ENSC 427: Communication Networks
Spring 2023

Final Project Presentation
ANALYSIS OF CLOUD SECURITY USING TLS/HTTP/TCTP

www.sfu.ca/~alons/ProjectHomepage.html

WRITTEN BY GROUP 3

ALON SINGH	301381523	alons@sfu.ca
RIKU MAKITA	301381399	rmakita@sfu.ca

Roadmap

- Introduction
- Overview
- Simulation
- Results
- Future Direction

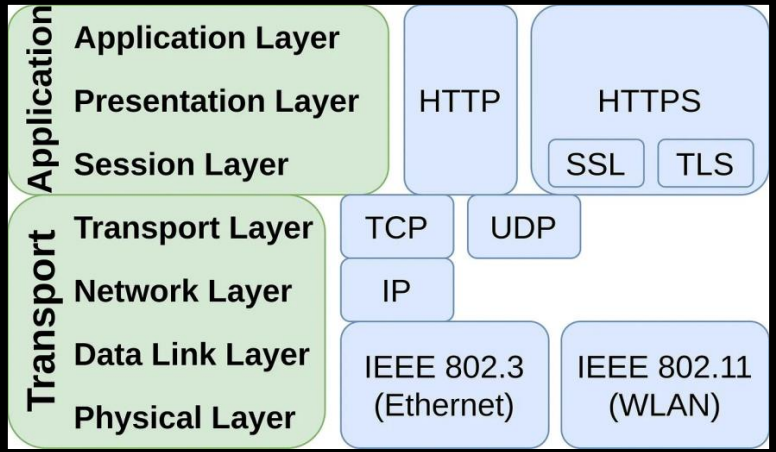
Introduction

- Cloud Security: A shared responsibility model
- Why is Cloud Security important?
- Industry Leaders:
  - Cloudflare
  - Crowdstrike
  - VMware
- Types:
  - Encryption
  - Identity Access Management
  - Firewall
  - Security monitoring

Overview

Encryption: Purposeful scrambling of data

- Encryption methods:
  - Secure Socket Layer (SSL)
    - Explicit connection
  - Transport Layer Security (TLS)
    - Implicit connection



[10] Thomas, M. (2021, January 17). HTTPS vs SSL vs TLS. Medium.

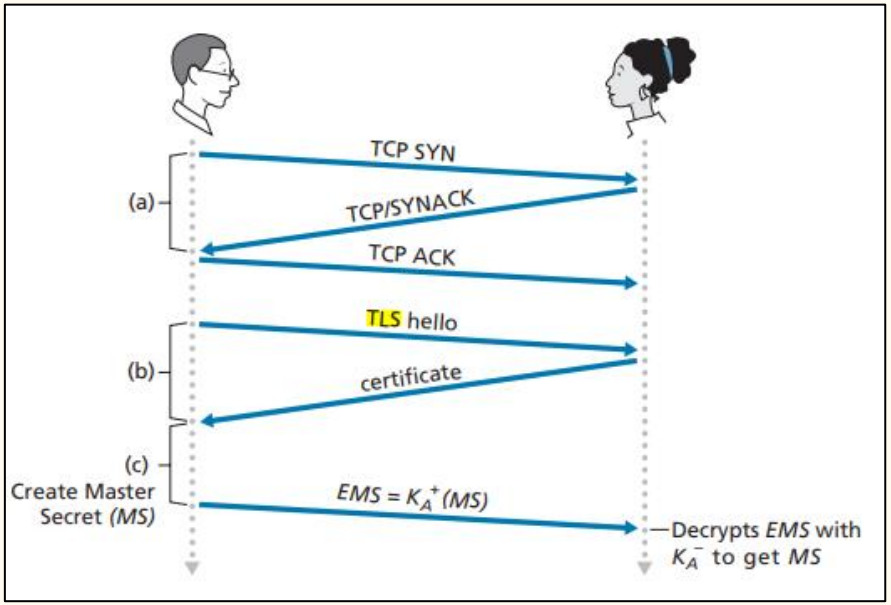
Transport Layer Security (TLS)

Advantages

- Encryption, authentication, integrity
- Improves security
- Instills trust
- Easily deployed

Drawbacks

- Dependence on intermediaries
- Legal obligations
- Can't be used with HTTP



[11] J. F. Kurose and K. W. Ross, Computer networking: A top-down approach.

The Experiment

Simulation - The Good

- Using the website “HTTP vs HTTPS” we can download 360 new non-cached through both HTTP and HTTPS.
- Combined with wireshark to capture the data packets, and the command below to retrieve them, we can compare the different protocols.
- PCAP files were saved from and graphed as well

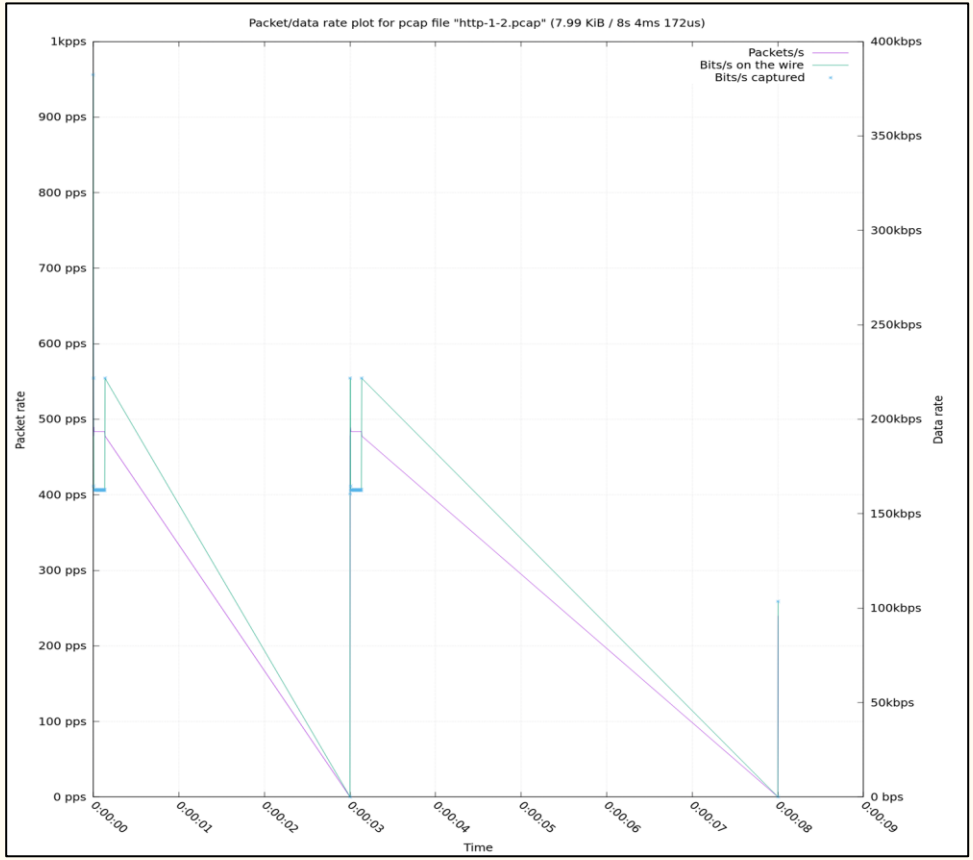
```
curl http://www.httpvshttps.com
```

➔ Command to retrieve data from the link.

```
<!--
    Created November 2014
    chris@anthum.com
    www.anthum.com
-->
<html>
<head>

    <script src="https://www.httpvshttps.com/check-server.js"></script>

    <script>
                function log(o) {if (console) console.log(o);}
                var proto = window.location.protocol;
                proto = proto.substring(0,proto.length-1);
                function setActiveMenu() {
                                if ('http' == proto) {

document.getElementById('menu-http').className += ' active';
                                } else if ('https' == proto) {

document.getElementById('menu-https').className += ' active';
                                }
                }
    </script>

    <script>
    …
```

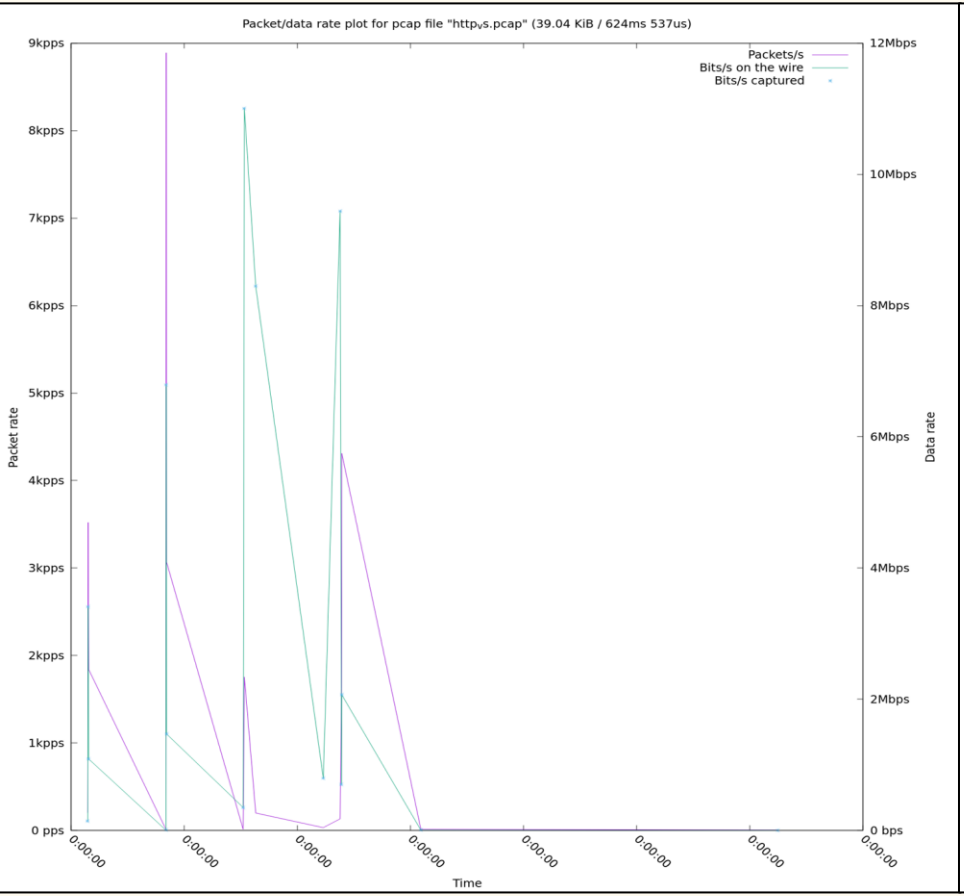
➔ Portion of output from the command.

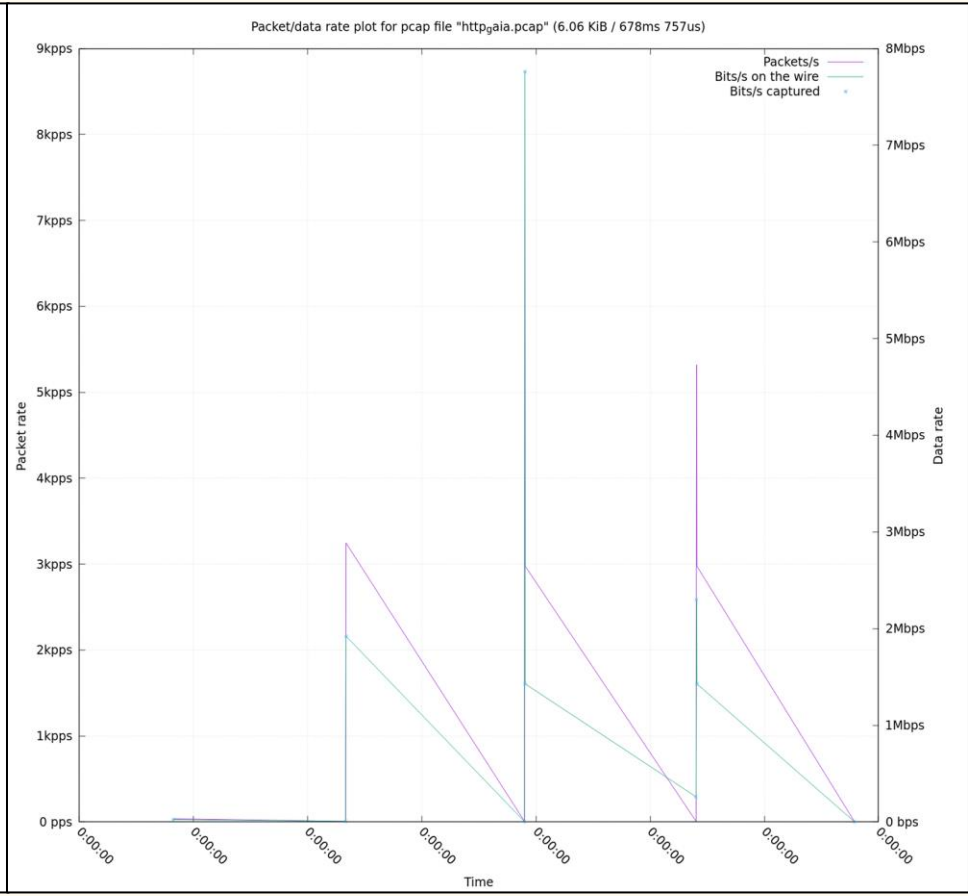
Simulation - The Bad



- Simulations in ns3 by default only use HTTP.
- There will not be a uniform way to compare these results to any TLS encrypted data.
- Encryption algorithms can be implemented in ns3, but do not interface well with a network simulation.

Simulation - The Results - HTTP

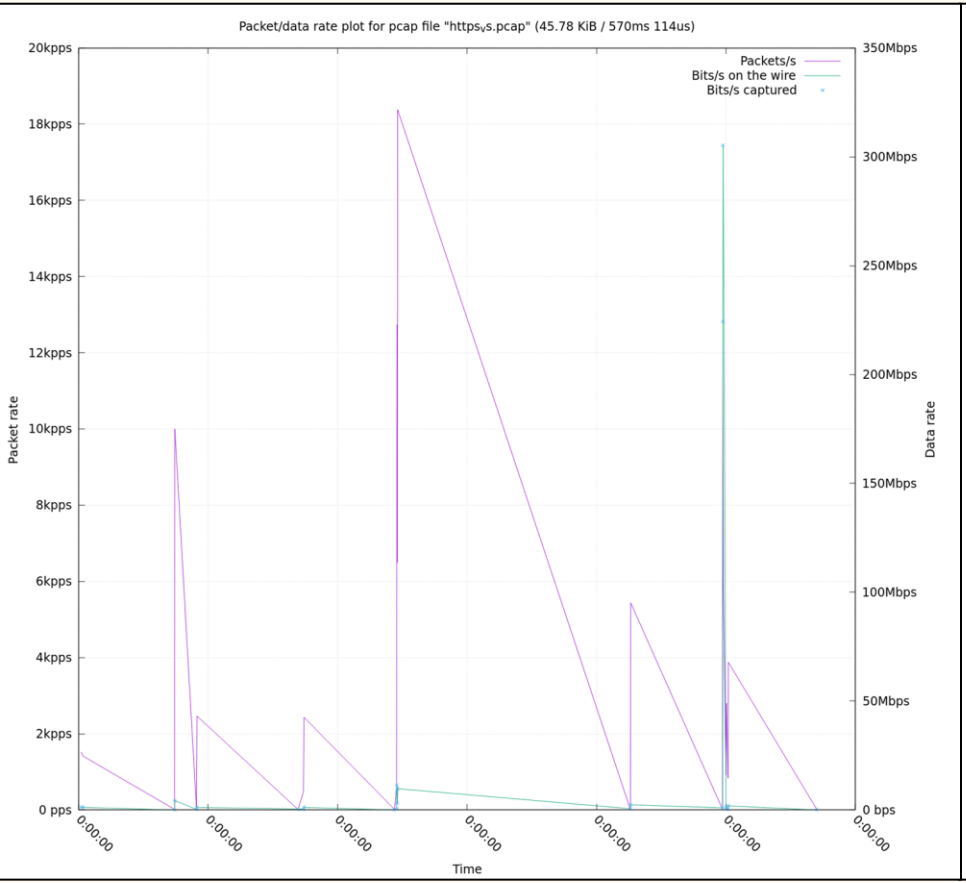


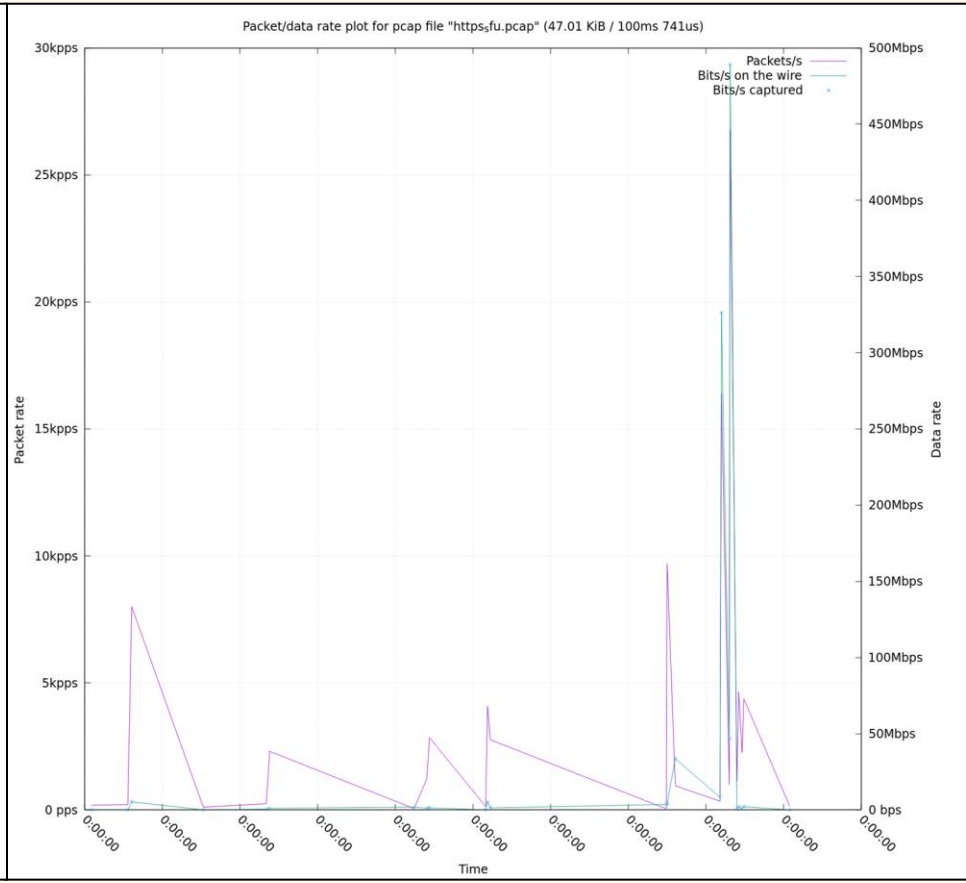


➔ http://www.httpvshttps.com

➔ http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html

Simulation - The Results - TLS

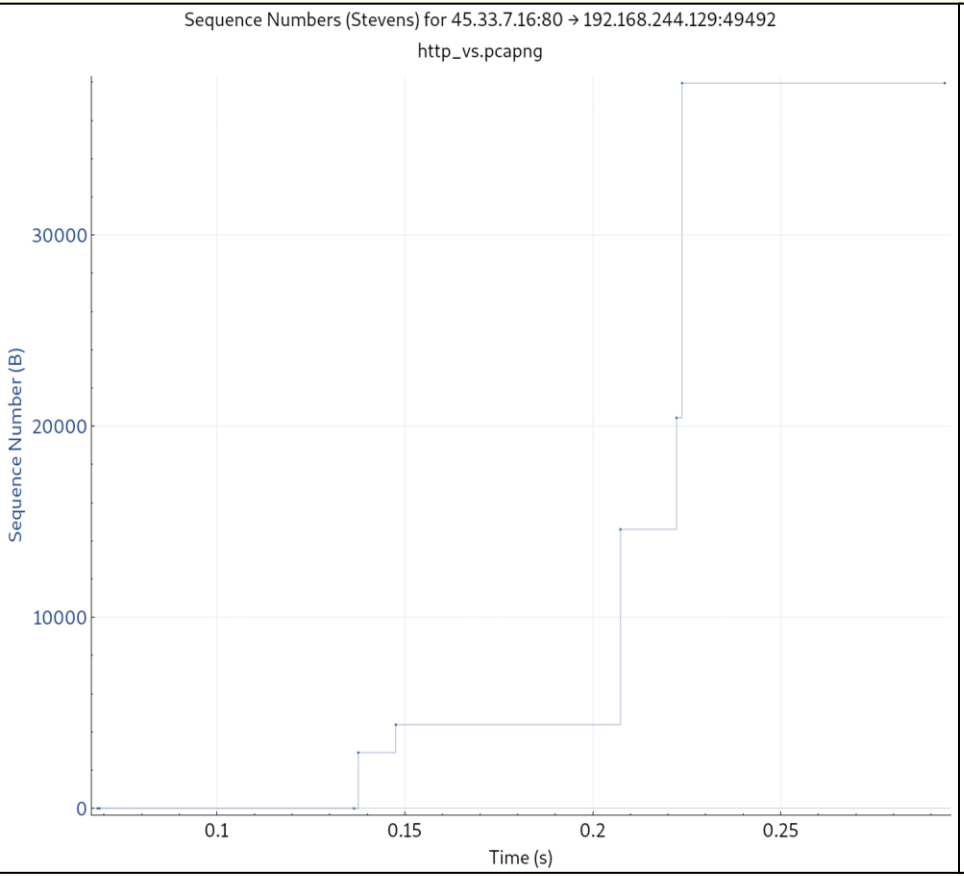


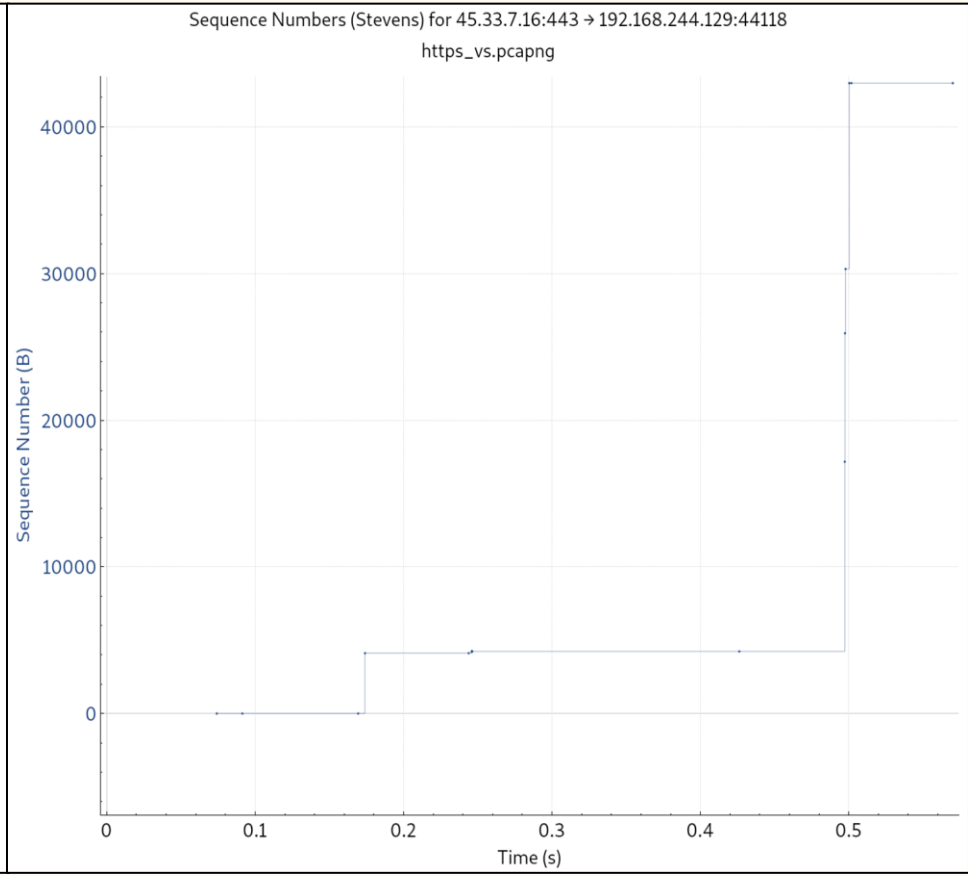


➔ https://www.httpvshttps.com

➔ https://www.sfu.ca

Simulation - The Results



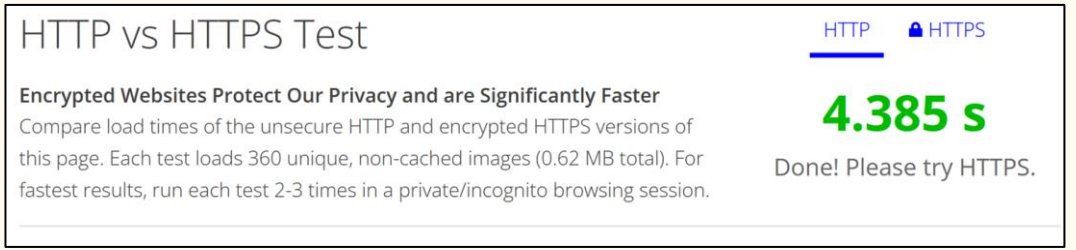


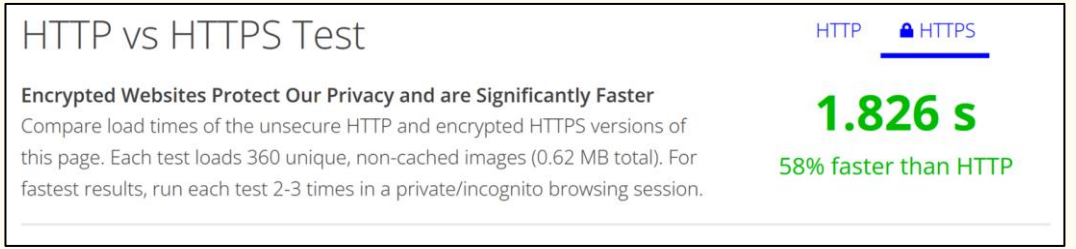
➔ http://www.httpvshttps.com

➔ https://www.httpvshttps.com

Discussion of Results

- HTTP is faster than the encryption method of HTTPS.
- However, TLS will protect the data you're sending and receiving.
- Additionally, the use of protocols such as SPDY and the development of HTTP/2 means most HTTPS websites can now mean perform faster than HTTP.

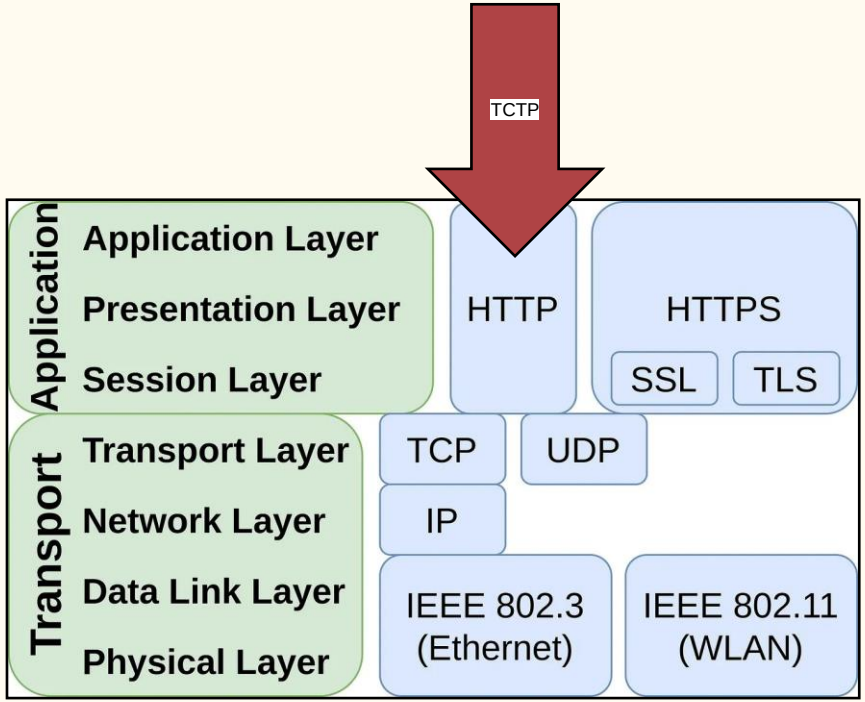




Future Works

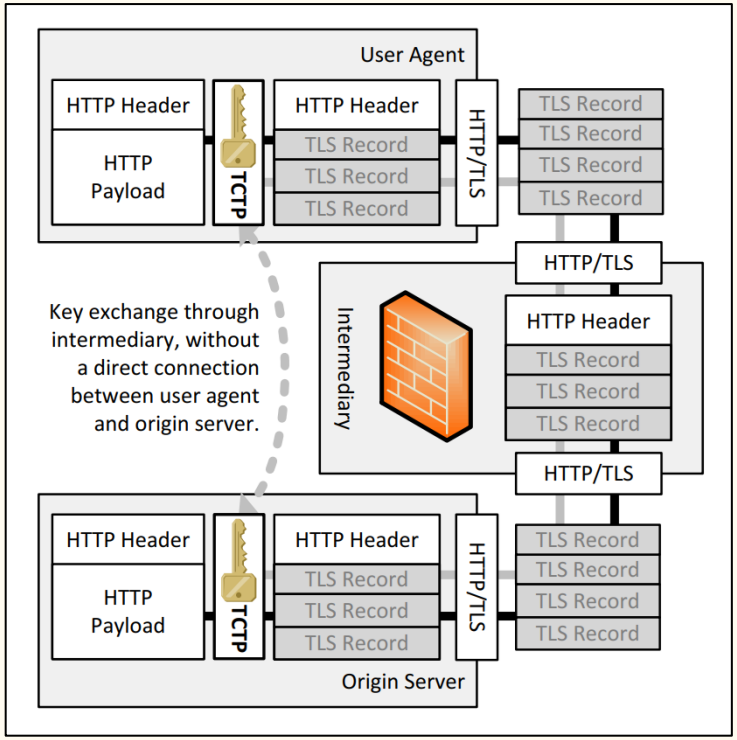
Trusted Cloud Transfer Protocol (TCTP)

- Entity-body encryption technique
  - Fully HTTP compliant
  - Authenticates HTTP using TLS at application layer
  - Wrap TLS handshake protocol into HTTP payload
    - Reduces intermediary data leak risk



[10] Thomas, M. (2021, January 17). HTTPS vs SSL vs TLS. Medium.

Trusted Cloud Transfer Protocol (TCTP)



[1] M. Slawik, "The Trusted Cloud Transfer Protocol,"

- Very similar to IPv4 using IPv6 as its payload to be compatible with both platforms.
- Using the TLS method of encryption, the HTTP data will be encoded and sent as a HTTPS datagram.
- At the application level, the datagram will be decoded back into its HTTP format.
- This method of TCTP will enable site to be cross-compatible on both platforms.

Thanks

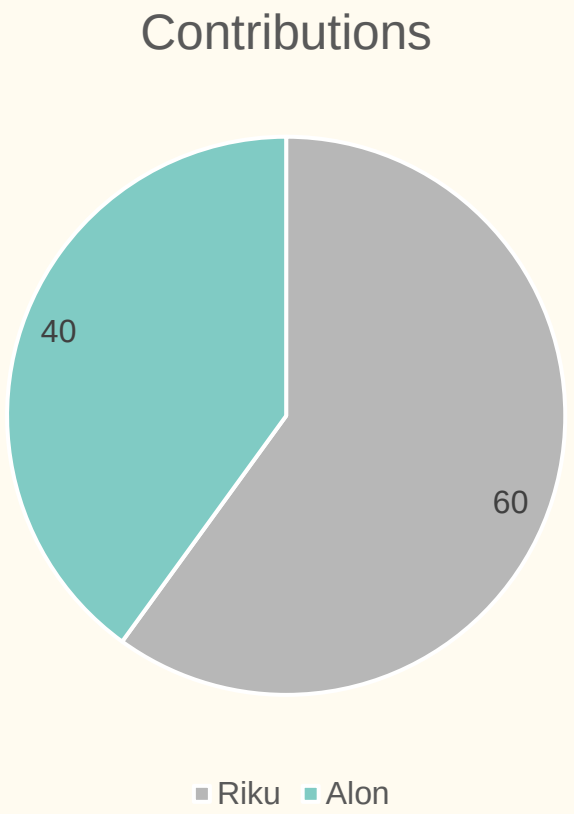
Work Split

Riku

- Idea formation
- Introduction
- Conclusion
- Results interpretation

Alon

- Literature review
- Simulation design



References

[1] M. Slawik, "The Trusted Cloud Transfer Protocol," 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, Bristol, UK, 2013, pp. 203-208, doi: 10.1109/CloudCom.2013.126. [Accessed: 26-Feb-2023]

[2] S. Müller, D. Bermbach, S. Tai and F. Pallas, "Benchmarking the Performance Impact of Transport Layer Security in Cloud Database Systems," 2014 IEEE International Conference on Cloud Engineering, Boston, MA, USA, 2014, pp. 27-36, doi: 10.1109/IC2E.2014.48. [Accessed: 26-Feb-2023]

[3] M. Msahli, M. T. Hammi and A. Serhrouchni, "Safe box cloud authentication using TLS extension," 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, China, 2015, pp. 1-6, doi: 10.1109/SSIC.2015.7245679. [Accessed: 26-Feb-2023]

[4] Jabir, Raja & Khanji, Salam & Ahmad, Liza & Alfandi, Omar & Said, Huwida. (2016). Analysis of cloud computing attacks and countermeasures. 1-1. 10.1109/ICACT.2016.7423295. [Accessed: 26-Feb-2023]

[5] Singh, I. D. (2013, December). Data Security in cloud oriented application using SSL/TLS protocol - IJAIEM. Data Security in Cloud Oriented Application Using SSL/TLS Protocol. Retrieved February 27, 2023, from https://ijaiem.org/volume2issue12/IJAIEM-2013-12-10-022.pdf [Accessed: 26-Feb-2023]

[6] Corelight. (n.d.). Corelight/plotcap: Plot packet and data rates over time given a PCAP file, with gnuplot. GitHub. Retrieved April 11, 2023, from https://github.com/corelight/plotcap

[7] HTTP vs HTTPS TEST. HTTP vs HTTPS - Test them both yourself. (n.d.). Retrieved April 11, 2023, from http://www.httpvshttps.com/

[8] National Archives and Records Administration. (n.d.). The bill of rights: A transcription. National Archives and Records Administration. Retrieved April 11, 2023, from https://www.archives.gov/founding-docs/bill-of-rights-transcript

[9] Simon Fraser University. (n.d.). Retrieved April 11, 2023, from https://www.sfu.ca/

[10] Thomas, M. (2021, January 17). HTTPS vs SSL vs TLS. Medium. Retrieved April 11, 2023, from https://medium.com/plain-and-simple/https-vs-ssl-vs-tls-8a0ad0604276

[11] J. F. Kurose and K. W. Ross, Computer networking: A top-down approach. Harlow: Pearson Education Limited, 2022.