

Timothee Guerin
260447866

Question 1

All the code is in cryptography.java

1. Transpose

First insert the messages in the grid(, to separate messages)

```
b o b
t h i s
  i s
m a r y
, d o w
n l o a
d d a
t a f
i l e
n o w
```

Then transpose

```
-----
b t m , n d t i n
o h i a d l a l o
b i s r o o d e w
  s y w a a f
-----
```

Finally shift

```
-----
f w n , q f u m q
q i m d f m d n p
f l u s s r f i z
  t b y b e i
```

The message encrypted is "fw n,qfumqqimdfm dnpflussrf iz t bybei"

The decrypt the message we first need to insert the letter back into a a grid shift back with the same 4-key block and transpose then concatenate the rows and split with the , to separate all the messages

2. Hash

The hash with method 1 is: 1.0590456726379646E73

The hash with method 2 is: 6.262211084873715E134

3. Private Public key

The formula for private public key with u=50 is:

$$C = w * l \text{ mod } 50$$

$$D = w^{(-1)} * C \text{ mod } 50$$

with:

- C: encrypted letter
- D: Plain letter
- w: encrypting key(public)
- $w^{(-1)}$: Decrypting key(private)

Timothee Guerin

260447866

and such that

$\gcd(50, w) = 1$ and $w \cdot w^{-1} \bmod(50) = 1$

To encrypt each letter we first have to find w and w^{-1} such that the conditions hold.

We can choose $w=9$ and $w^{-1}=39$

$\gcd(50, 9) = 1$ & $9 \cdot 39 = 351 = 1 \bmod 50$

To encrypt our message we have to assign a number to each letter of the alphabet.

We take: $a=0$, $b=1$ and so on until $z=25$

We have to encrypt the following message: "Bob this is Mary", "Download data file now".

Using the algorithm we get [9, 26, 9, -1, 21, 13, 22, 12, -1, 22, 12, -1, 8, 0, 3, 16, null, 27, 26, 48, 17, 49, 26, 0, 27, -1, 27, 0, 21, 0, -1, 45, 22, 49, 36, -1, 17, 26, 48]

Calling the decrypt algorithm return the the initial messages.

Question 2

The website is at <http://linux.cs.mcgill.ca/~tgueri/comp307>

The question2.zip contains the code for the website

Question 3

Types of packets

- Application Data
- Router solicitation
- Neighbour solicitation
- Multicast listener report
- Standard query response
- Get http url
- DHCP request
- TCP segment of a reassemble PDU
- Client hello
- TCP window update

Protocols

- TCP IP
- ICMP
- UDP

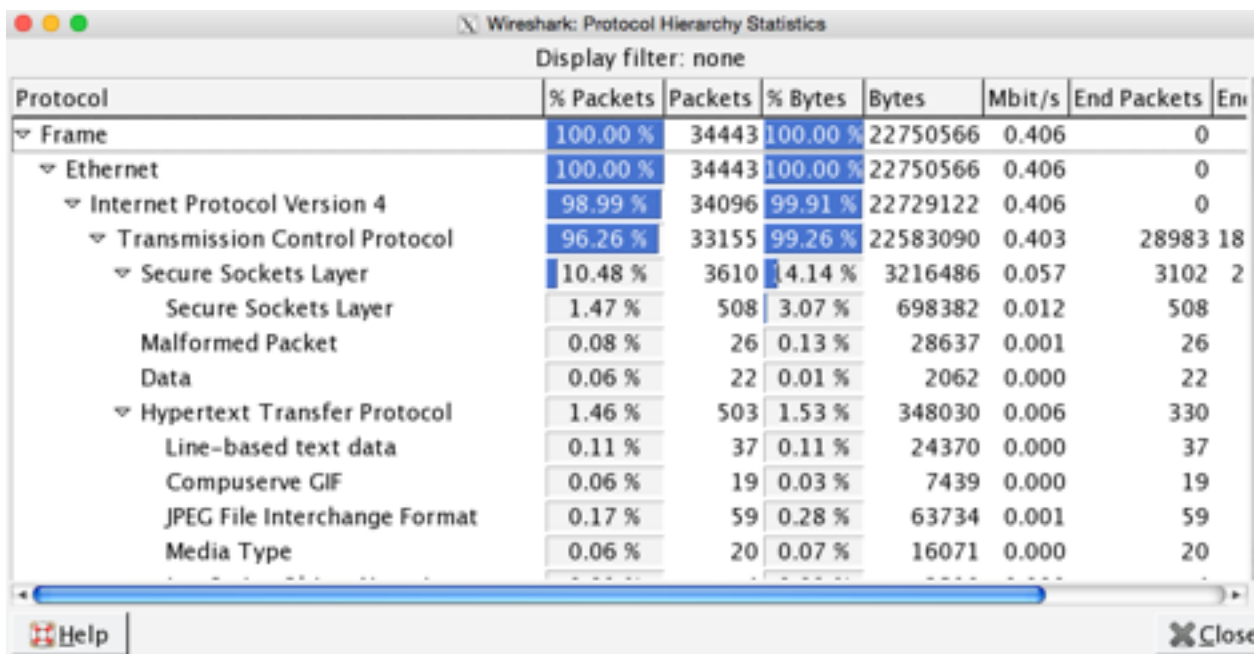
Percentages:

- Bad TCP: $\text{tcp.analysis.flags} \&\& \text{!tcp.analysis.window_update}$ - 19% **Unreadable**
- UDP: udp - 2,8% **Partially readable**
- HTTP State Change: $\text{hsrp.state} \neq 8 \&\& \text{hsrp.state} \neq 16$ - 0%
- Spanning Tree Topology: $\text{stp.type} == 0x80$ - 0%
- OSPF State Change: $\text{stp.type} == 0x80$ - 0%

Timothee Guerin
260447866

- **ICMP Errors:** icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2 || icmpv6.type eq 3 || icmpv6.type eq 4 - 0% (only 2) **Unreadable**
- **ARP:** arp - 0.7% **Unreadable**
- **ICMP:** icmp || icmpv6 - 0.3 **Unreadable**
- **TCP RST:** tcp.flags.reset eq 1 - 1.3 **Unreadable**
- **SCTP ABORT:** sctp.chunk_type eq ABORT - 0%
- **TTL low or unexpected:** (! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp || carp)) - 0%
- **Checksum error:** eth.fcs_bad==1 || ip.checksum_bad==1 || tcp.checksum_bad==1 || udp.checksum_bad==1 || sctp.checksum_bad==1 || mstp.checksum_bad==1 || cdp.checksum_bad==1 || edp.checksum_bad==1 || wlan.fcs_bad==1 - 0%
- **SMB:** smb || nbss || nbns || nbpx || ipxsap || netbios - 0%
- **HTTP:** http || tcp.port == 80 || http2 - 36.9% **Partially Unreadable**
- **IPX:** ipx || spx - 0%
- **DCERPC:** dcerpc - 0%
- **Routing:** hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp - 0%
- **TCP SYN/FIN:** tcp.flags & 0x02 || tcp.flags.fin == 1 - 5.3% **Unreadable**
- **TCP:** tcp - 96.3 **Unreadable**

Protocol hierarchy



Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes
Frame	100.00 %	34443	100.00 %	22750566	0.406	0	
Ethernet	100.00 %	34443	100.00 %	22750566	0.406	0	
Internet Protocol Version 4	98.99 %	34096	99.91 %	22729122	0.406	0	
Transmission Control Protocol	96.26 %	33155	99.26 %	22583090	0.403	28983	18
Secure Sockets Layer	10.48 %	3610	4.14 %	3216486	0.057	3102	2
Secure Sockets Layer	1.47 %	508	3.07 %	698382	0.012	508	
Malformed Packet	0.08 %	26	0.13 %	28637	0.001	26	
Data	0.06 %	22	0.01 %	2062	0.000	22	
Hypertext Transfer Protocol	1.46 %	503	1.53 %	348030	0.006	330	
Line-based text data	0.11 %	37	0.11 %	24370	0.000	37	
Compuserve GIF	0.06 %	19	0.03 %	7439	0.000	19	
JPEG File Interchange Format	0.17 %	59	0.28 %	63734	0.001	59	
Media Type	0.06 %	20	0.07 %	16071	0.000	20	

Help Close

3. Data types

Readable

No relevant data

Partially readable

Common properties: lots of url, lots of common source and destination address

Protocol concerned: DNS (Domain Name Server), some HTTP

Timothee Guerin
260447866

Some DHCP gives us information about people using their phone to access a browser. In most cases, the partially readable frames are using protocols from the application layer which means that security at this layer is probably weak as we can catch and analyze the information in those packets.

Unreadable

Common properties: most of them are TCP protocols.

We can notice that as almost everything is unreadable, security is stronger for the TCP protocols.

4. Source and address

It seems some source ip are having more or less frequent unreadable message. Similarly some destination always have unreadable data(e.g. 79.99.33.92). Which probably means that some user were visiting secure website(https) while other were visiting more regular website.

Question 4

1. Layers of network stack:

1. Physical
2. Data link
3. Network
4. Transport
5. Session
6. Presentation
7. Application
8. User
9. Management
10. Money

2. Details

1. Physical

Cables, room, doors / IEEE 802.3u (Fast Ethernet 10Mbit/s)

Physical connections are made between network nodes and/or infrastructure devices (hubs, switches, routers) by various type of copper or fiber cable.

2. Data link

Ethernet

The Ethernet divide a stream of data into shorter pieces called frames which contain the source and the destination addresses, as well as error-checking data so that data can be located and re-send.

3. Network

IP

Delivers packets from source host to destination host based on IP addresses which is located in the packet header. To do this, it defines packets structure to encapsulate the data to be

Timothee Guerin
260447866

delivered, as well as defines addressing methods that are used to label datagram with source and destination information.

4. Transport

TCP

Source PC creates a packet of data with the destination IP address. Set a timeout time and saves packet in OS space. It then transmits the packet to host device. The Hop-To-Hop protocol takes over and try to send packet to destination PC. If it succeeds then the saved packet is deleted. If there is an error or a timeout, it will resend the saved packet as well as increment a counter which counts the number of time it can resend the packet in case of multiple delivery failure. If it still fails, the packet is deleted and an error is returned.

5. Session

TLS/SSL

Initialized in session layer and works at the presentation layer.

Cryptographic protocols designed to provide communication security over the internet. Uses asymmetric cryptography to authenticate the one with whom we are communicating. It uses a shared key for that session.

6. Presentation

SSL

Encrypt or decrypt packets.

7. Application

HTTP

It is a structured text that uses hyperlinks between nodes containing text. HTTP works as a request-response protocol in the client server computing model. The client submits an HTTP request to the server and the server provides resources (HTML files etc). The server returns a response message to the client with requested content or completion status information depending on the request.

8. User

Behavior, Awareness & Education

Safe and responsible behaviour to make sure the user is not willingly disrupting the stack.

9. Management

Policies

This affects and determines all the other layers.

10. Money

Security budget

Determines how the security stack is elaborated.

3. Security

1. Physical

Wired network vs wireless.

Makes it easier to trace.

Can install camera to check who gets in the room etc.

Timothee Guerin

260447866

2. Data Link

Content address table

The table maps the switch's port to specific MAC addresses. It allows the switch to securely deliver packet to its intended physical address only which provides much greater security.

Address routing protocol

As we want to ensure reliable data communications, all switches in the network must maintain up-to-date tables for mapping IP to MAC addresses. If a client/switch is unsure of the mapping of a data packet it will send an Address Resolution Protocol message to the nearest switch asking for the MAC address mapped with a specific IP address. Then the table is updated to mirror the new mapping.

3. Network

IPsecurity: Suite of protocols for securing Internet Protocol communications by authenticating and encrypting each IP packet in a data stream.

4. Transport

Encryption: Prevent "attackers" to read packets.

Port Scan: Scan ports and if one open then the OS completes a three-way handshake and the port scanner immediately closes the connection to avoid denial-of-service attacks.

5. Session

Login key exchange

6. Presentation

Permissions: Different types of permissions for different type of users.

7. Application

SFTP: Uses SSH to transfer files. Encrypts both command and data. This prevents password and sensitive information from being openly transmitted over the network.

FTSP

Extension of FTP which allows clients to request that the FTP session be encrypted.

8. User

Discipline, training, fear and warnings

Makes sure the users know the security protocols and are able to report any issues. It also prevents (in most cases) users to disrupt the system.

9. Management

Training the management to understand and apply security protocols at all level of the stack.

10. Money

Security budget: Makes sure there is enough investment for security. Allows to implement more security protocols to the stack.

4. Use case

The main security concern for a online clothing store(or any kind of online store) is transaction as we want to avoid man-in-the-middle attack. We absolutely need to prevent packets going from the store to the bank for instance to be intercepted and have credit card number stolen etc... Henceforth, the following layers are the most important:

Transmission: Using encryption and eventually port scanner.

Session & Presentation: Using SSL for communication security.

Application: using SFTP to transfer file.

Timothee Guerin
260447866

As we are looking at the minimum security cost possible, this is the most adequate as trying to implement security for the other layers is expensive in terms of dollar, throughput of packets, and annoyance of human interaction. For the other layers, security is less of a concern. As this is an online store, it seems hard to believe that someone would attack the physical layer. Similarly for the data link layer as the most valuable data is usually easier to access in the above layers. Finally, as this is an online store, our last three layers namely, user, management and money are not really concerned though we need money anyway...