Network Security Protocols and Beyond…

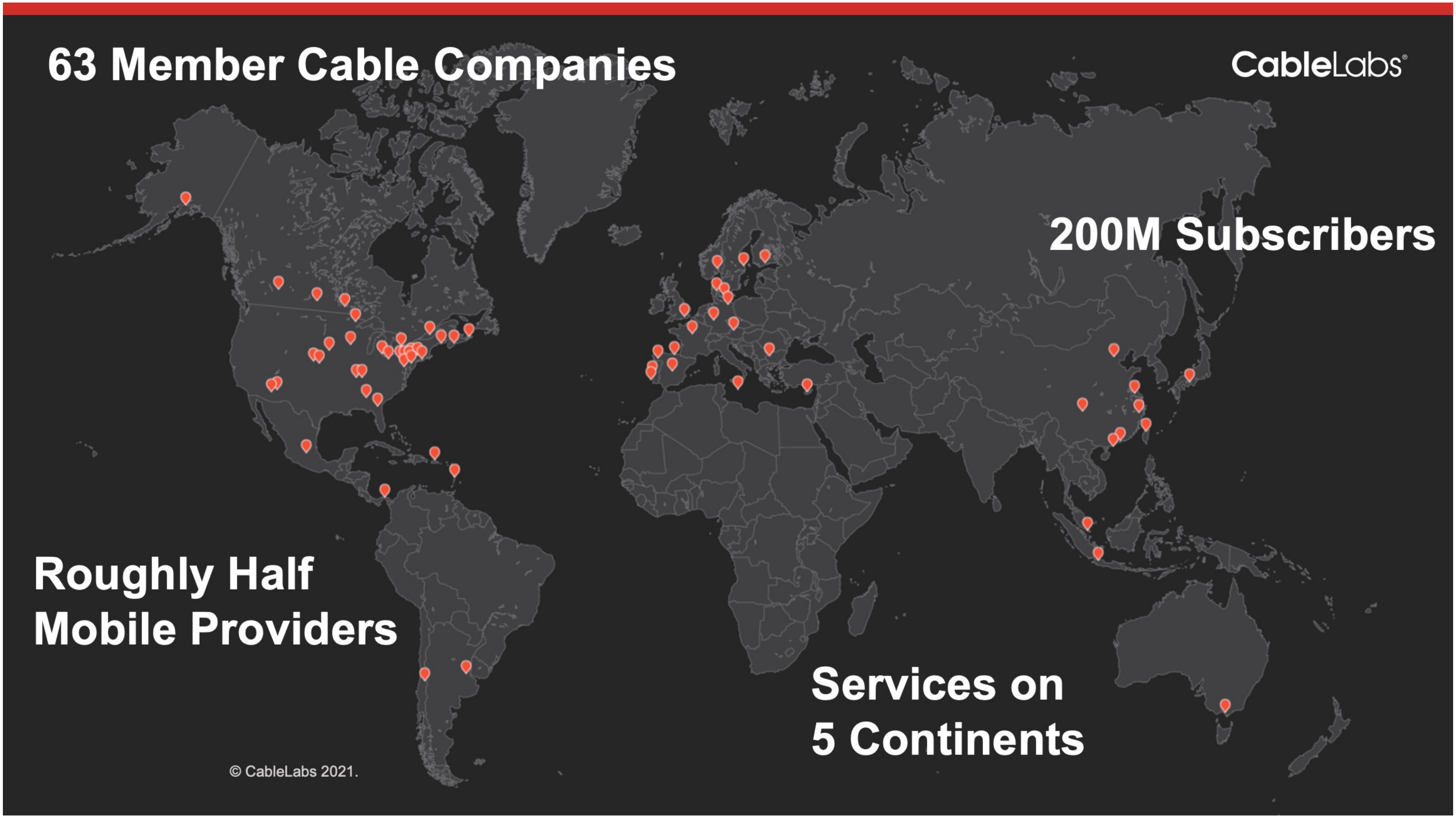
May 2022

- Security & Privacy Technologies Overview
- DOCSIS® Security 4.0
- Route Engineering
- Gateway Device Security

Security & Privacy Technologies

CableLabs®

Brian Scriber
Distinguished Technologist & Vice President
Security & Privacy Technologies, CableLabs
b.scriber@cablelabs.com



63 Member Cable Companies

CableLabs®

200M Subscribers

Roughly Half Mobile Providers

Services on 5 Continents

CableLabs Governance

Board of Directors & Technical Committee, CEOs and CTOs from...

CABLE ONE

COGECO

VIDEOTRON

Charter COMMUNICATIONS

J:COM

MIDCO

LIBERTY GLOBAL

vodafone

COMCAST

ROGERS

Shaw)

COX

Mediacom

GCI Liberty

Vision

Security & Privacy Technologies
CableLabs

The CableLabs Security and Privacy Technologies team drives innovation toward a unified threat-resistant networking environ for both wired and mobile experiences.

Security & Privacy Technologies Mission

We research, develop, publish, improve, and influence tools and standards to advance security and privacy.

We develop new controls to keep our industry ahead of threats and adversaries on the network.

We develop communities that evangelize and foster collaboration, dissemination of knowledge, best practices and training.

Security & Privacy Technologies
CableLabs®

Foundations of Digital Security

Identity:

- Network endpoints should have a digital ID that is immutable, attestable, and unique

Confidentiality:

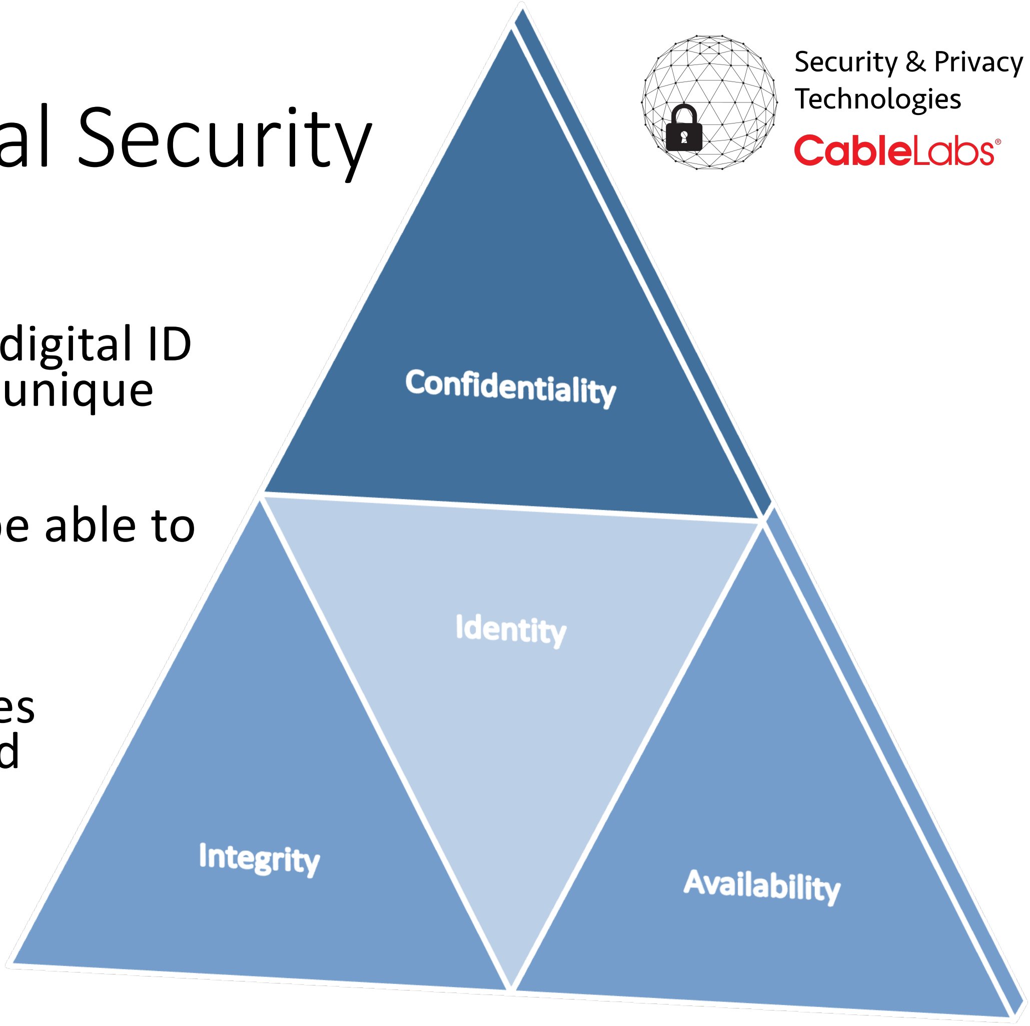
- Third party observers should not be able to read or intercept traffic

Integrity:

- Must be able to trust that messages have not been altered or corrupted

Availability:

- Network services and endpoints are reachable and functional

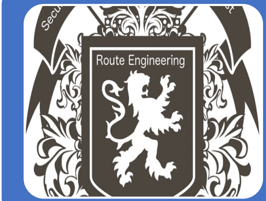


Protocols and Beyond:

Security & Privacy Technologies
CableLabs®

DOCSIS® 4.0 Adoption

- Confidential Traffic Delivery
- Provide Upgradeable Security Posture



BGP - CREST: Cable Route Engineering

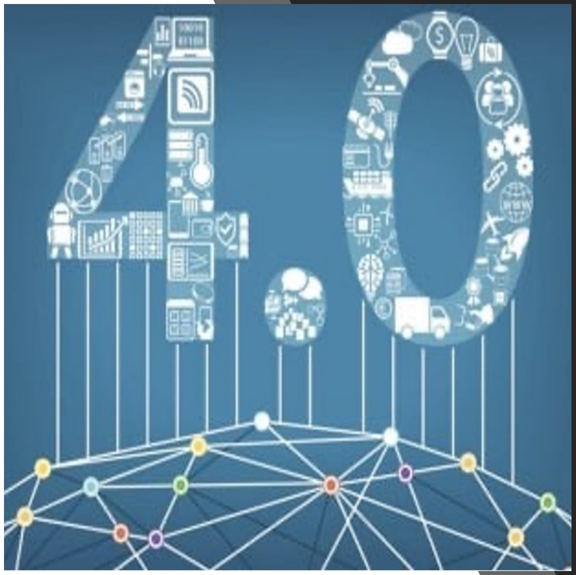
- Implementation guide for RPKI and BGP
- Best Common Practices Published in January 2022

Gateway Device Security

- Best Common Practices doc for ONT/routers/modems/gateways
- October 2021 Published & Released

DOCSIS 4.0 Security

Security & Privacy Technologies
CableLabs



Objectives:

- Deliver traffic confidentially
- Dissuade theft of service
- Provide an upgradeable security posture

New Features:

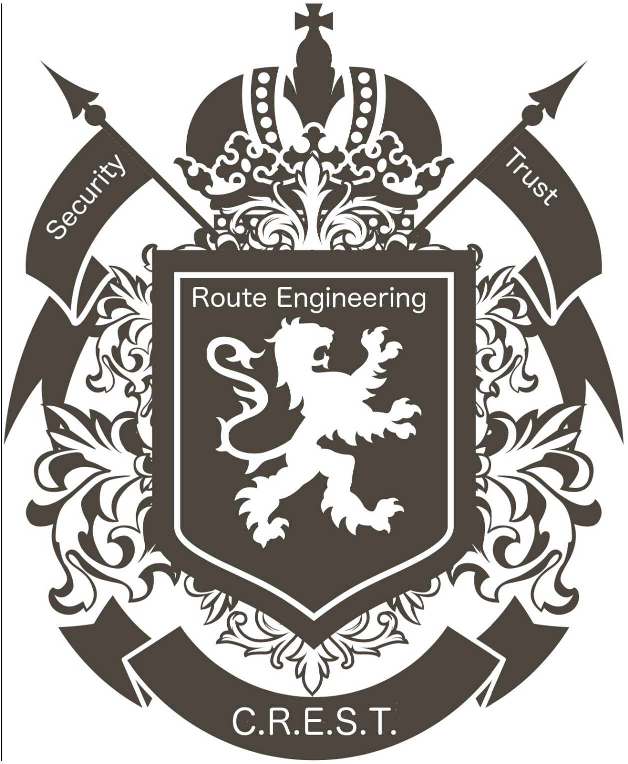
- Mutual authentication between modem & network
- New cryptographic parameters
- New security controls
- Enhanced digital certificate capabilities

Security & Privacy
Technologies
CableLabs

C.R.E.S.T.

Cable Route Engineering for Security and Trust

- BGP Route Hijacks and DNS Hijacks
- RPKI (Resource Public Key Infrastructure)
  - Cryptographic improvement to BGP
  - Sign prefix ownership (Route Origin Auth)
  - Verify inbound route announcements (ROV)
- Risks & Benefits
  - Mitigates hijacking of your prefixes
  - Protect customers from other prefixes
  - Doing this wrong can result in isolation
  - Reconnection can be time-consuming & challenging



Gateway Device Security

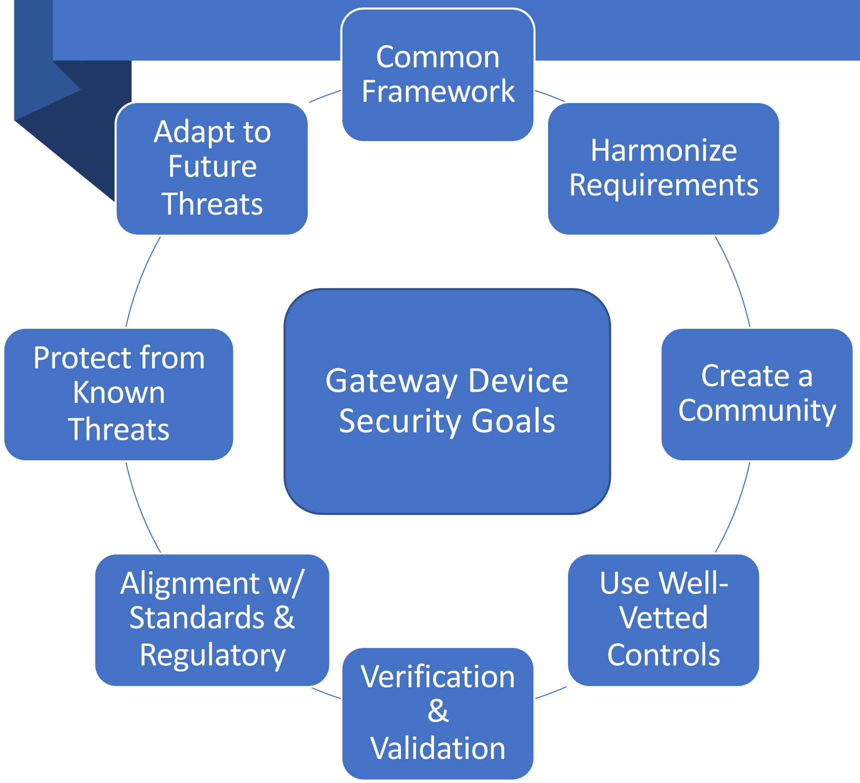
Security & Privacy Technologies
CableLabs

- Cable industry initiative to build a “Best Common Practices” document for the security of leased and retail devices

- Scope:
  - Gateways, home routers, and cable modems in scope
  - Hardware/software/firmware/process/supply chain security
  - Manufacturing process and supply chain

- Provides a consistent framework for devices across the industry
- Influences manufacturer product roadmaps

Gateway Device Security: Goals & Scope



Gateway Device Security Goals

Common Framework

Harmonize Requirements

Create a Community

Use Well-Vetted Controls

Verification & Validation

Alignment w/ Standards & Regulatory

Protect from Known Threats

Adapt to Future Threats

Key Elements of the GDS Best Common Practices:

1. Hardware
2. Secure Boot
3. Configuration
4. Data Encryption & Integrity
5. Cryptographic Material
6. Interfaces
7. Diagnostic/Development Access
8. Logging/Audit
9. Time Synchronization
10. Software BOM and Updates
11. Network and Processes
12. Network Mechanisms (e.g., Wi-Fi/BT/NFC/Cellular)
13. Audio and Video Sensors

CableLabs®

Network Security: Protocols and Beyond

May 2022

CableLabs

Brian Scriber
Distinguished Technologist & Vice President
Security & Privacy Technologies
b.scriber@cablelabs.com