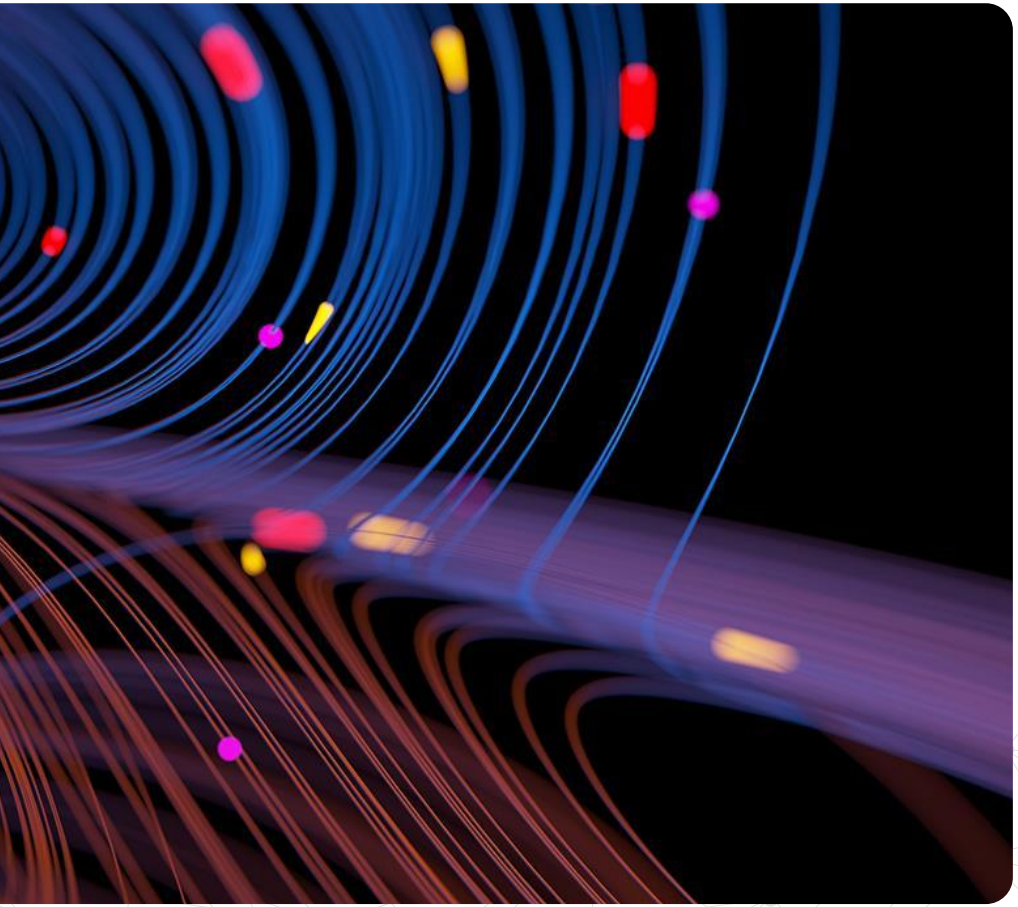
Securing modern telco networks

What's new & why should you care?

Patrick Ohearn – AusNOG 2026



Why are we here?

- We want secure networks
- We care about customers privacy
- You want to see me shout into the void about securty
- PC didn’t have enough submissions

Who am I?

- Patrick Ohearn
- Network Architect – International @ AARNet
- 15 years of experience working for Aussie telcos
- Enjoy talking about service provider networking & security
- patoh @ b4p slack

What makes a modern telco network?

Why do we care about secure networks?

- **Confidentiality, Integrity, Availability**
- **Privacy**
- **Being a good network operator**
- **Regulation under TSSR, now SOCI (TSRMP)**
- **CI Fortify guidelines**
- **Do we actually care?**

Current state of play

- Increased number of commodity breaches
- *“Nation states gonna nation state”*
- Increased regulation
- More service offerings
- Hardware vendors
- Software vendors
- Telemetry / Agents reaching into more systems than ever
- Fortnightly NOS updates coming to a vendor near you soon™

What's new?

- Speed some attackers are moving
- Resources attackers have access to
- Operators have forgotten lessons of the past
- Converged packet & optical networks
- Government compliance & oversight is catching up
- It's here because of industry failures
- Rogue employees
- Fundamentals *really* matter

Anthropic partners have used its bug-hunting Claude Mythos AI to uncover 10,000 "high- or critical-severity vulnerabilities across the most systemically important software in the world.

May '26 - au.pcmag.com

High velocity of slop

Mythos & other security-focused models are here

Some vendors working directly with frontier labs

- **Cisco:** Working with frontier labs directly
- **Juniper HPE:** Working with frontier labs directly
- **Nokia:** Customers working with frontier labs
- **Arista:** Customers working with frontier labs
- **Mikrotik:** No public info on use of security focused LLMs

Fundamentals

Fundamentals

SSO & RBAC	MFA external & critical access paths	Per device/ service creds	Segmentation	Backups
Don’t share auth between Corp & Telco	Jumphost/TS controls	Break glass accounts	Inband management	Online
JIT access		One time use creds	Out of band management	Offline
			Food & water services	Restoring from a total compromise

Fundamentals - NOS

Consistent software deployment	Consistent config deployment	Monitoring & alerting	Vendor hardening guides	Basic hygiene
	Automated deployment	Alert on reboots, FW/SW changes	CoPP/RE Filters	Time synchronisation
	Automated verification	Investigate all coredumps	App. Filters	Remote logging
			Please, please, please disable telnet	Disable unused services / packages

Fundamentals – Supply Chain

Equipment Vendors	Software suppliers	Cloud Providers	Managed Service Providers	Outsourcing Arrangements
Decrease use of 2nd hand gear	Signed package updates	Trusted Computing	Vetted Suppliers	Rogue Employees
Secure shipping				

Fundamentals - Hardware

SecureBoot	Physical security	Hardware inventory monitoring	Hardware supply chain	High risk environments
Understand its limitations	Central access control	Log inventory changes in realtime		Reduce active equipment
	Passive asset monitoring			
	Cameras			

Fundamentals – OSS/BSS

BSS systems such as billing are key targets	Visibility into externally hosted platforms	External vendor & contractors	Isolate OSS/BSS functions from vital systems
Financially motivated attackers love customer data	Audit & logging of SASS solutions	Treat access as JIT	
Juicy targets for espionage (CDRs, metadata)		Verify identities & audit access logs	

Quick Wins

Transport encryption

- L1 – OTNSec, WDM encryption & black boxes
- L2 – MacSec & blackboxes
- L3 – IPSec, Wireguard etc;
- L4+ - SSH, TLS
- Performance impacts
- Costs & licencing needs to be factored in
- Vendors need to improve encryption features
- Make it a selling point

PQC (Post Quantum Encryption)

May be required sooner than we think

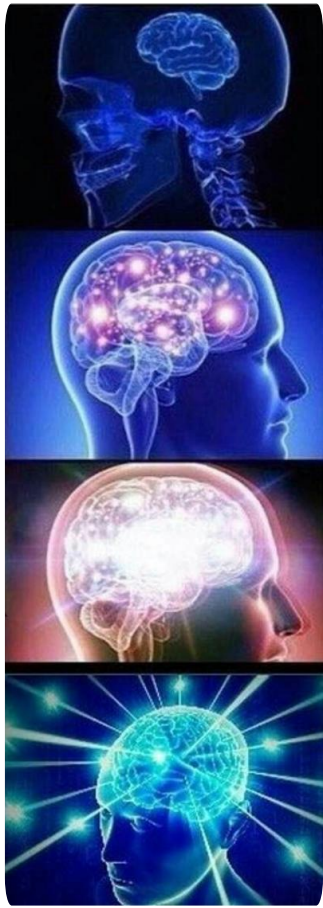
ECC/RSA are dead

Lattice based schemes

Unlikely to impact transport encryption

Impacts SecureBoot, package signing, etc;

Can require new hardware



Routing Security

RPKI

Route Filtering
Prefixes | ASNs

BGP Enforce First AS

OTC (RFC 9234)

ASPA (Draft)
APNIC support as of July ‘26

Industry Collaboration

Build & maintain relationships with other telcos

Compare notes with other Service Providers

Talk to ASD/Home Affairs

Share with others

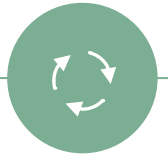
- Present @ Conferences
- AusNOG List
- Industry Forums

Bringing it all together

Bringing it all together

Fundamentals are critical

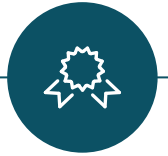
Monitor & chase continuous improvement



Software patching cadence is more important than ever

Deploy PQC where practicable all the way up/down the stack

Transport encryption is an easy win



Vendor QA needs to keep up – currently lacking

Other great talks & articles

- Building an OOB network – APRICOT 2026 (Phil Mawson)
- Communicating Under Pressure – CISA Sept 2026
- Defending Telco Networks – AusNOG 2025 (Anthony Schofield)
- Frontier AI: A New Era of Cyber Resilience – Visa June 2026
- Photonic and Packet Networks Collide – AusNOG 2024 (Nic Tipplet)

Links – https://400gbits.net/ausnog2026

Thank You

Questions?