted), would it be possible for the device to block that website?

Yes, even if the website is being visited via HTTPS, the website can be prevented even before the encryption begins. Once the destination of the SYN is shown to be a prohibited destination, the website can be blocked. This is obviously true as some countries can block Facebook or social medias with HTTPS.

1c. [4 pts] How would the device enforce a different BedTime for different devices, say, 7pm for a child and 9pm for an adult?

The Circle with Disney can have a time server allowing the device to know the time. For each packet being received, it can reference the source MAC address with the "BedTime" held in a table. If the time sent is after the BedTime, the packet can be dropped or rejected. So a child's computer will stop having its packets and data let through the device at a certain time, while the adult's computer will have a different time.

1d. [4 pts] Describe in detail a way for a technically savvy user to bypass the website blocking

The website blocking can be done through a shell account. Let's say engineering.nyu provides a shell account, the user can access engineering.nyu as it is an allowed website. From this website and the shell account, you can bypass the block and access any website. The way to counter this is to make it really slow so it's not worth bypassing the block as the website will take forever to load.

2 Perform Diffie-Hellman shared key generation with g=6, n=13, Alice selects a=4 as her secret, Bob selects b=6 as his secret.
2a. [2 pts] calculate Alice's public key A

$A = g^a \bmod n$
$A = 6^4 \bmod 13$
$6 \bmod 13 = 6$
$6^2 \bmod 13 = 6 * 6 \bmod 13 = 36 \bmod 13 = 10$
$6^4 \bmod 13 = 10 * 10 \bmod 13 = 100 \bmod 13 = 9$
<u>A = 9</u>

2b. [3 pts] calculate Bob's public key B

$B = g^b \bmod n$

$B = 6^6 \bmod 13$

$6^6 \bmod 13 = (6^4 \bmod 13) * (6^2 \bmod 13) \bmod 13 = 9 * 10 \bmod 13 = 90 \bmod 13 = 12$

$\underline{B = 12}$

2c. [3 pts] calculate Alice's shared key K

$K = B^a \bmod n$

$K = 12^4 \bmod 13$

$12 \bmod 13 = 12$

$12^2 \bmod 13 = 12 * 12 \bmod 13 = 1$

$12^4 \bmod 13 =1 * 1 \bmod 13 = 1$

$\underline{K = 1}$

2d. [2 pts] calculate Bob's shared key K

$K = A^b \bmod n$

$K = 9^6 \bmod 13$

$9 \bmod 13 = 9$

$9^2 \bmod 13 = 9 * 9 \bmod 13 = 3$

$9^4 \bmod 13 = 3 * 3 \bmod 13 = 9$

$9^6 \bmod 13 = 9 * 3 \bmod 13 = 1$

$\underline{K = 1}$

2e. [2 pts] If Trudy was watching the exchange between Alice and Bob, what would Trudy see?

If Trudy were watching the exchanges, Trudy would be able to see A,g,n, and B. However, even with this information, Trudy cannot determine the key K because Trudy does not know a and b, Alice and Bob's secret Key.

3a. [4 pts] All SHA1 are changed to SHA256 (Line 4, 9, and 10)

Yes, SHA1 is deprecated and can be broken. Changing SHA1 to SHA256 will increase security to the protocol as the challenge hash will be harder to crack.

3b. [4 pts] Line 8 changed to: MD4(MD4(MD4(UserPassword))) = NTHashHash

Yes, adding another layer of MD4 will increase security. This way, if being brute forced, the attacker will have to apply MD4 again, making the process longer.

3c. [4 pts] Line 6 changed to: ChallengeResponse = DESChallengeHash[00:07](NTHash)

No, this will simplify the Challenge Response as the not all bits will be incorporated in the Challenge Response. Although this gets rid of the hanging bit, the overall effect is a weaker security.

4a. [8 pts] Suppose Trudy wants to authenticate to the same AP. The AP sends the nonce 01011100 with ICV 1001. What are the four SimpleWEP fields (after encryption) that Trudy will send to the AP to be authenticated? For full credit, must show all steps and also explain the answer in detail.

(I know this was one of the problems on the practice test)

First, we know that the KeyID rotates every 24 hours, so as long as Trudy sends this message before the KeyID rotates, the same KeyID can be used.
KeyID: 01
Same IV: 001011

We know that the initial message and key XOR with once gives us the cipher message. Due to discrete math properties, we also know that the Once XOR Cipher message gives us the Message with key. Once we have to original message and key, we can re-encrypt it using the new once to determine the new cipher message.

0010 0100 (Original Nonce)
1001 1001 (Cipher Message)
=
1010 1101 (using message)
0101 1100 (New Once)
=
1111 0001 Cipher Message

So the four SimpleWEP fields are:
001011 01 11110001 1000

4b. [5 pts] Suppose Trudy is a MITM between Alice and the AP. Trudy intercepts Alice's encrypted payload: 011000 01 01000110 0101. Trudy wants to flip the 7th bit of the message (01000110 -> 01000100). Explain how Trudy needs to modify the payload to ensure that the plaintext passes the ICV check.

We are told that the ICV is an XOR of the first four bits of the message with the last four bits. Therefore, if we want to flip the 7th bit of the message, in order to pass the ICV check, we will need to flip the 3rd bit of the ICV.

4c. [3 pts] Suppose Trudy is at a coffee shop and wants perform a DOS attack to ensure no one can get a reliable connection to the Internet. Explain how she can achieve that using only the 802.11 protocol.

Trudy, if she just wanted to DOS everything, she could perform a "Fork in the Microwave" attack where it would disrupt all wireless packets. Trudy can see the mac addresses of each person on the network still and can attack each one individually if needed.

5a. [6 pts] Suppose the server selected the ciphersuite SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA. Explain which steps of the diagram keys

are sent over. Be sure to specify which step sends what keys. (e.g., step 1 & 2: no keys are sent.)

Step 1: No keys are sent
Step 2: No keys are sent
Step 3: Certificate is sent over to be verified
Step 4: n,g,A signed with RSA since it's DHE
Step 5: No keys are sent
Step 6: B signed with RSA
Step 7: Nothing Sent (Change Cipher Spec)
Step 8: Encrypted Hash of Previous Messages(1-6); 3DES_EDE_CBC and SHA1 for encryption
Step 9: Nothing Sent (Change Cipher Spec)
Step 10: Encrypted Hash of Previous Messages(1-6, 8); 3DES_EDE_CBC and SHA1 for encryption

5b. [2 pts] Does this ciphersuite have Perfect Forward Secrecy? How do you know?

Yes, this ciphersuite has Perfect Forward Secrecy. We know because the key exchange being used is Diffie-Hellman Ephemeral. The ephemeral guarantees PFS.

5c. [4 pts] What are all the reasons that this ciphersuite should not be used anymore?

This ciphersuite should not be used for more than one reason. Firstly, 3DES is deprecated and should not be used. Furthermore, SHA-1 is also deprecated and should not be used.

6a. [8 pts] Both the Guest and the Employee network has port 80 and 443 access to the Internet via the Web Proxy only.

Both (Setting default rules to drop)

```
iptables –P INPUT DROP
iptables –P OUTPUT DROP
iptables –P FORWARD DROP
```

Firewall A

```
iptables –A FORWARD  -p tcp --dport 80 -d 10.10.111.3 -j ACCEPT -m conntrack --ctstate NEW,ESTABLISHED,RELATED

iptables –A FORWARD  -p tcp --dport 443 -d 10.10.111.3 -j ACCEPT -m conntrack --ctstate NEW,ESTABLISHED,RELATED

iptables –A FORWARD  -p tcp --sport 80 -s 10.10.111.3 -j ACCEPT -m conntrack --ctstate ESTABLISHED,RELATED

iptables –A FORWARD  -p tcp --sport 443 -s 10.10.111.3 -j ACCEPT -m conntrack --ctstate ESTABLISHED,RELATED
```

Firewall B

```
iptables –A FORWARD  -i eth0 -o eth1-p tcp --dport 80 -s 10.10.111.3 -j ACCEPT -m conntrack --ctstate NEW,ESTABLISHED,RELATED

iptables –A FORWARD  -i eth0 -o eth1-p tcp --dport 443 -s 10.10.111.3 -j ACCEPT -m conntrack --ctstate NEW,ESTABLISHED,RELATED

iptables –A FORWARD  -o eth0 -i eth1-p tcp --sport 80 -d 10.10.111.3 -j ACCEPT -m conntrack --ctstate ESTABLISHED,RELATED

iptables –A FORWARD  -o eth0 -i eth1-p tcp --sport 443 -d 10.10.111.3 -j ACCEPT -m conntrack --ctstate ESTABLISHED,RELATED
```

6b. [4 pts] All hosts in the Guest and Employee Network are required to use the Primary DNS Server. Write the rules so all the hosts can perform a DNS lookup on fakebook.com.

Firewall A

```
iptables –A FORWARD  -s 10.20.111.0/24 -d 4.4.4.4 -j ACCEPT -m conntrack --ctstate NEW,ESTABLISHED,RELATED

iptables –A FORWARD  -d 10.20.111.0/24 -s 4.4.4.4 -j ACCEPT -m conntrack --ctstate ESTABLISHED,RELATED
```

Firewall B

```
iptables –A FORWARD  -s 10.20.111.0/24 -d 4.4.4.4 -j ACCEPT -m conntrack --ctstate NEW,ESTABLISHED,RELATED

iptables –A FORWARD  -d 10.20.111.0/24 -s 4.4.4.4 -j ACCEPT -m conntrack --ctstate ESTABLISHED,RELATED

iptables –A FORWARD  -s 10.10.111.0/24 -d 4.4.4.4 -j ACCEPT -m conntrack --ctstate NEW,ESTABLISHED,RELATED

iptables –A FORWARD  -d 10.10.111.0/24 -s 4.4.4.4 -j ACCEPT -m conntrack --ctstate ESTABLISHED,RELATED
```

6c. [6 pts] All hosts in the Guest and Employee Network, including the two Firewalls, must send event logs (TCP 5985) to the SIEM.

Firewall A

```
iptables –A OUTPUT  -p tcp --dport 5985 -d 10.10.111.4 -j ACCEPT -m conntrack --ctstate NEW,ESTABLISHED,RELATED
iptables –A INPUT  -p tcp --sport 5985 -s 10.10.111.4 -j ACCEPT -m conntrack --ctstate ESTABLISHED,RELATED
```

```
iptables –A FORWARD  -p tcp --dport 5985 -d 10.10.111.4 -j ACCEPT -m conntrack --ctstate NEW,ESTABLISHED,RELATED
```

```
iptables –A FORWARD  -p tcp --sport 5985 -s 10.10.111.4 -j ACCEPT -m conntrack --ctstate ESTABLISHED,RELATED
```

Firewall B

```
iptables –A OUTPUT  -p tcp --dport 5985 -d 10.10.111.4 -j ACCEPT -m conntrack --ctstate NEW,ESTABLISHED,RELATED
```

```
iptables –A INPUT  -p tcp --sport 5985 -s 10.10.111.4 -j ACCEPT -m conntrack --ctstate ESTABLISHED,RELATED
```

6d. [4 pts] The Fakebook server may connect to the Database server on TCP port 1433.

Firewall A

Nothing

Firewall B

```
iptables –A FORWARD  -i eth1 -o eth0 -p tcp --sport 1433 -s 5.1.2.3 -d 10.10.111.2 -j ACCEPT -m conntrack --ctstate NEW,ESTABLISHED,RELATED
```

```
iptables –A FORWARD  -o eth1 -i eth0 -p tcp --dport 1433 -d 5.1.2.3 -s 10.10.111.2 -j ACCEPT -m conntrack --ctstate ESTABLISHED,RELATED
```

7a. The ChangeCipherSpec message is encrypted.

False

Nothing is even sent over?

7b. The TLS Finished message is encrypted.

True

First encrypted message and the hash of previous messages

7c. TLS uses Encrypt then HMAC. (Encrypt the message first, then append the HMAC of the ciphertext.)

False

Append HMAC then Encrypt

7d. Compression should not be used anymore due to major vulnerabilities.

True

No one uses compression really for this reason

7e. A website can only be issued one TLS certificate at a time.
False
Can be issued multiple

7f. In the TLS Abbreviated Handshake, the certificate is not sent over.
True
2,9,10 is sent over.