ENTELEC conference & expo

New perspectives on cyber security for radio and LTE field area networks

John Yaldwyn, CTO

4RF USA, Inc

ENTELEC conference & expo

Field area networking

Field area networking

Introduction to field area networking

Private narrowband **radio** is a key technology for field networks addressing SCADA needs with **reliability, redundancy, and resilience**

Point-multipoint private radio SCADA operating in available licensed channels has stepped up to supporting full **multi-application IP-based Field Area Networks** with new high capacity radio options with the bandwidth necessary to support multiple applications over a common radio infrastructure

Recent developments in private spectrum availability has made possible **private LTE**, while **public LTE** is also an option for less critical applications

Today's oil and gas operations require a range of applications to be supported while the costs of networking are under pressure with low oil prices

- IP SCADA products bring **new protocol, security, and management needs** that drive expectations for radio system capacity requirements
- Private and public LTE is tempting from capacity and costs perspectives but again security, both interception and service continuity, are key issues

From SCADA to the Field Area Network

SCADA radio is a **widely deployed** traditional solution with a **strong heritage**

Point-to-multipoint operation, typically with directional antennas at remote sites

Private licensed sub 1 GHz QAM **high capacity** radio is now a strong FAN option, bands include

- VHF, UHF and 700/900 MHz

Public LTE from well known common carriers like AT&T and Verizon

Private LTE using purchased spectrum examples include Anterix Band 8 or CBRS Band 48

FAN technology toolbox for field networks and M2M / IIoT

Tasks include data gathering and remote control of machinery

Distances are typically in the range 5 to 75 miles, sometimes more

Number of remotes can vary from hundreds to thousands

Communication options

- Private radio VHF/UHF and 700/900 MHz SCADA
- Unlicensed spread spectrum
- IEEE 802.16S
- LTE IoT (NB-IoT and CAT-M)
- LTE (private and public)

What are the options?

What do field area networks need?

Licensed / unlicensed radio and public / private LTE

Metric	VHF/UHF/700/900	Unlicensed Radio	Public / Private LTE	NB-IoT	CAT-M
Dedicated spectrum needed	No	No 900 MHz	Yes 1.4 – 20 MHz	Usually 200+ kHz	Yes 1.4 MHz
Speed	60 – 500 kbps	60 – 500 kbps	5 – 100+ Mbps	50 – 75 kbps	375 kbps – 1 Mbps
Latency	Low 10 – 50 ms	Variable	Variable	High 1.6 – 10 s	Low 10 – 15 ms
Priority	High	Variable	Variable	Medium	Medium
System cost	Low	Low	High	High	High
Terminal cost	Medium	Medium	Low	Low	Low
Security	Very high (vendor)	Variable	High	High	High
UE transmit power	High 37 dBm	High 30 dBm	Low 23 dBm	Low 20 / 23 dBm	Low 20 / 23 dBm
Reliability	High	Low	Variable	High	High
Deployment time	Low	Low	Variable	Variable	Variable
Recovery time	Low	Low	High	High	High
Standards	Few	None	Yes	Yes	Yes

Recommend for real time control and product metering

Recommend for non-critical metering, GUI, and mobile workforce productivity

ENTELEC conference & expo

Security basics

Radio system threat vectors – including cellular

CIA three pillars – confidentiality, integrity, and availability

Confidentiality – critical data and configurations

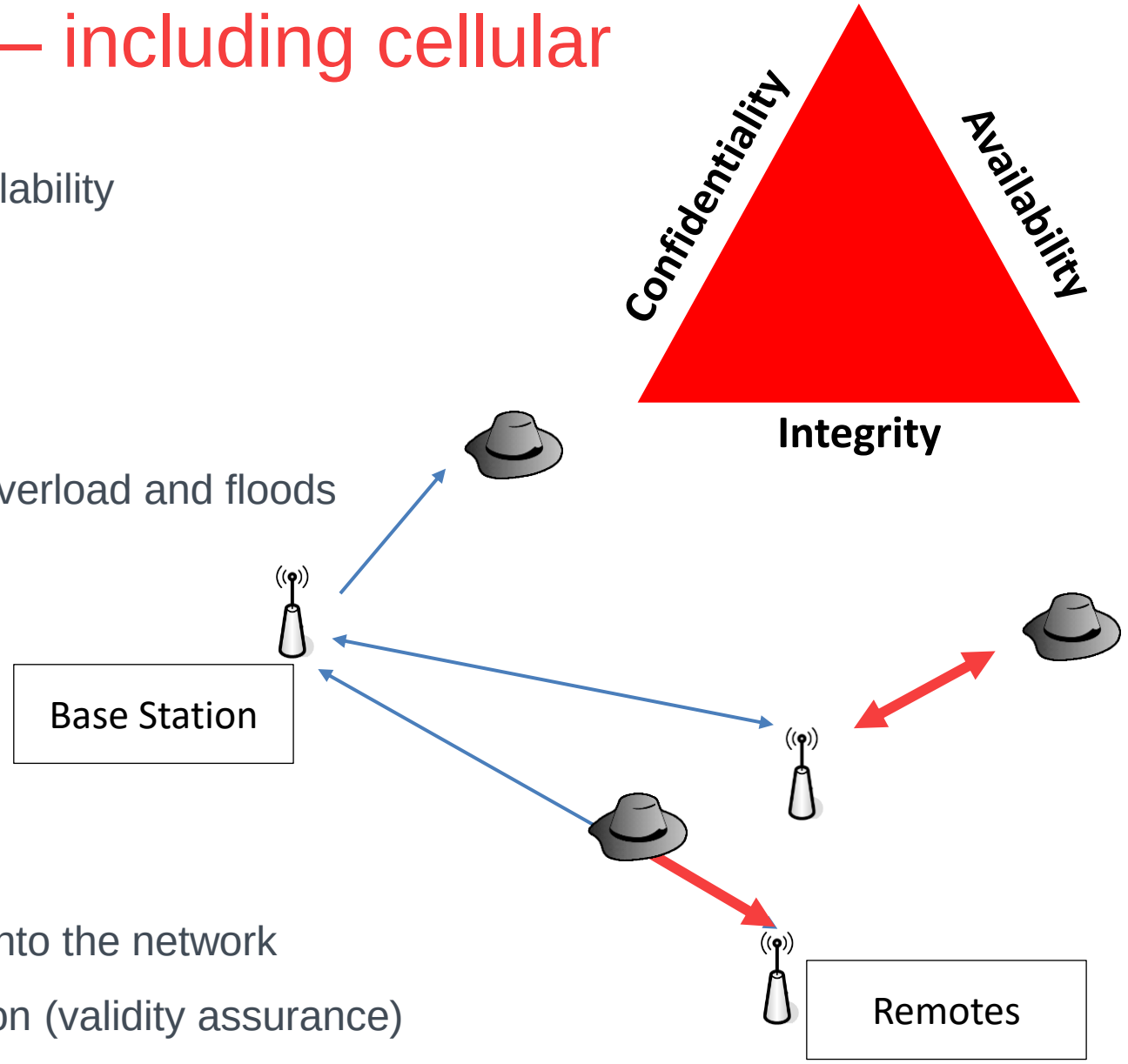
- Eavesdropping

Availability – denial of service

- Robust wireless physical layer – proof against overload and floods

Integrity – man in the middle (anti-replay)

- Authentication is key – encryption little help



In SCADA context we need to add

- Management functionality – possible backdoor into the network
- Accountability (user tracking) and non-repudiation (validity assurance)

Radio system protections – including cellular

Protections – both vendor and implementation dependent

Critical that appropriate safeguards are specified

Pillar	VHF/UHF/700/900 Licensed Radio	Unlicensed Radio	Public / Private LTE
Confidentiality	AES encryption	AES encryption	IPsec
Availability	High	Low	Public – medium / Private High
Integrity	NIST CCM	NIST CCM	IPsec
Management	SNMPv3 & RADIUS	SNMPv3 & RADIUS	Complex

AES = NIST advanced encryption standard

IPsec = Configured correctly provides data integrity, encryption, authentication and anti-replay

NIST CCM = Message authentication mechanism (NIST and IETF standards)

SNMPv3 = Industry standard management protocol, version 3 specifies authentication and encryption

RADIUS / TACACS = Validation of users at management interfaces via centralized database

Over-the-air Symmetric Encryption

Encryption is used to reduce information leakage

Robust cryptographic algorithm important, today this is AES

Key is symmetric, same key used to decrypt and encrypt

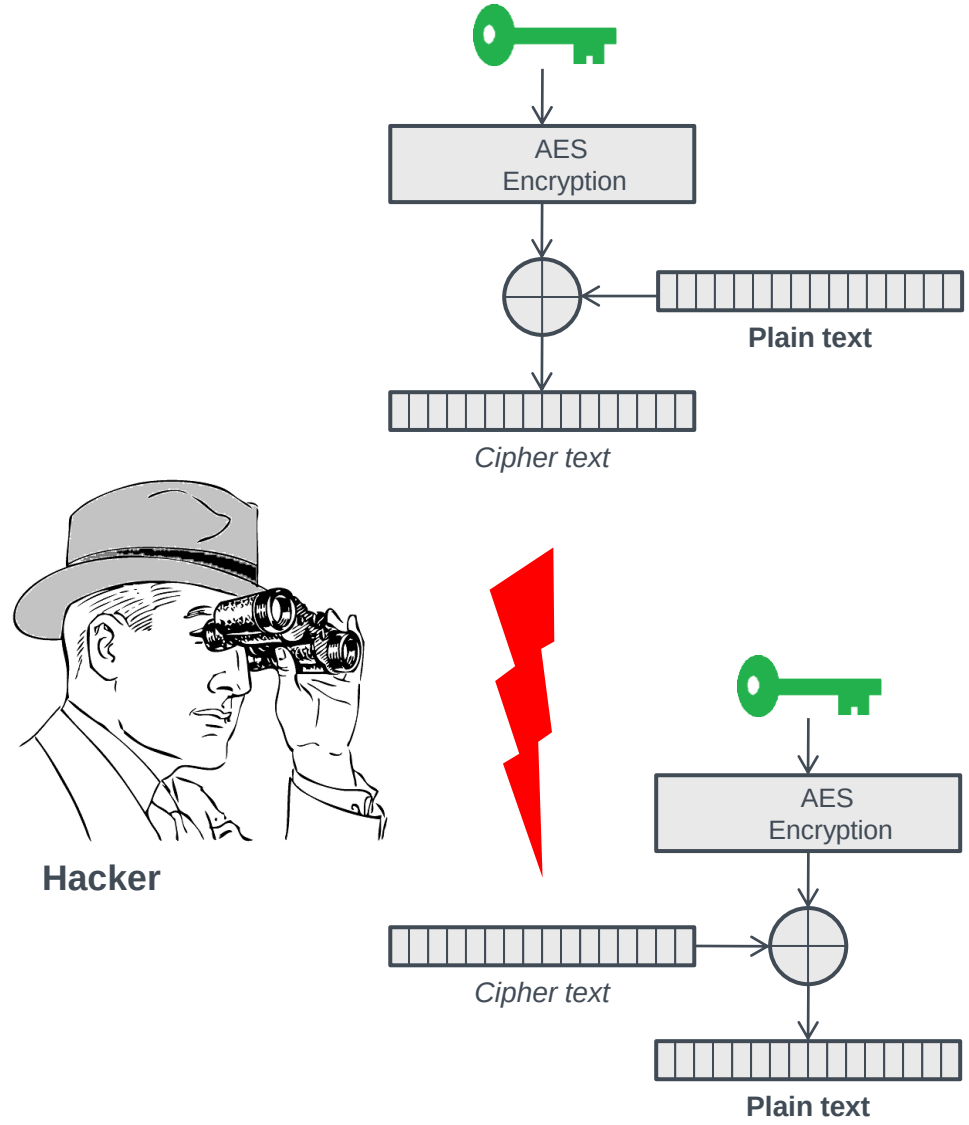
AES 128 bit block with 128, 192, or 256 bit keys

Security based on algorithm and shared secret key

Algorithm is public so key must be secret

Why change the key?

- Repetitive traffic increases ‘depth’ weakens protection
- **Regularly changing key** guards against compromise
- So we need a means to distribute new keys



Message Authentication – CCM CBC MAC

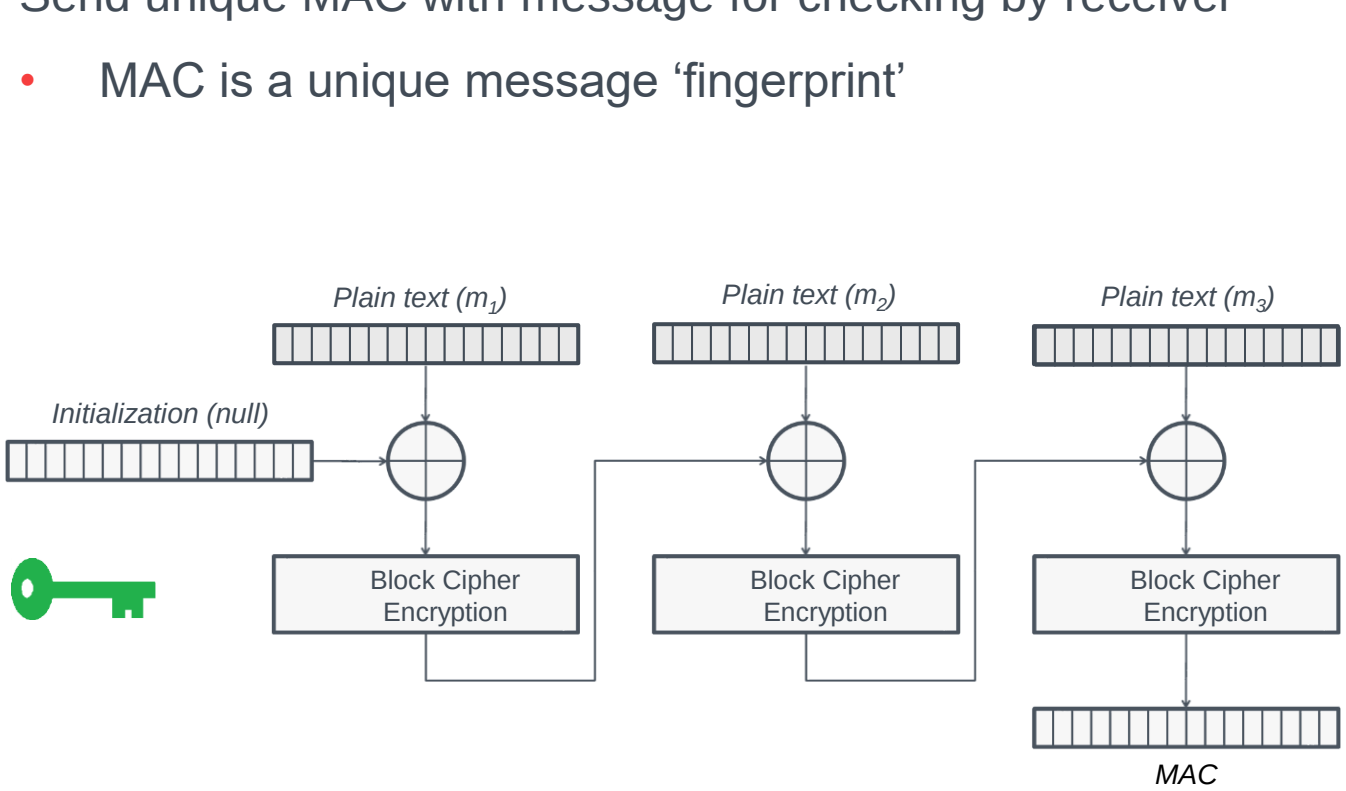
Counter mode encryption with cypher block chaining message authentication

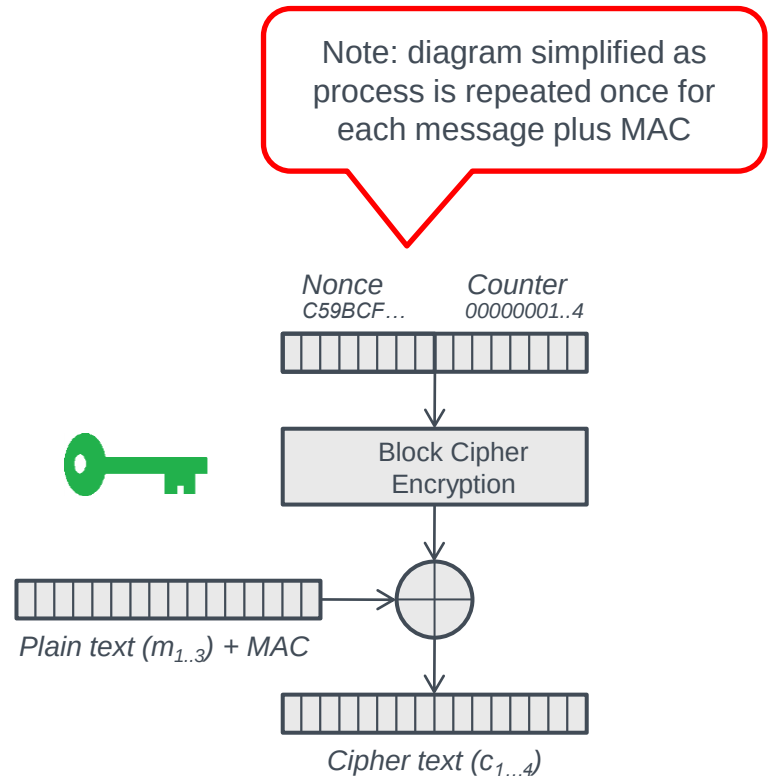
CCM CBC MAC method with AES block cipher = AES (NIST SP 800-38C / RFC3610)

Message authentication code (MAC) then optionally encrypt

Send unique MAC with message for checking by receiver

- MAC is a unique message ‘fingerprint’





What is RADIUS and AAA?

RADIUS is a client/server system that secures user access against unauthorized logins

- Transactions between the RADIUS client and RADIUS AAA server/accounting server are authenticated through the use of a shared secret, which is never sent over the network
- RADIUS access a central RADIUS server, makes management of users easier and more consistent
- SR+ authentication can be configured to use RADIUS only, local access only or both
- Based on IETF RFCs 2865/6, 5607, 5080, and 2869

User is prompted for username and password

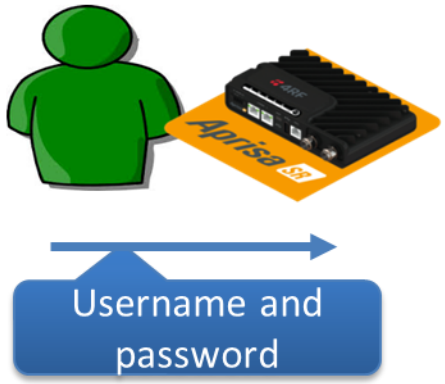
- Credentials sent to RADIUS server

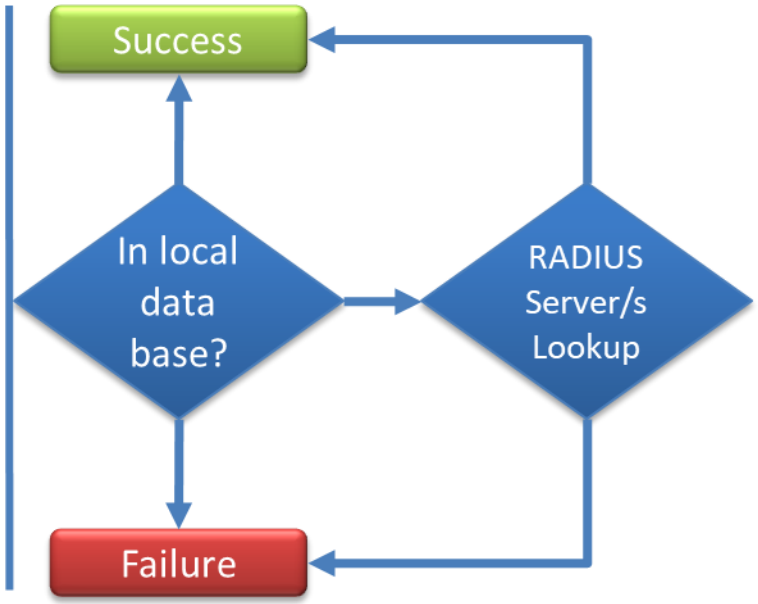
End device receives from server

- ACCEPT or REJECT response

Accounting audit process invoked

- Records time/date, etc

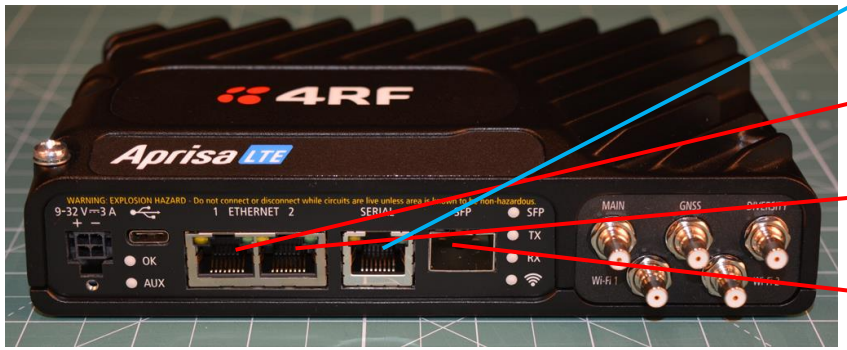


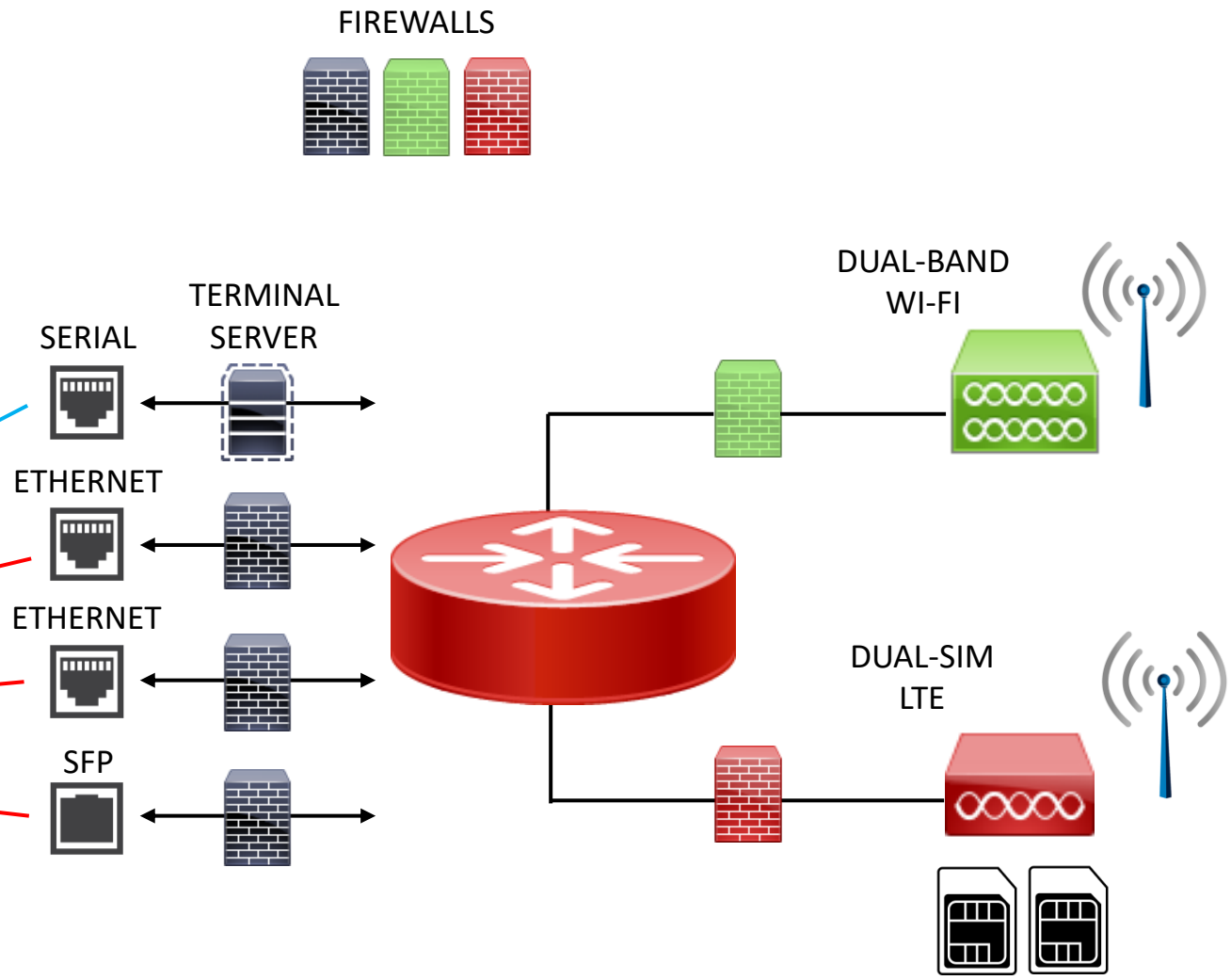


Use of internal firewall features in end devices

Good practice to distribute firewall technology right out to the network edge

- So called micro firewall approach
- Possible today to include enterprise grade firewalls in UE and even IoT devices





FAN optimization – modelling and IP traffic

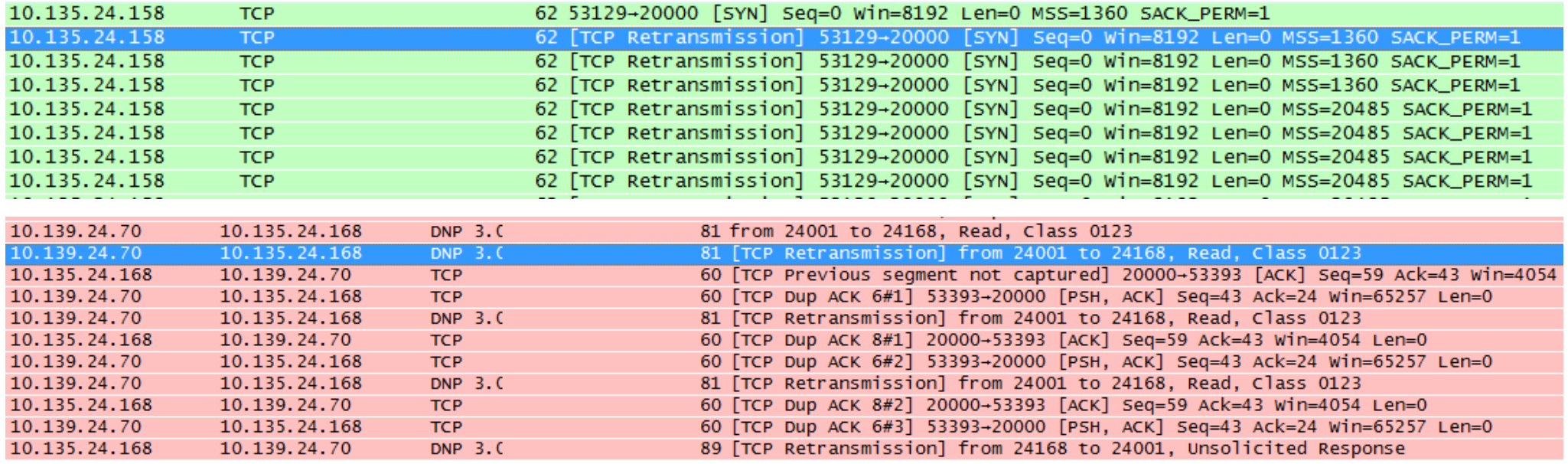
Important not to overlook tools needed to model and understand system usage

- Use tools to consider the types of IED / RTU traffic and payloads

IP investigation (Wireshark)

- Excessive TCP connection SYN packets and excessive TCP retries

Migrate to report by exception, use UDP traffic, and use traps rather than polling



ENTELEC conference & expo

NIST Special Publications

ICS Security

Security implementation underpinnings

Security must be designed in from the start

Strong AES (128 or 256) over-the-air security with provision for routine rekeying

Sequential message authentication CBC-MAC (prevents replay attacks)

Secure NMS SNMPv3 and element management via HTTPS with ECC

User authentication and AAA via RADIUS

Implementation of general agency advice and specific standards

- FIPS PUB 197 AES encryption
- IEC/TR 62443 Industrial Communications Networks – Network and System Security
- IEEE P1711/P1689/P1686 Substation Committee cyber standards
- IETF RFC 3394 Key wrap, RFC 3610 CBC CCM, RFC 4492 ECC Cipher Suites for TLS
- NIST IR-7628, Smart Grid Cyber Security Strategy and Requirements
- NIST Special Publication 800-56A, NIST SP 800-38D
- NIST cellular Special Publication 800-187 and IoT standards NISTIR 8228 & NISTIR 8259

NIST – Information Technology Laboratory

National Institute of Standards and Technology, part of the U.S. Department of Commerce, publishes a wide range of industrial control system (ICS) security related materials and is a very useful resource for both equipment designers and network implementers

Guide to LTE Security – NIST Special Publication 800-187

- A guide to the fundamentals LTE networks security architecture
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-187.pdf

Foundational Cybersecurity Activities for IoT Device Manufacturers – NISTIR 8259

- Advice for IoT manufacturers for improving IoT security
- https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf

Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks – NISTIR 8228

- Understanding and managing IoT device cybersecurity and privacy risks
- https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf


ENTELEC
conference & expo
UBBA
Security work

Broadband LTE ecosystem advocacy

UBBA

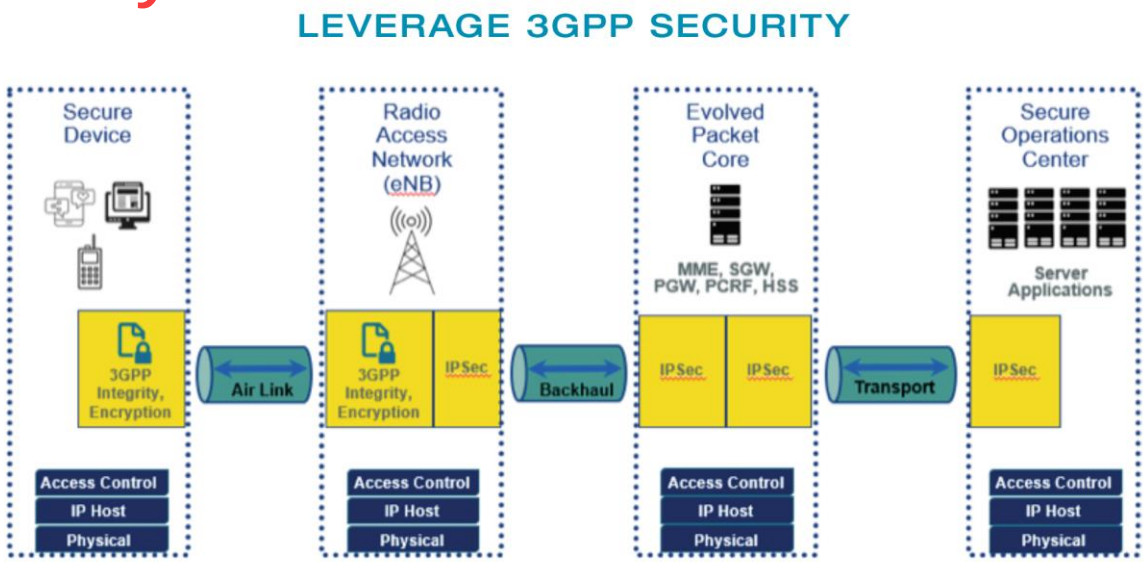
Cyber Security and Use Case working groups

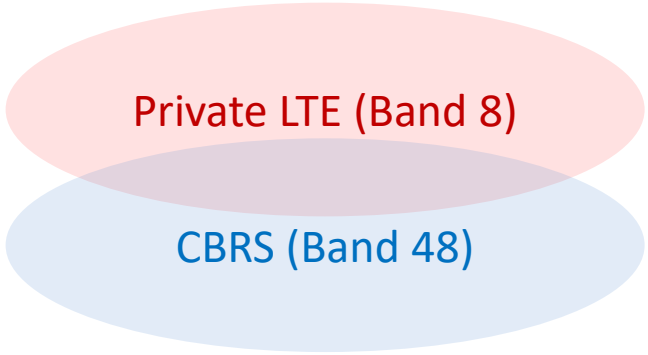
- White papers
- Industry and vendor workshops

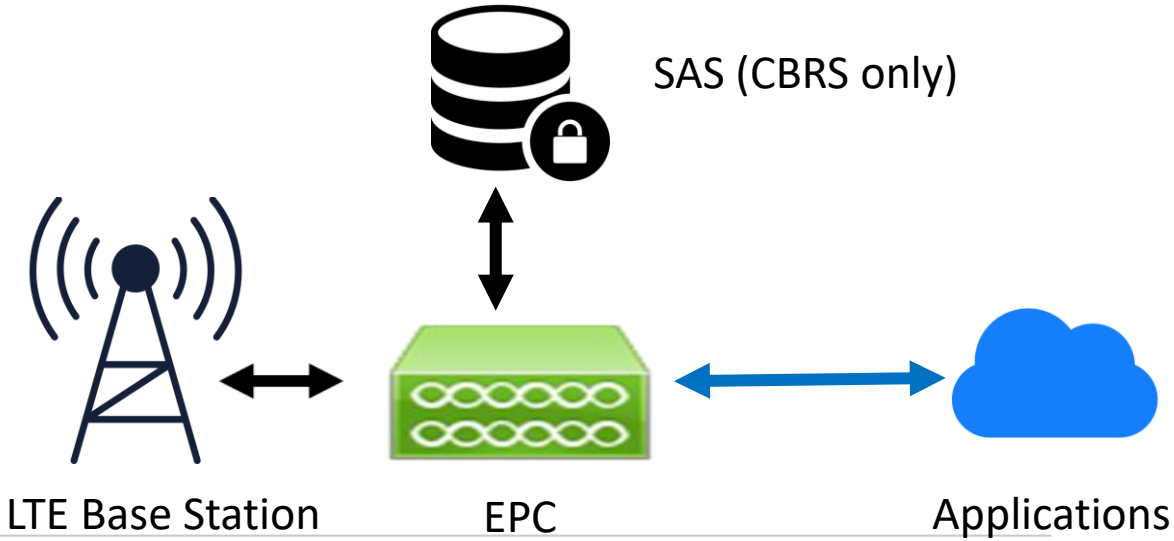
CBRS Alliance

Support the development of 3.5 GHz CBRS

- Technical speciation overviews
- Network and spectrum economics
- Use cases







UBBA broadband alliance

UBBA members represent a wide range of utility industry stakeholders including utilities, oil and gas, and pipelines

- Championing the development of private broadband networks for America's critical infrastructure industries

Through UBBA vendors, carriers, and end users have joined to work together towards developing private LTE ecosystems

ENTELEC conference & expo

Post-Quantum Cryptography

Certificates and Post-quantum Cryptography

Quantum computing will eventually threaten many if not most public/private key systems used to establish trust and exchange symmetric algorithm keying material

- Examples are RSA, Diffie-Hellman, and ECC (elliptic-curve cryptography) used primary for symmetric key exchange

Unknown if ‘quantum supremacy’ will actually threaten existing methods but NIST is taking precautionary approach

NIST Post-Quantum Cryptography Standardization Process underway, started with 26 candidate methods

- More or less evenly split of ring theory lattice methods, linear code based, and other methods

Of these, the lattice theory ideas have predominated

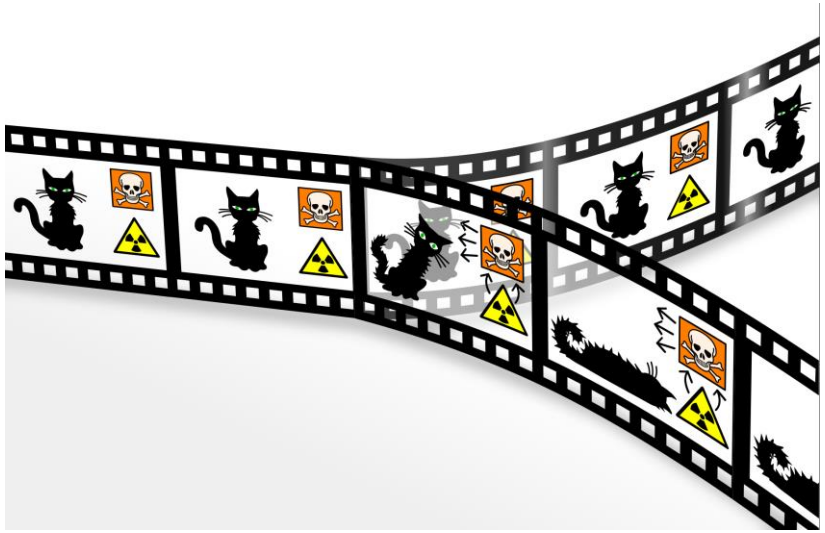


Image Christian Schirm

NIST PQC standardization process

In December 2016 NIST invited submissions for public-key cryptographic algorithms that would resist quantum computer based attacks

Now 18 months after the start of the second round of the standardization process, NIST announced in July the third round candidates

- Public-Key Encryption – McEliece, CRYSTALS-KYBER, NTRU, SABER
- Digital Signatures – CRYSTALS-DILITHIUM, FALCON, Rainbow

The following eight alternative candidate algorithms will advance to the third round

- Public-Key Encryption – BIKE, FrodoKEM, HQC, NTRU Prime, SIKE
- Digital Signatures – GeMSS, Picnic, SPHINCS+

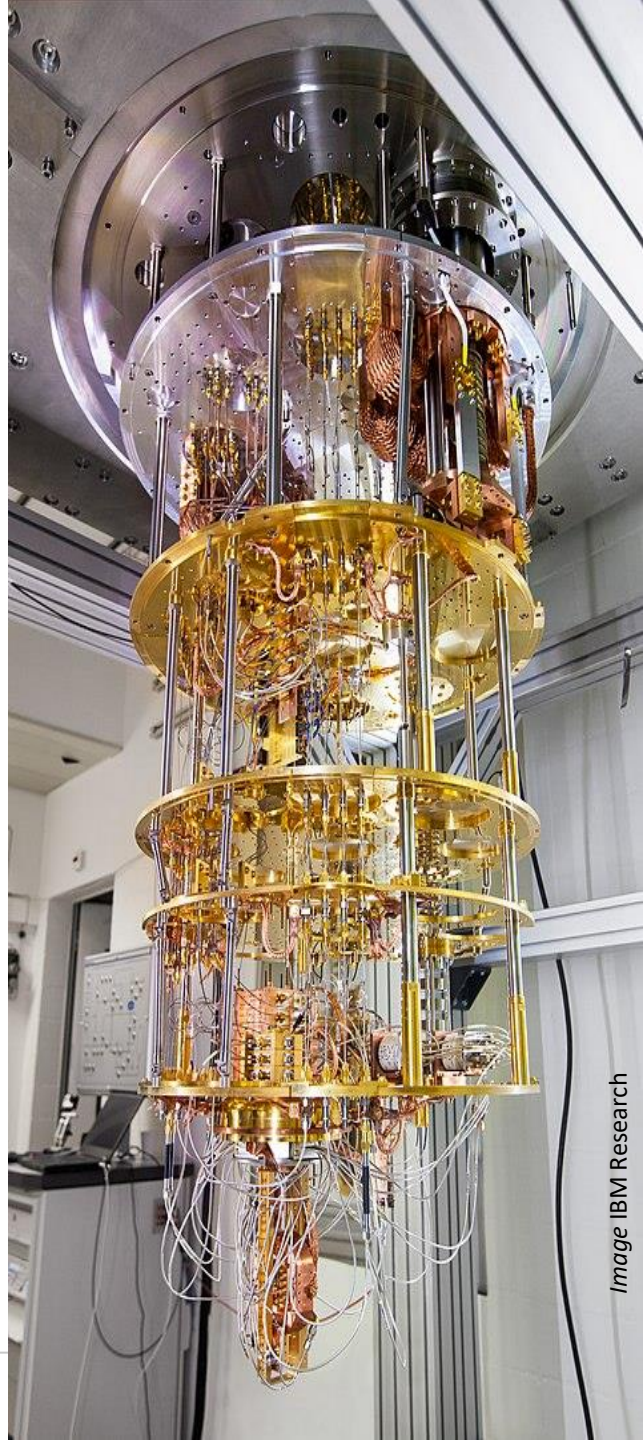


Image IBM Research

Example – quantum problem

1994, Peter Shor developed a quantum algorithm for factoring integers that had the potential to break the security of the widely used RSA method of asymmetric public key encryption

If feasible, a quantum computer would post a risk to the methods used to secure most communications systems such as the public key exchange use to secure web sites

- If solving RSA with a 512 bit key takes say 3 months to solve, then changing to a 1024 bit key we would expect the problem to take longer than the age of the universe

This very great computational effort required by all known classical factorization techniques underlies the security of the RSA method.

The amount of time a classical computer takes grows exponentially with number of bits but with a quantum computer it grows only linearly

- Doubling the key length would simply double the time, in the example from 3 to just 6 months!

Research into the feasibility of quantum computers is a matter of considerable interest

ENTELEC conference & expo

Image: Paul Lowry

Thank you