UTC TELECOM & TECHNOLOGY 2015

2050: CREATING THE MID-21ST CENTURY UTILITY

Security Challenges In Narrowband SCADA Radio Networks

John Yaldwyn, CTO, 4RF

4RF

SCADA – supervision control and data acquisition definition

SCADA is a transformative process, connecting the real world with a digital counterpart

MEASURE

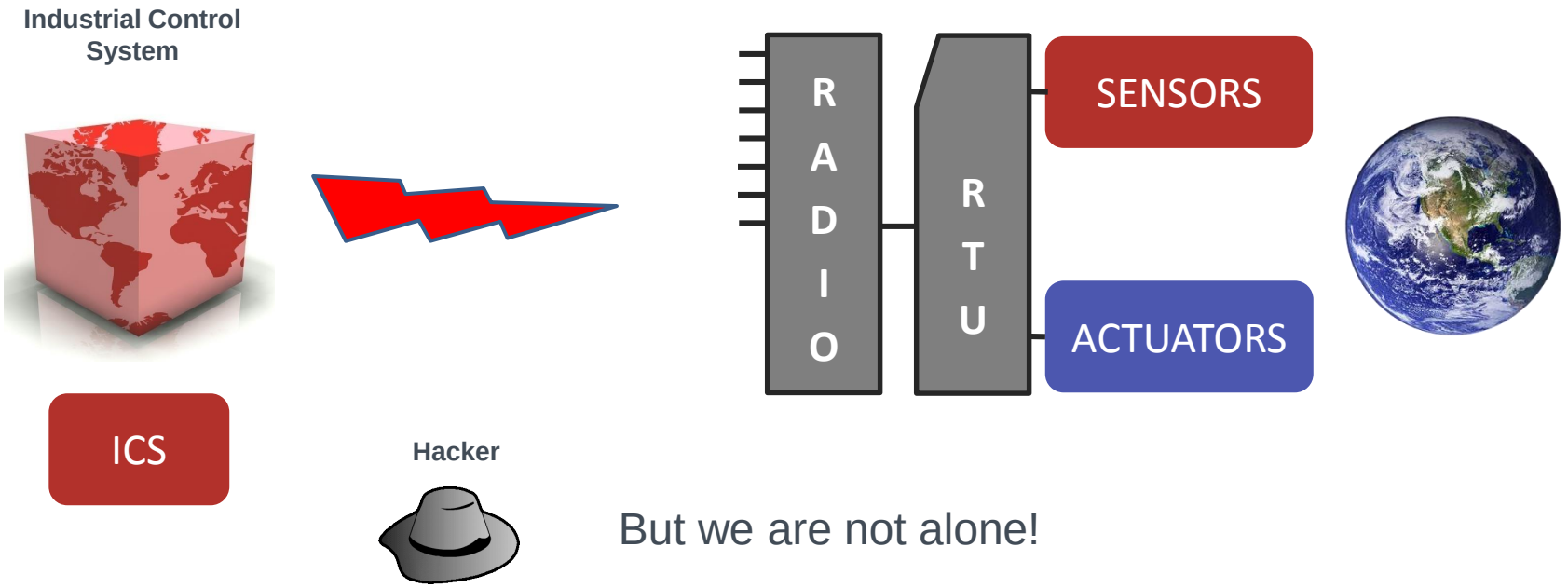
CONTROL

CYBER WORLD

REAL WORLD

SCADA – supervision control and data acquisition

Connection between field area network devices and utility industrial control system (ICS) is commonly over a private wireless network using radio or cellular backhaul



But we are not alone!

21st Century SCADA radio

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

Dedicated system are highly resilient compared with shared public solutions [1]

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

Licensed narrowband options

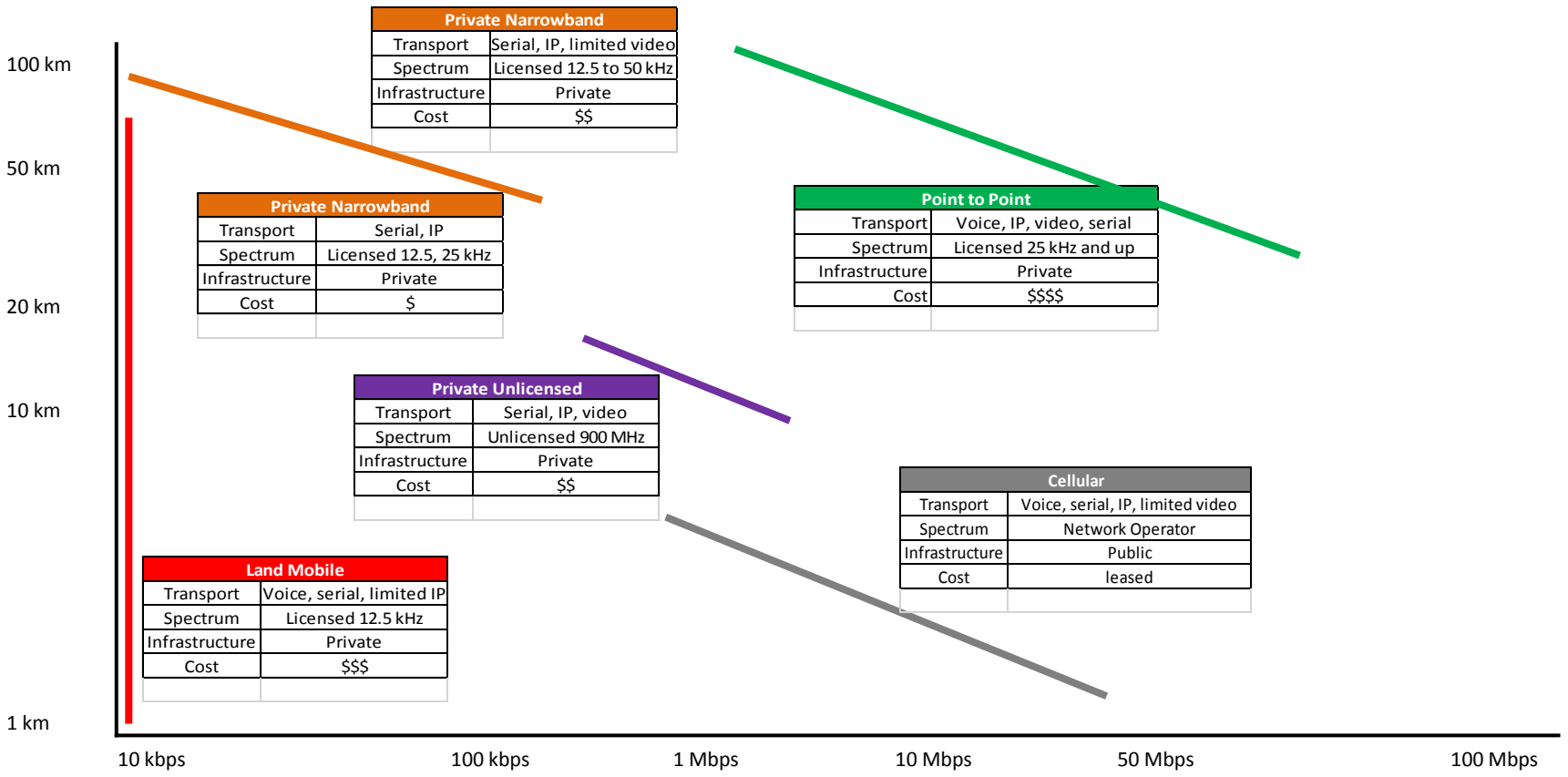
- 220, 450, and 900 MHz FCC Part 90, Part 24, and Part 101 (including MAS)

SCADA radio much faster than systems based on land mobile radio standards [2]




Wireless technology options

Narrowband → Broadband



Over The Air Speed

Real world drivers

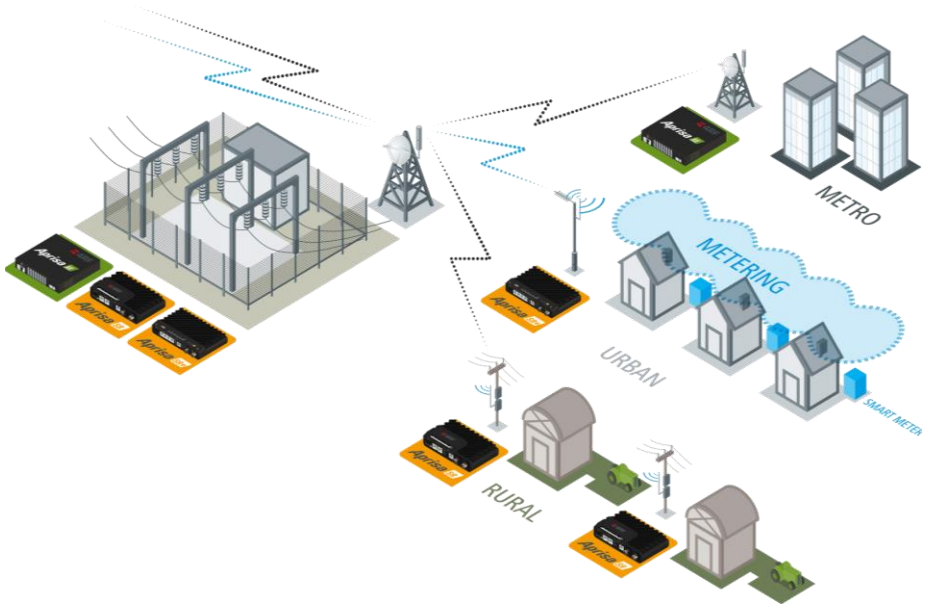
Private narrowband radio is a key technology for utility SCADA addressing the needs of reliability, redundancy, and resilience

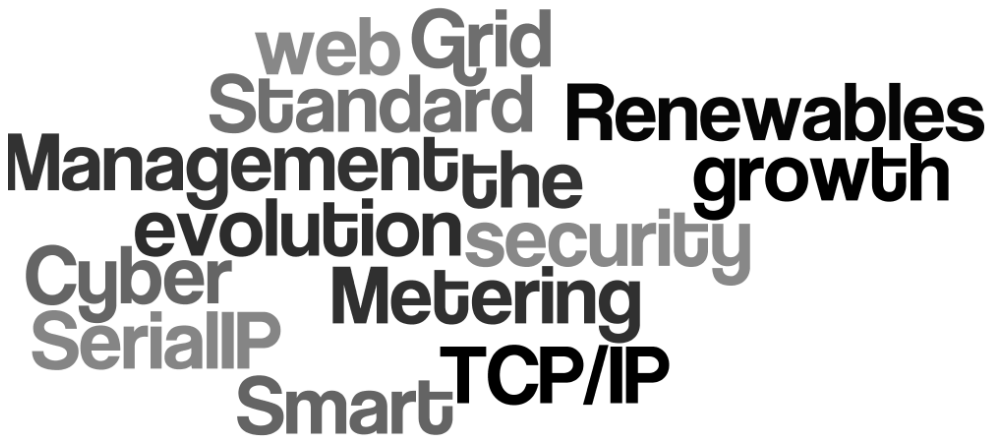
IP SCADA products bring new **protocol, security, and management** needs and drive expectations for radio system capacity requirements [3]

- Vendors are responding with new high speed designs up to 200 kbps

Using IP is not the same as ‘the Internet’ but they share the same protocols

- Need for a **careful security approach**





Security – typical ICS network architecture

Use of IP provides well standardized interface hence well defined attack surface [3]

ICS integrity critical

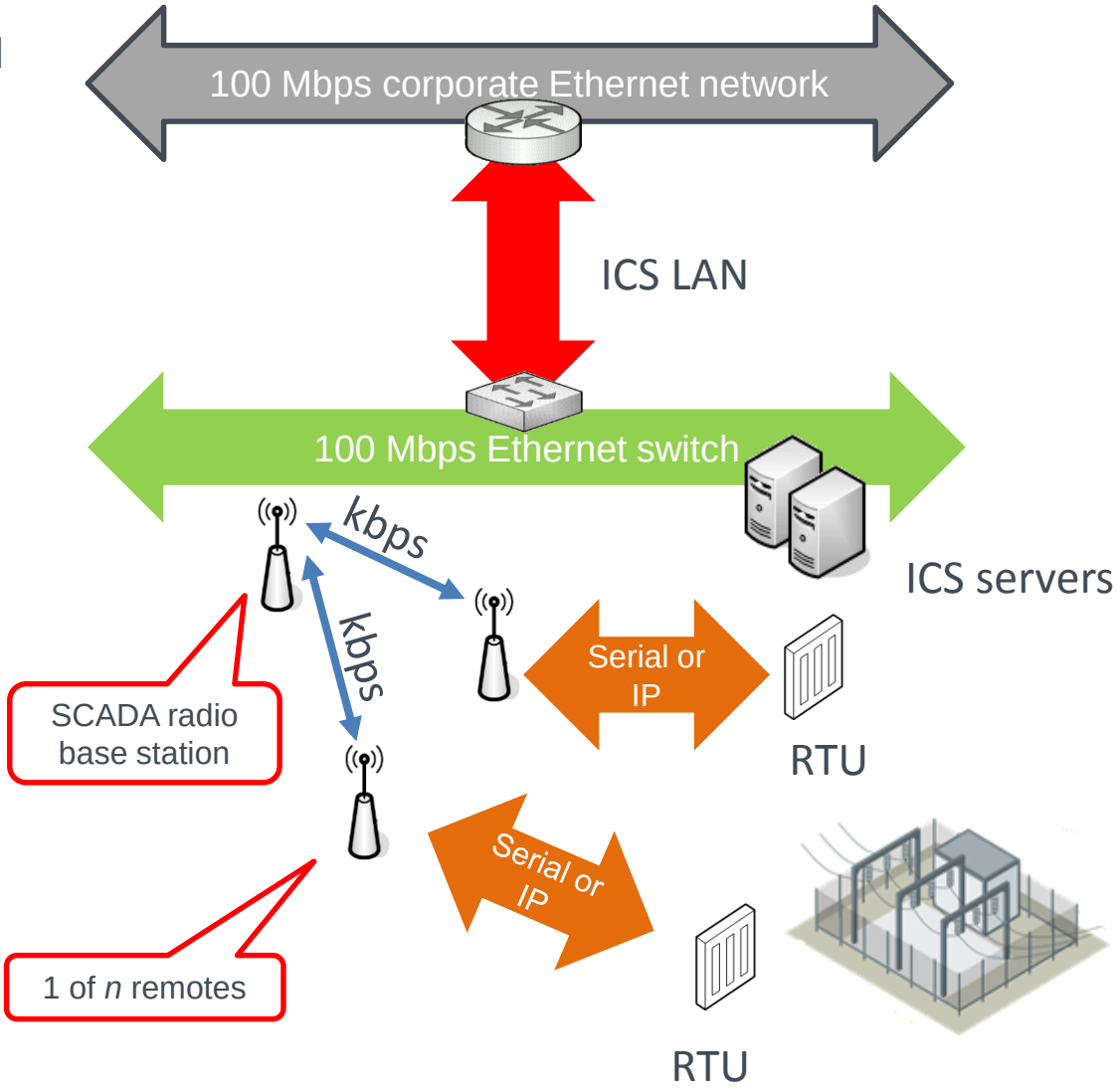
- The **security of all interfaces** must be considered [4]

Capacity considerations

- ICS LAN fast while radio links slow 10 to 240 kbps

System design is important

- Filtering rules [10, 11]
- Routing tables
- VLAN arrangements [5]
- QoS measures



Security should be designed in from the start

A comprehensive and in-depth approach to cyber security from the start is the best way to protect a network

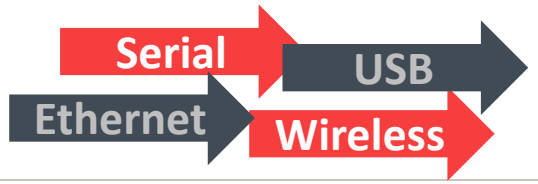
Must take into account key concerns

- **Security fundamentals** of integrity, availability, confidentiality and non-repudiation
- Communications and control systems are subjected to **attack** from many sources, internal and external, malicious and accidental (disable unused features)
- Types of **traffic and interface** ports, management and data that could be compromised – disable insecure protocols
- Security **standards and recommendations**, NERC CIP, NIST, FIPS, IETF, etc

Image: Vincent Diamante

360° Security

Secure the **perimeter** around the environment of the SCADA product, all external ports must be secured – traffic and management



Security – confidentiality and authentication

A secure network must be designed around maintaining **confidentiality** and **authenticating** devices, users, and messages

Encryption is used to reduce information leakage as far as possible

- Today the robust cryptographic **AES algorithm** is used [FIPS 197]
- Industry best practice is regular key change (over the air)

Network authentication of devices and messages

- Prevents replay and man-in-the-middle attacks
- Implemented using AES combined with the NIST specified **CBC MAC** method of authentication [NIST report SP 800-38C 2004 and RFC 3610]

Management authentication of users

- Username / password with access control lists
- Move to remote user authentication with **RADIUS**
- Audit user activity

Security – SNMP management

SNMP is a unified, open network management protocol, supported by many vendors

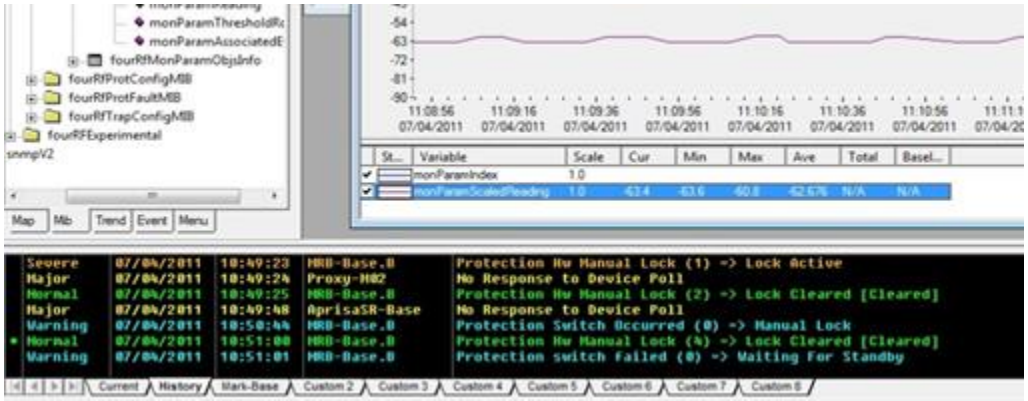
Industry converging on SNMP and away from proprietary applications

Authorisation levels verify that the user sending command is authorized to access the information but must use SNMPv3 as this version has security extensions [14]

- Allow only AES and SHA, disable DES and MD5 as these are no longer secure

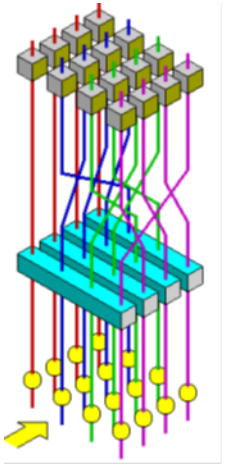
Built-in credential change mechanism, use this regularly over secure IP circuit

- Keys generated from USM user passphrases [RFC 3414]



Ethernet Management Protocols Security

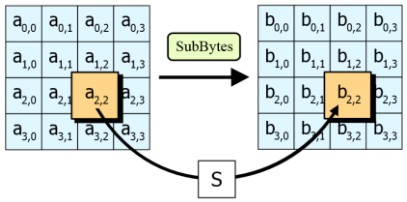
Over-the-air symmetric message encryption



Encryption is used to **reduce information leakage**

Robust cryptographic algorithm approach important, today this is **AES** [6]

- FIPS 140-2 Level 1 (algorithm) Level 2 (physical considerations) [13]
- Key is symmetric, same key used to decrypt as used to encrypt
- AES block size is 128 bits with a **key lengths of** 128, 192, or 256 bits



Security based on algorithm design and **shared secret key**

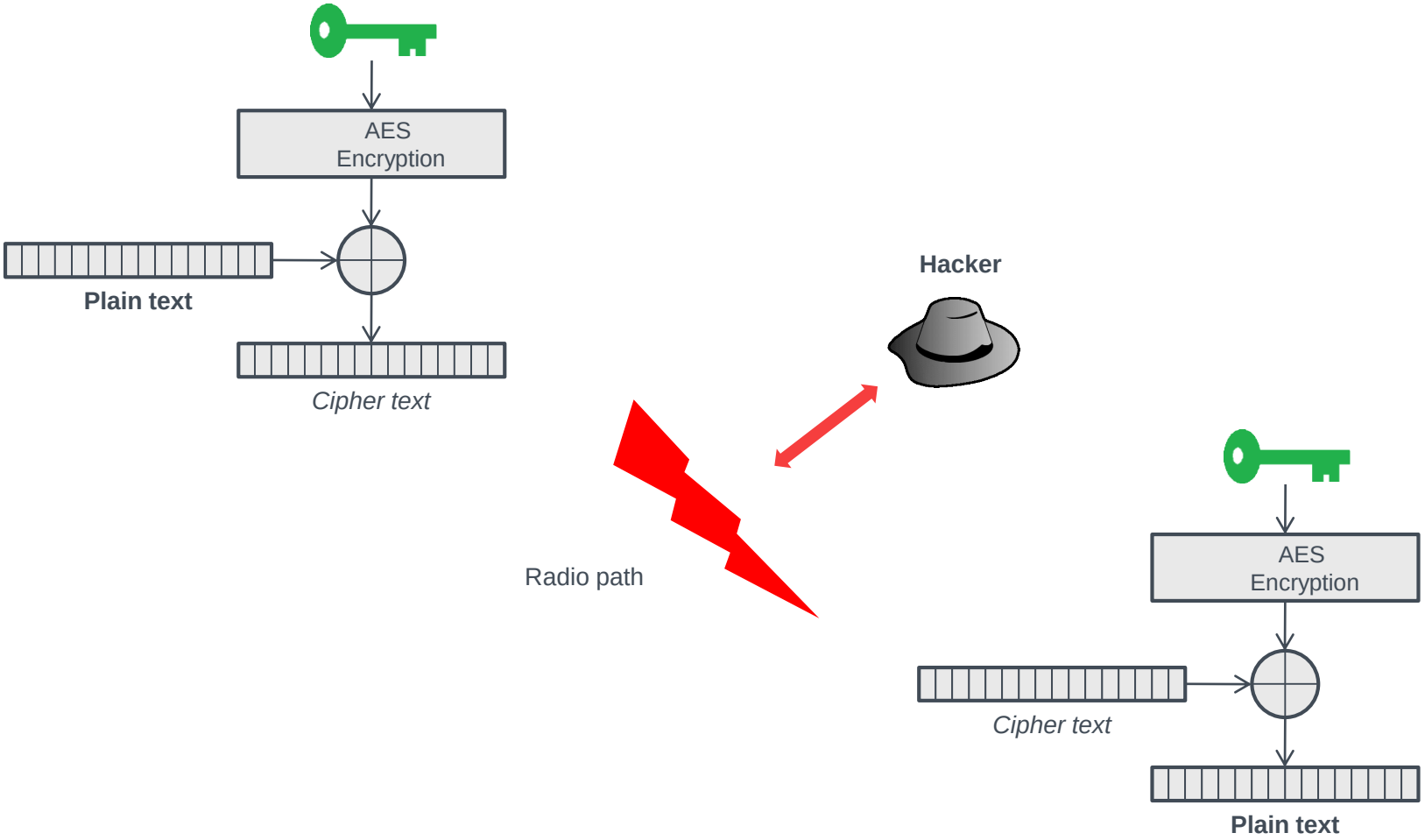
- Algorithm is public so key must be secret

Why change the key?

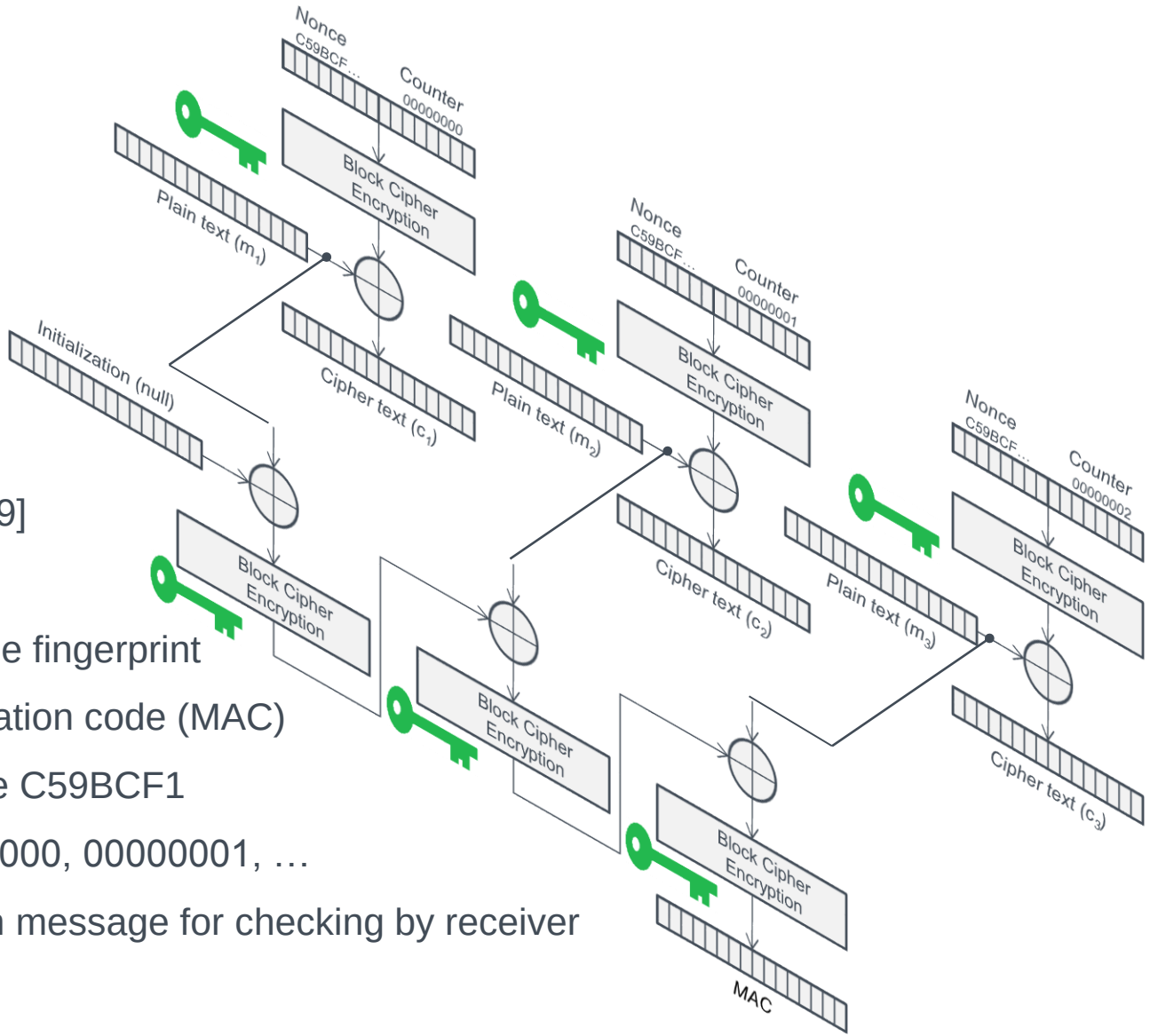
Regularly changing key increases security and guards against compromise

- Need a means to distribute new keys

Over-the-air message encryption



Over-the-air message authentication – CBC MAC



CBC MAC method [8, 9]

Block cipher = AES

Create unique message fingerprint

- Message authentication code (MAC)

Randomize with Nonce C59BCF1

- and Counter 00000000, 00000001, …

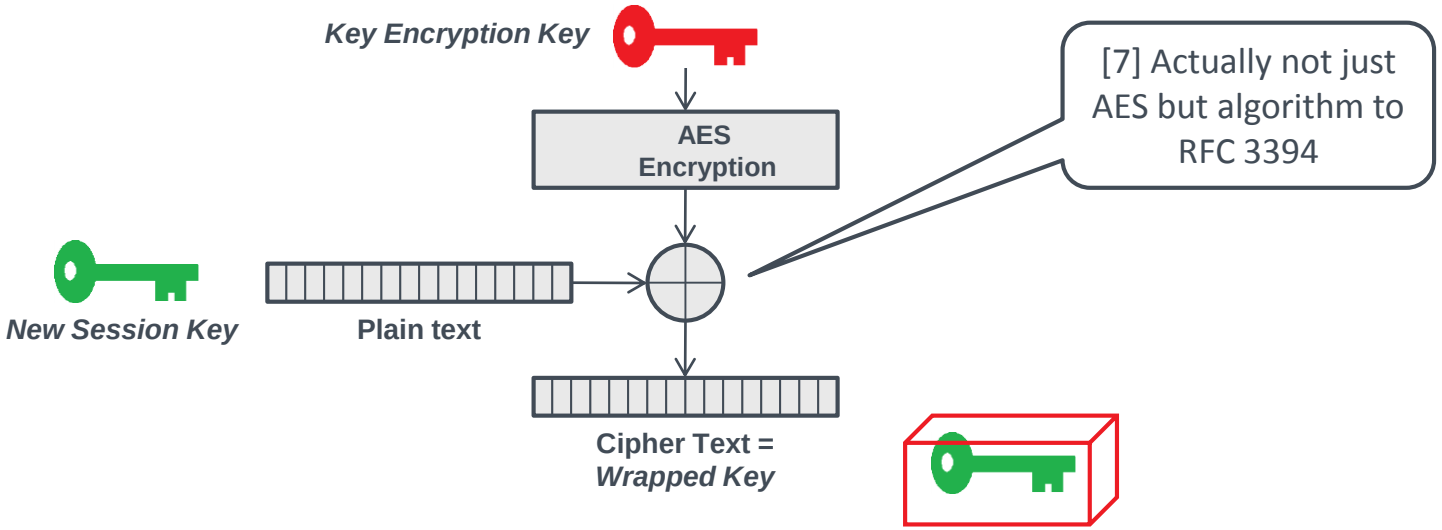
Send unique MAC with message for checking by receiver

Over-the-Air Rekeying – NIST Key Wrap

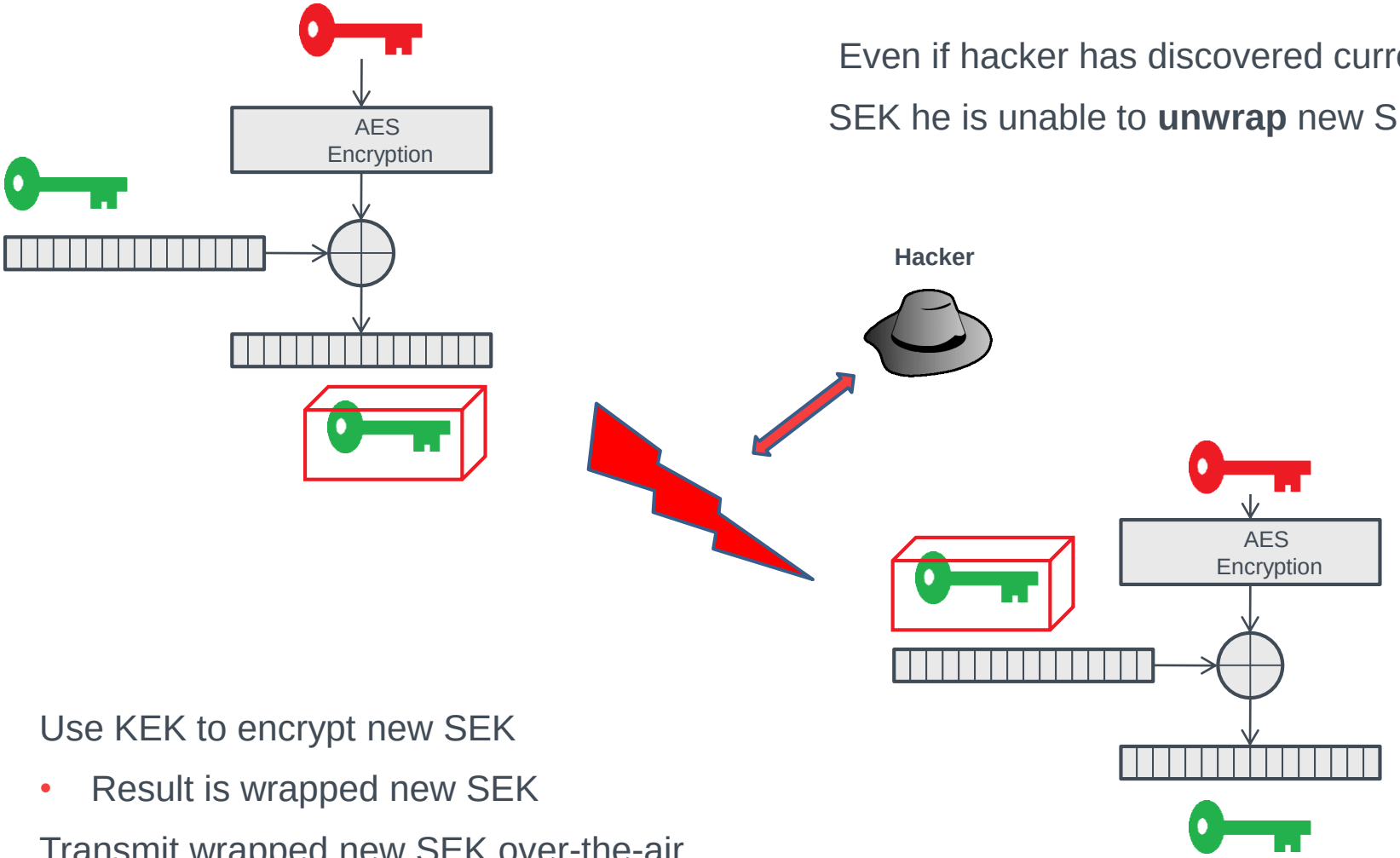
Key Wrap mechanism supports the secure distribution of a session encryption key (SEK) by encrypting with a pre-stored encryption key (KEK) [7]

- SEK used for **normal traffic transmission**, changed over-the-air
- KEK used for **encrypting keys**, manually loaded into terminals at deployment

The input to the key wrap process is the KEK and the new SEK (optionally with other data) treated as the plaintext to be wrapped



OTAR operation using Key Wrap



Even if hacker has discovered current SEK he is unable to **unwrap** new SEK

Use KEK to encrypt new SEK

- Result is wrapped new SEK

Transmit wrapped new SEK over-the-air

Unwrap new SEK using previously loaded KEK

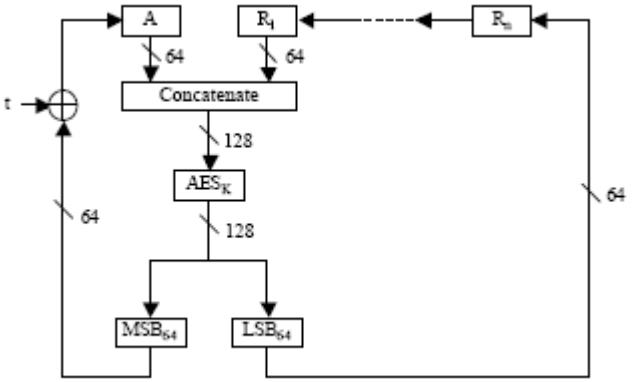
Security key management summary

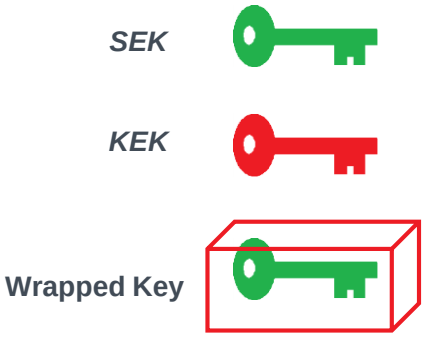
Changing encryption keys at **regular intervals** significantly improves the security of the network

The NIST Key Wrap method provides the ability to **change the encryption keys remotely** throughout the network

Need to **carefully maintain** shared secret keys

- Change SEK daily/monthly/quarterly as desired
- Change KEK when crypto officer changes or in any circumstances that could give rise to compromise i.e. NERC defined cyber incident [12]





GUI security

Most modern SCADA devices include an embedded **web server** to provide convenient configuration by installers and end users

Authorisation levels **limit end user** accessible parameters

- Limiting the number of personnel who can change functional settings reduces the potential of **inadvertent change or malicious tampering**

Authentication with username and password ensures that the end user must be **approved** by the system administrator before gaining access to the radio

- Can be done with **locally stored** credentials
- Most popularly done with **centralized authorization** server using RADIUS method

Session cookies should expire when the end user's browser is closed

Automatic logout in the event of a user failing to end their management session

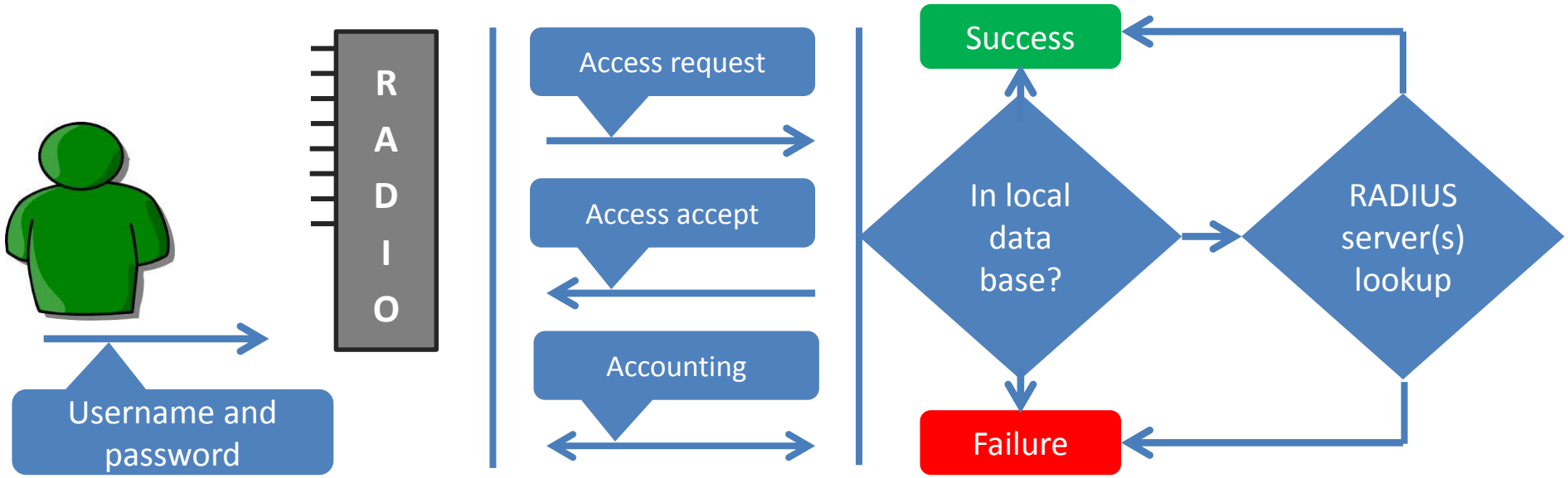
Also need to secure browser to web server communications to **prevent hacker observing** username and password credentials

RADIUS authentication, authorization, and accounting

Username/password required, these can be stored locally or in corporate cloud or both

Methods include RADIUS [RFC 2865, and RFC 5080]

- Local database often **retained** to allow access if corporate server not available
- **Audit** functions via Accounting Start/Updates/Stop records [RFC 2866]



Browser to web server security

Need to **secure browser to web** server communications

HTTPS secures normal web HTTP over a encrypted link implemented with TLS

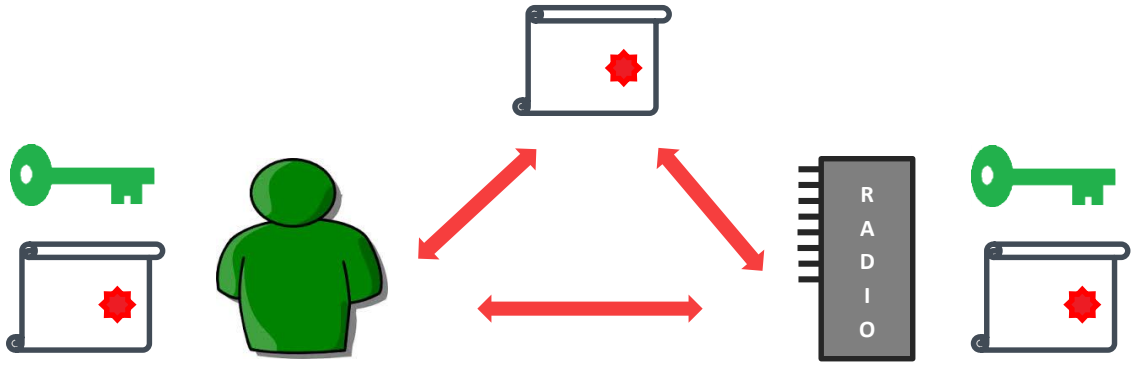
Two step process

- Establish trust between browser and server to facilitate exchange of session key
- Use session key as a shared secret key to encrypt [15] communications

Trust process usually based on certificate supporting a public key infrastructure

- Historically based on RSA public key – difficult factorization of large integers
- Industry migrating to ECC [16] – difficult solution to elliptic curve discrete logarithm

Certificates installed in web server and in browser, verified via a central known root



Browser to web server security – elliptic curve crypto (ECC)

NIST deadline for 1024 to 2048 bit RSA certificates was end of 2013

As RSA keys get longer the CPU load increases, important for embedded device servers

ECC offers more security for shorter key size, ECC 256 similar difficulty to 3072 bit RSA

- ECC 256 said to be 10,000 times harder to ‘crack’ than 2048 RSA

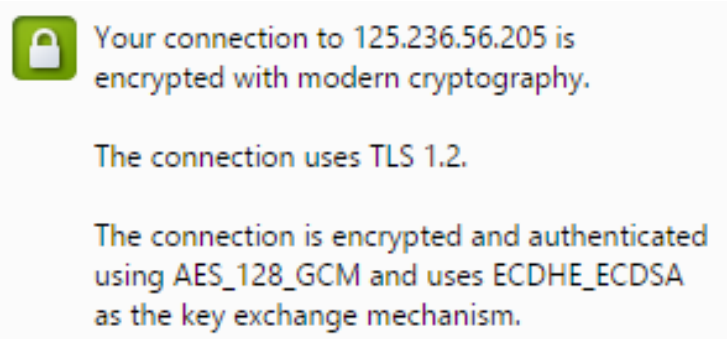
PKI certificate and ECC used to exchange session key for encryption

NIST recommends AES in GC mode (RFC 5288 for TLS) based on NSA Suite B

- Key aspect of Suite B is use of ECC technology

NIST recommends a 256 bit ECC or 3072 bit RSA key for 128 bit AES key transfer

Google’s Chrome considers TLS 1.2 + AES 128 GCM ‘modern cryptography’



How does RSA / ECC work?

The security of PKI systems is based on difficult solutions to mathematical problems, the difficulty forming a one-way function often called a trapdoor

RSA is based on difficult factorization of large integers

- RSA biprime number n has prime numbers p and q such that $n = p \times q$
- Find two primes p and q given only n i.e. factoring n = 91 gives p = 7 and q = 13
- Easy to multiply but harder to factor, increase integer to hundreds of digits …

ECC security based on the ease of a point multiplication and the difficulty to compute the multiplicand given the original and product point – a one way function

- Elliptic curves defined as $y^2 = x^2 + ax + b$
- Restricting the number field to a finite number of points Fp
- Generates a finite group of points (y pairs for each x value)
- Can add a point to itself $nP = P + ... + P$ for integer n and a point P = (x, y)
- But can't find n from $Q = nP$ given known values of Q and P

Image: Wikimedia

Apologies to mathematics for this gross simplification!

Secure access summary

Disable non-secure management protocols

- Telnet
- Old SNMPv1 and v2 versions
- Insecure proprietary methods

Consideration of physical means to circumvent protections – FIPS 140-1 L2 tamper evident

Modern security protocols

- SNMP v3
- Encryption / authentication / OTAR
- HTTPS TLS ECC

Restriction on management access

- By port
- By authentication
- Access control, audit, and RADIUS

Restrict
reassure
record

References

1. Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, Order, EB Docket No. 06-119, WC Docket No. 06-63
2. TETRA+ Critical Communications Association 'TETRA versus DMR', October 2012
3. Kwok-Hong Mak, 'Migrating electrical power network SCADA systems to TCP/IP and Ethernet networking', Power Engineering Journal Volume 16, Issue 6, December 2002
4. ABB Switzerland Ltd 'SCADA over IP-based LAN-WAN connections', March 2011
5. NSA Systems & Network Analysis Centre 'Securing Supervisory Control and Data Acquisition (SCADA) and Control Systems (CS)'
6. NIST FIPS PUB 197 Advanced Encryption Standard (AES)
7. RFC 3394 Advanced Encryption Standard (AES) Key Wrap Algorithm
8. NIST publication SP 800-38C 'Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality'
9. RFC3610 Counter with CBC-MAC (CCM)
10. Muralidaran Gangadharan, Kai Hwang, 'Intranet Security with Micro-Firewalls and Mobile Agents for Proactive Intrusion Response', Proceedings of the 2001 International Conference on Computer Networks and Mobile Computing, p.325, October 16-19 2001
11. CPNI Firewall Deployment for SCADA and Process Control Networks Good Practice Guide'
12. NERC CIP-008 Incident Reporting and Response Planning
13. FIPS 140-2: Security Requirements for Cryptographic Modules
14. RFC 3410 'Introduction and Applicability Statements for Internet Standard Management Framework'
15. NSA Suite B and NIST Special Publication 800-56A, NIST SP 800-38D, and RFC4492
16. NSA 'The Case for Elliptic Curve Cryptography'
17. NERC CIP Version 5 Reliability Standards