**Zoom, Webex Traffic Analysis**

**2017313135 소프트웨어학과 권동민**

**Q1. Uses WireShark to capture the live Zoom and Webex Traffic**

* Saved separated files(zoom.pcap, webex.pcap)

**Q2. What ports and protocols zoom traffic uses**

1. Three-hand-shaking

텍스트이(가) 표시된 사진

자동 생성된 설명

Port: TCP 443

2. When participants join the room

텍스트, 벽이(가) 표시된 사진

자동 생성된 설명

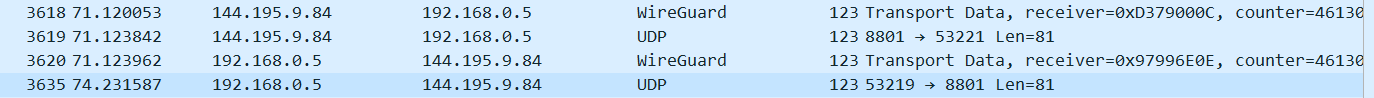
텍스트, 오렌지이(가) 표시된 사진

자동 생성된 설명

Port : UDP 3478

3. Send and receive data(video, audio)

* Send nothing(not video, audio)



* Send just audio

텍스트이(가) 표시된 사진

자동 생성된 설명

* Send audio and video

텍스트이(가) 표시된 사진

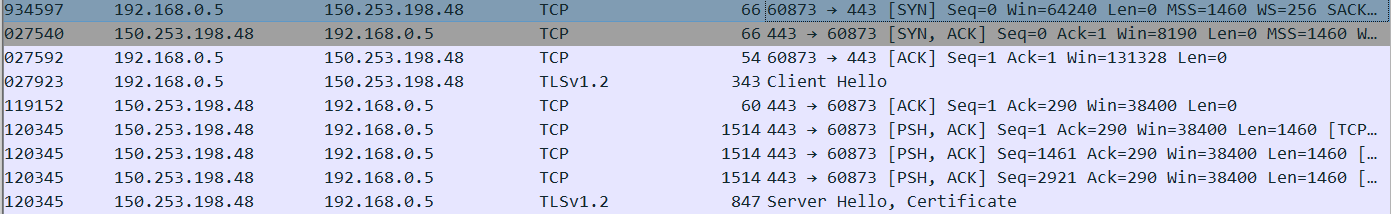
자동 생성된 설명

We can see that the length of data increases. (123 -> 300 -> 1100)

Port : UDP 8801, wireGuard

**Q3. What ports and protocols Webex traffic uses**

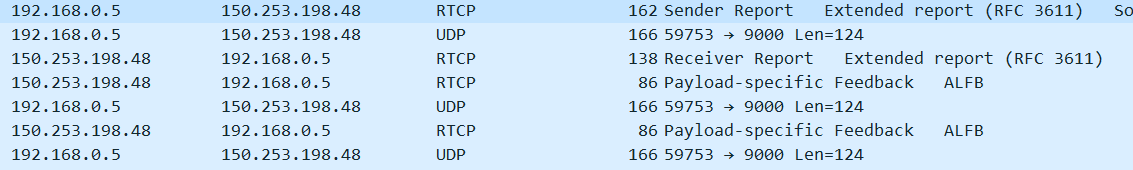
1. Three-hand-shaking



Port: TCP 443

2. Send and receive data(video, audio)

* Send nothing(not video, audio)



* Send just audio

테이블이(가) 표시된 사진

자동 생성된 설명

* Send audio and video

테이블이(가) 표시된 사진

자동 생성된 설명

Port : UDP 9000

**Q4. Sender’s and receiver’s information observed by traffic**

* Ip, port, protocol( zoom and webex is not p2p communication so the ip is server ip)
* Mac address
* Transmission time
* Data(voice and video information are transferred)

**Q5. Authentication process of Zoom and Webex**

* Zoom : Password Authentication.(if you don’t set the password, zoom makes password automatically.) And people can participate zoom meeting by clicking url link.
* Webex : webex uses e-mail id of users for authentication. People can also participate by room link.

**Q6. Key distribution protocol of Zoom and Webex**

Zoom and Webex both support E2EE(End to End Encryption). So all client has their own private Key and public key. And sender make random key to encrypt data, also encrypt the key by receiver’s public key.(uses public key encryption) Receiver finally encrypt the key and data to read. Zoom supports the E2EE in version 5.4.0 or higher.

Zoom:



Webex:



**Q7. Encryption method of Zoom and Webex**

Zoom : AES – 256 – GCM

텍스트이(가) 표시된 사진

자동 생성된 설명

In Zoom version 5.0, all client are using “AES-256-GCM” algorithm to encrypt data.

Webex : AES 128, AES 256, SHA 256, RSA

During data transfer between server and client, Webex uses https(ssl). Also, Webex uses AES, SHA, RSA to encrypt.