TLS IN THE HOMELAB: THE EASY WAY AND THE HARD WAY

Ketan Vijayvargiya April 27, 2024

Introduction

- Principal Engineer at AWS.
- Self-hosting as a hobby.



Disclaimer: This talk is based on my own experience and understanding of the technology landscape. It does not represent policies or business practices of my current or past employers.

This talk is about ...

- 3 approaches to implement TLS, in increasing order of complexity.
- Practical, with minimal working code: <u>https://github.com/ketan-vijayvargiya/linuxfestnorthwest-talk-2024</u>

This talk is not about ...

- Low-level details of TLS handshake.
- Cryptographic algorithms or math.
- Software recommendations.

Instead, we'll discuss concepts that you can replicate in your setup.

What is TLS, in brief?

- TLS == Transport Layer Security.
 - TLS vs HTTPS.
 - TLS vs SSL.
- Types of encryption:
 - Public key cryptography == asymmetric cryptography.
 - Symmetric cryptography.

Approach 1: Self-signed certificates



Approach 1: In practice

This Connection Is Not Private

This website may be impersonating "whoami-0.wagondime.duckdns.org" to steal your personal or financial information. You should go back to the previous page.

Show Details Go Back



Safari is using an encrypted connection to whoami-0.wagondime.duckdns.org.

Encryption with a digital certificate keeps information private as it's sent to or from the https website whoami-0.wagondime.duckdns.org.

🔀 TRAEFIK DEFAULT CERT



TRAEFIK DEFAULT CERT Self-signed root certificate Expires: Tuesday, April 22, 2025 at 7:56:30 AM Pacific Daylight Time

▲ This certificate has not been verified by a third party

Approach 1: Considerations

Doesn't scale well.

Approach 2: Certs generated by a Certificate Authority

- Noteworthy in the image:
 - ACME protocol.
 - Certificate authority could be:
 - Public, possibly free, such as Let's Encrypt.
 - Custom or self-hosted.



Approach 2.1: In practice, when using a public CA

curl https://whoami-1.wagondime.duckdns.org

	sing an encrypted connection to wagondime.duckdns.org.
	with a digital certificate keeps information private as it's sent to or from the te whoami-1.wagondime.duckdns.org.
☐ ISRG Root X1 L, R3	
🖵 📴 whoami-1.wa	gondime.duckdns.org
Issuer Name	
Country or Region	
Organization Common Manua	Let's Encrypt
Serial Numbe Versior	r 03 C2 82 DF 87 E5 E4 B7 D8 83 68 05 5E 99 84 19 F1 E7
Version	
? Hide Cer	rtificate OK

Approach 2.1: Considerations

- Verify validity of the certificates.
- Certificates publicly logged on <u>https://crt.sh/</u>.
 - Wildcard certs through "DNS challenge" provide some mitigation. (See accompanying code.)

Approach 2.2: In practice, when using custom CA



. LinuxFestNorthwestTalk Root CA LinuxFestNorthwestTalk Root CA Certificate Root certificate authority Expires: Tuesday, April 4, 2034 at 6:13:50 PM Pacific Daylight Time S This root certificate is not trusted ✓ Trust When using this certificat ✓ Use System Defaults ? Always Trust Secure Sockets Layer (SSI Never Trust Secure Mail (S/MMI Extensible Authentication (EAP) no value specified IP Security (IPsec) no value specified Code Signing no value specified Time Stamping no value specified X.509 Basic Policy no value specified ✓ Details Subject Name Organization LinuxFestNorthwestTalk Common Name LinuxFestNorthwestTalk Root CA

Kevchain Access File Edit View Window Help

Approach 2.2: Considerations

- curl --cacert root_ca.crt <u>https://whoami-2.wagondime.duckdns.org</u> works.
- BUT curl --insecure <u>https://whoami-2.wagondime.duckdns.org</u> also works.

How does TLS handshake work, in brief?



Image credits: https://www.cloudflare.com/learning/access-management/what-is-mutual-tls/





How does mTLS handshake work, in brief?



Image credits: https://www.cloudflare.com/learning/access-management/what-is-mutual-tls/

Approach 3: mTLS (== mutual TLS)



Approach 3: In practice

curl --cert client.crt --key client.key --cacert root_ca.crt \

https://whoami-3.wagondime.duckdns.org



Considerations while setting up a custom CA

- Manage root certificate on all clients.
 - Additionally, client certificates for mTLS.
- Rumors that:
 - Some reverse proxies don't play well with public and custom CA together.
 - Some Android apps don't work.

Accompanying code

https://github.com/ketanvijayvargiya/linuxfestnorthwest-talk-2024. (Scan the QR code.)

- Traefik: reverse proxy.
- Docker: service management.
- Domain: free from Duck DNS.
- Let's Encrypt: public CA.
- Step CA: custom CA.



Thanks!

Contact: <u>https://ketanvijayvargiya.com/</u> (Scan the QR code.)



Questions?

