A new gRPC service for Transport Layer Security (TLS) Configuration

Saju Salahudeen
Principal Consulting Engineer, NOKIA
Member – NANOG Education Committee

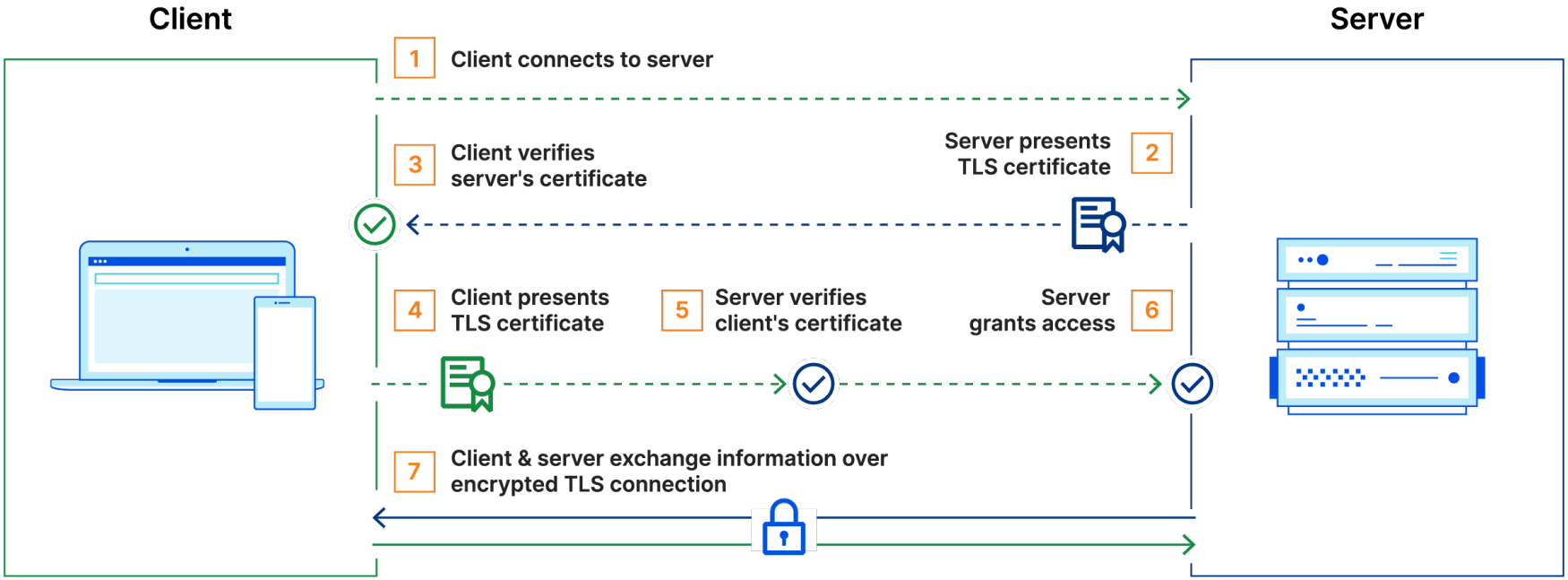
Why TLS and Certificates?

*13 reported data breaches in 2024 until June 1

- Protect applications from data breach
- Encrypt all communications between applications and servers
- Authenticate clients and servers before exchanging information
- Verify integrity of the received data

*Source - https://tech.co/news/data-breaches-updated-list

TLS Overview



Source:
https://www.cloudflare.com/en-gb/learning/access-management/what-is-mutual-tls/

Security on Routers

Non-TLS

- SSH for CLI and Netconf
- Protocol level (BGP)
- Encrypt locally stored password, config, files
- MACSec, IPSec, AnySec

TLS

- SNMPv3
- gRPC services
- PCEP
- LDAP, RADIUS
- Syslog
- Secure ZTP

Challenges with TLS Configuration on Routers

- Generating certificates
  - Initial communication is unencrypted
- Validating certificates
- Configuring applications to use certificates
- Debugging

Management of the PKI elements for a network system should have a clear and direct method for installation and update.

TLS Configuration Tools Used Today

OpenSSL
Cryptography and SSL/TLS Toolkit

CONTAINERlab

gNOIc

```
--{ + running }--[  ]--
A:srl1# tools system tls
                        generate-csr
                        generate-self-signed
                        server-profile
```

GitHub

gRPC Introduction

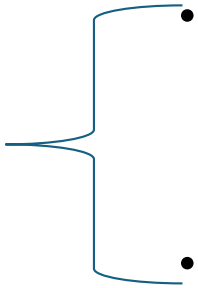
- RPC framework using HTTP 2.0 as underlying transport
- Does not expose HTTP 2.0 to the user (unlike REST)
- Uses a binary payload
- HTTP 2.0 helps with efficient management of connections
- Requires gRPC software on both client and server

gRPC Cert Management Services

- gNOI
  - gRPC Network Operations Interface
  - Execute Operational commands on the router
  - Cert service to manage TLS certs on the router
- gNSI
  - gRPC Network Security Interface
  - New gRPC service introduced for security configuration
  - Services – Authz, Certz, Credentialz

gNOI Cert Service and RPCs

- Cert
  - CanGenerateCSR
  - GenerateCSR
  - InstallCertificate
  - RotateCertificate
  - LoadCertificate
  - GetCertificates
  - RevokeCertificates



- Advertise router's capability to generate Certificate Signing Request (CSR) and generate one if supported.
- If not possible, certificate must be generated external to the router and both signed cert and key should be transferred over to the router

What is missing in gNOI?

- TLS Profile management on router
- Certification Revocation List
- Loading initial certificate is not supported and should be done manually

gNSI

- gRPC Network Security Interface
- gRPC based service for defining and retrieving security configuration
- Standards defined by OpenConfig - https://github.com/openconfig/gnsi

gNSI – Default TLS Profile

- A key requirement of gNSI
- System should boot up with a default TLS profile using a system generated signed certificate and private key.
- Allows gRPC server to start as part of default config
- Why does this matter - Initial gRPC communication can be encrypted

gNSI Certz Service

- Replace a certificate, trust bundle or CRL on a target
- Supported RPCs:
  - AddProfile
  - DeleteProfile
  - GetProfileList
    - Manage TLS profile on the router
    - Add/Delete/Get TLS profile
  - CanGenerateCSR
    - Respond with certificate if router can generate one
  - Rotate
    - Install or rotate certs, trust or CRL bundle

Summary

- gNOI can be used for certificate generation, load, rotate and revoke
- gNOI does not support configuring TLS profiles on the router
- gNSI supports RPCs to configure, delete or list TLS profiles on the router
- gNSI supports CRL bundle

Thank you