

SCADA Communications Security

**Authentication, Encryption,
Integration**

Philip Aubin


**Director of Technology, Control Microsystems Inc.
DNP3 User Group Technical Committee member**

SCADA Communications Security Methodology

- SCADA communications security standards attempt to protect:
 - Comms participants and Channels (Spoofing)
 - A 3rd party pretending to be one of the communication devices
 - Encryption attacks
 - Attempts to “crack the secret code” that protects data content
 - Signature attacks
 - Attempts to “crack the secret code” that proves data hasn’t been changed

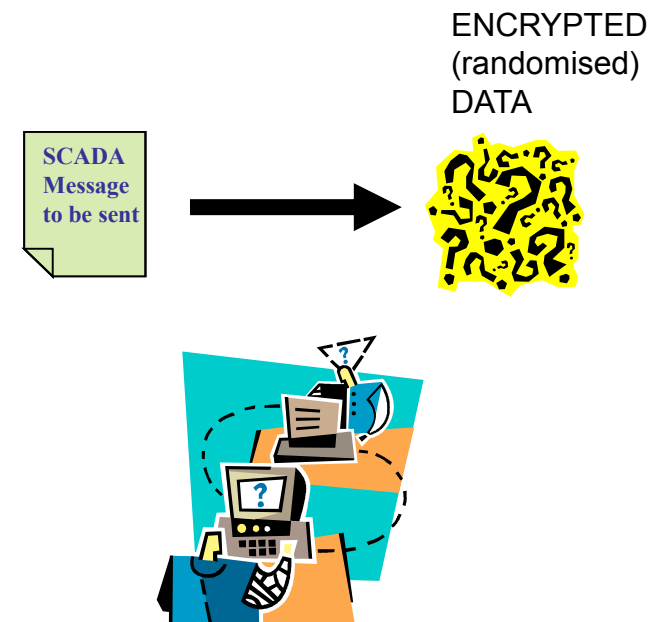


Security Methodology

- SCADA communications security standards attempt to protect:
 - Protocol attacks
 - injection of unintended messages, e.g. misleading data or unintended controls
 - Replay of messages 
 - 3rd party capturing old data and sending it again
 - replay particularly dangerous for controls
 - Data tampering 
 - 3rd party modifying the contents of messages
 - Eavesdropping (where encryption is used) 
 - 3rd party attempting to glean information from the data to their commercial or strategic advantage

SCADA Security

- Here are two common security mechanisms for SCADA systems:
 - Encryption – Hide the data content
 - Authentication – challenge the sender of data to prove identity
 - Both can be used concurrently



SCADA Security Standards

Two open standards for SCADA communications are available in the market now:

- AGA12 suite
 - also known as IEEE 1711 standard (part of substation communication security)
- IEC62351 suite
 - Secure Authentication for DNP3 released in 2007 is based on this

Modern Communications & Security Alternatives?

- Communication to remote devices using TCP/IP is becoming common
 - Is there a need for SCADA security independent of available IT security?
 - YES!
 - TCP/IP is not uniformly distributed to all end points in Wide area communication systems
 - Low cost & low processing power field devices typically don't provide for high overhead security e.g. TLS/SSL
 - There's a wide variety of physical media: dial-up, serial, radio, installed base of 1200bps line modems
 - Where TCP/IP is in use, SCADA standards now asking for both TLS and protocol security layers

Security Keys

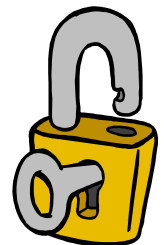
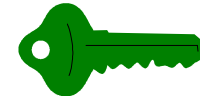
How the technology works ... (briefly)

- Many systems using Security Keys now dynamically change the keys used for signatures and encryption
 - (called key rotation)
 - E.g. 802.11b wireless Ethernet WPA security standard uses rotating keys and has much better security than the original WEP fixed key wireless standard
 - Dynamic key rotation is itself encrypted so it can't be learnt by eavesdropping
 - Requires fixed 'secrets' (update keys) at both ends for deriving the dynamic (session) keys
 - Signature & Encryption algorithms uses the dynamic key



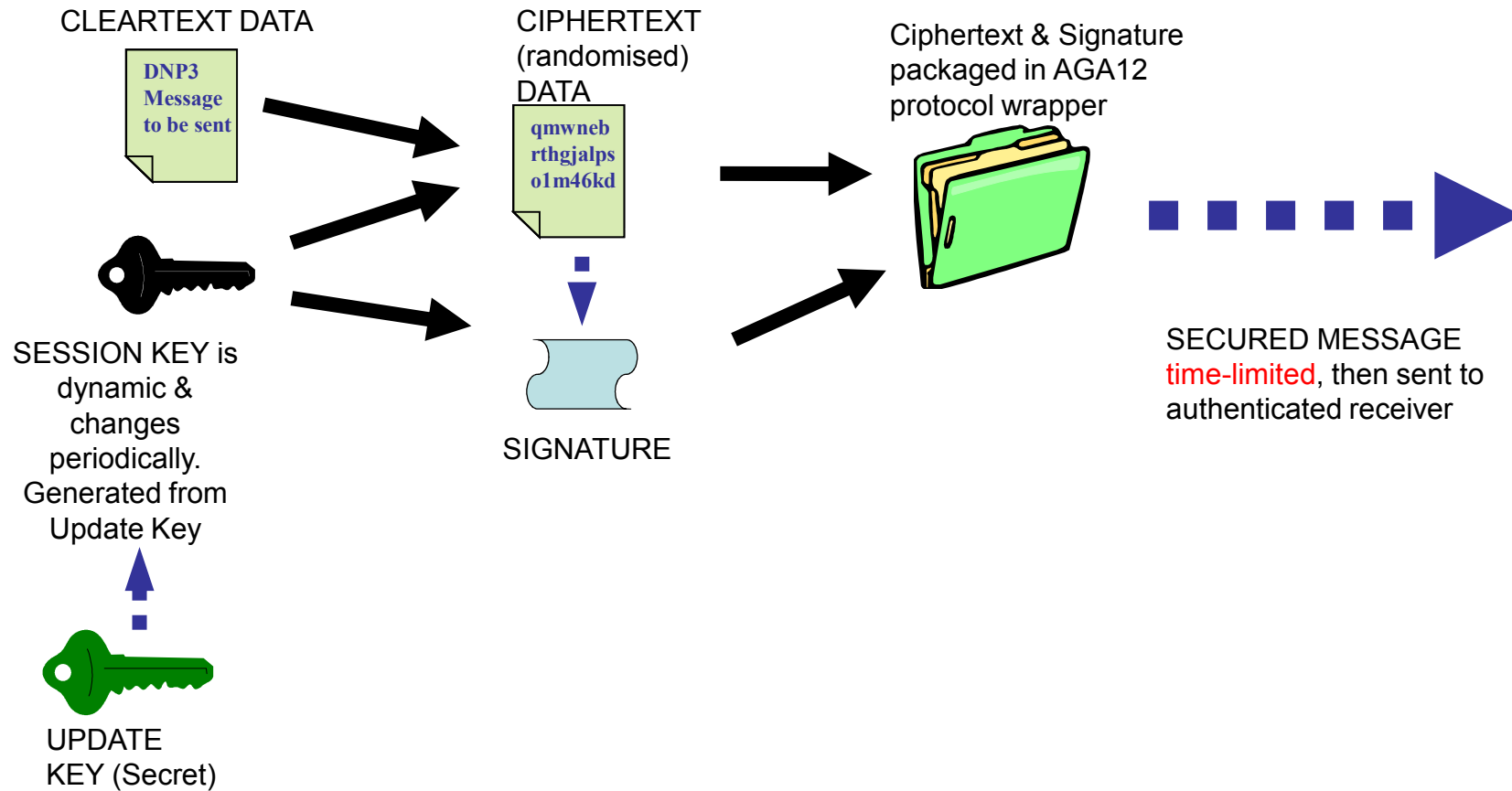
AGA12 / IEEE 1711 Standard

- Philosophy based on “ENCRYPTION”
 - Confidentiality: ‘Hide what you are saying’
 - Incorporates security “Key” technology
 - Based on open cryptography standards such as AES encryption
 - Validates ‘connection’ between users using secret keys
- Protects all messages through authenticating partner device and “randomizing” transactions between them
 - Signs and encrypts all messages
- Defines a device called an “SCM”
 - SCADA Cryptographic Module



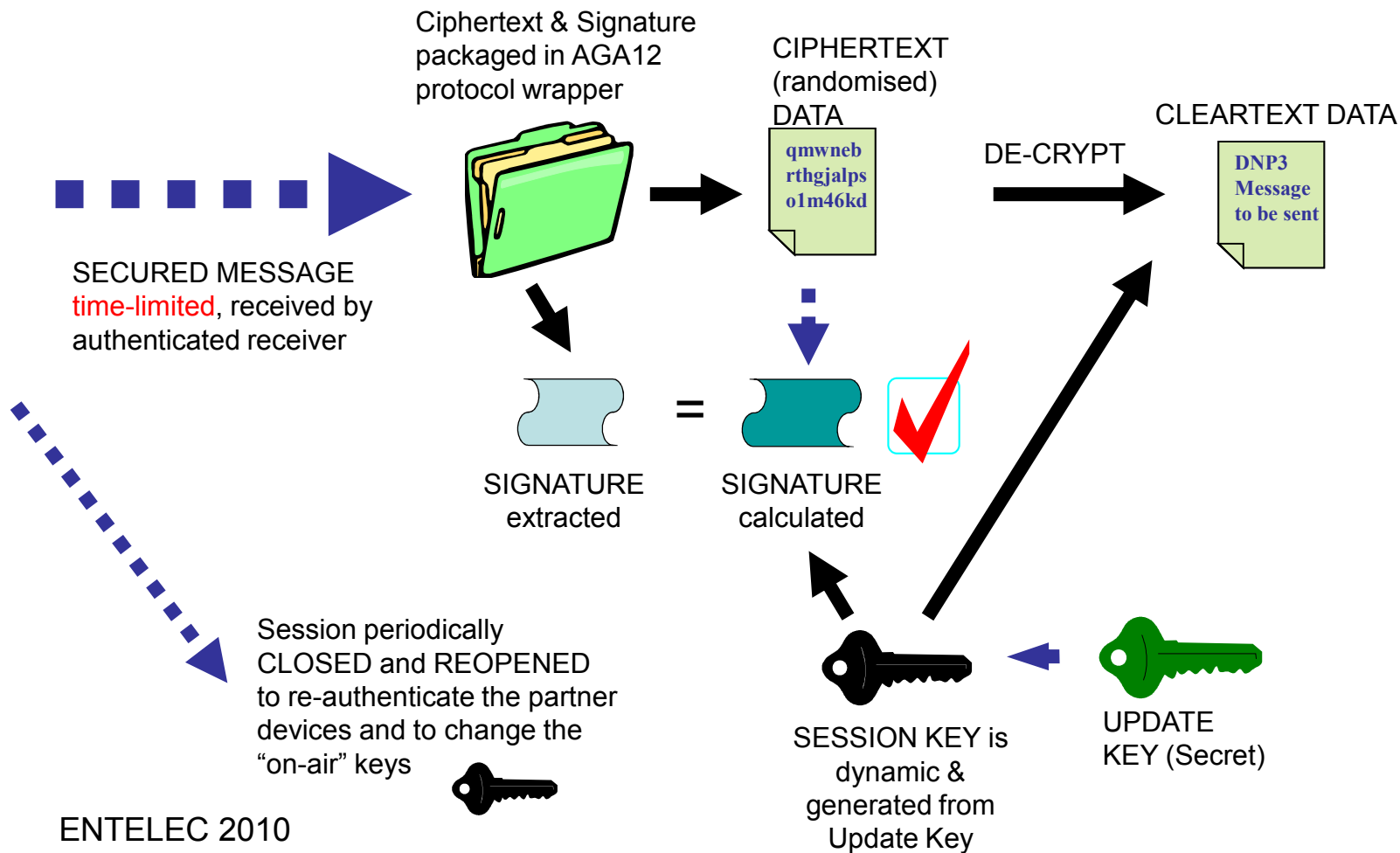
How AGA12 Works

Sending a message after the session is open



How AGA12 Works

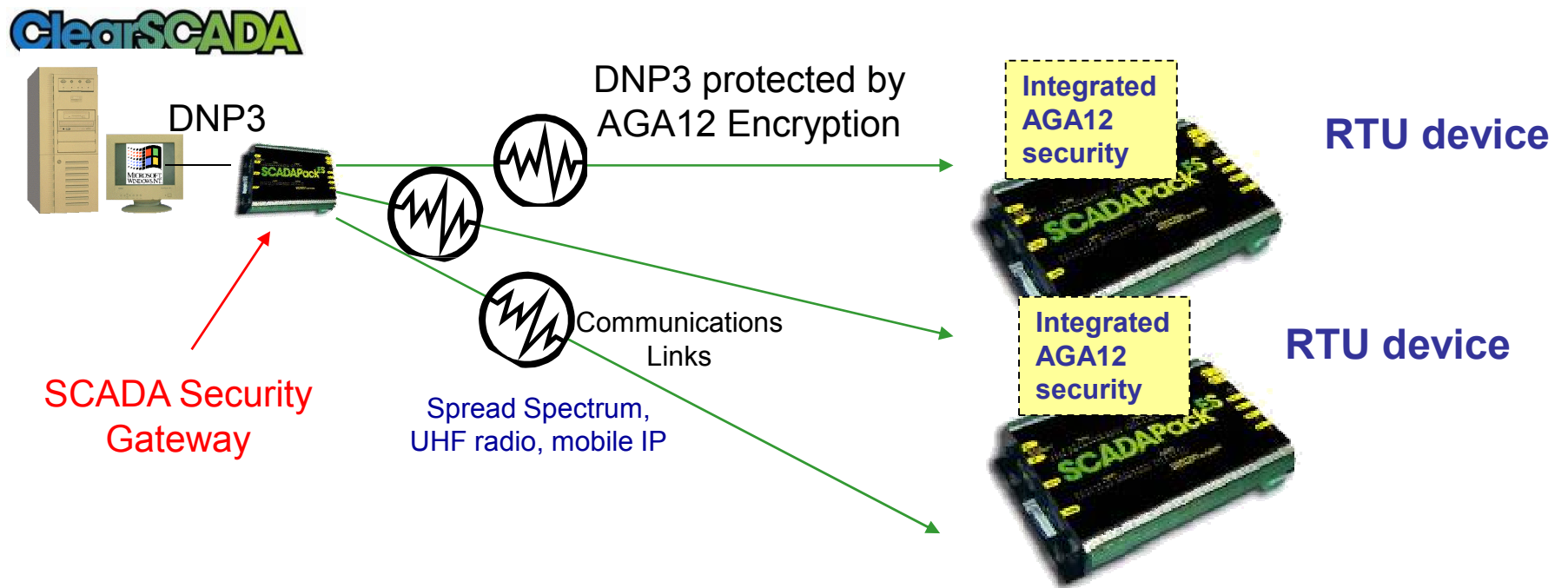
Receiving a message after the session is open



Case Study – AGA12 encryption for DNP3

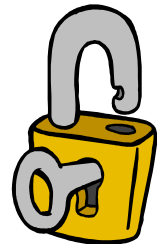
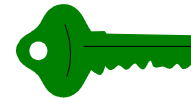
- Control Microsystems recently supplied SCADA technology products to a project requiring “integrated SCADA confidentiality”
- The application is in the water industry in USA for bulk water system SCADA and automated meter reading (AMR), with demand billing capabilities
- The implementation of data encryption was paramount in guaranteeing the security of billing data for both the purchaser and the seller and ensuring system security and integrity
- The project facilities encompass >40,000 sq. miles of territory and because of varying terrain, uses a mix of: spread spectrum radios, UHF licensed-band radios, mobile IP technologies
- The system comprises 450 SCADAPack RTU’s using DNP3 secured by AGA12 authentication and encryption
- The implementation includes a ClearSCADA master station system

Integrated AGA12 SCADA Security



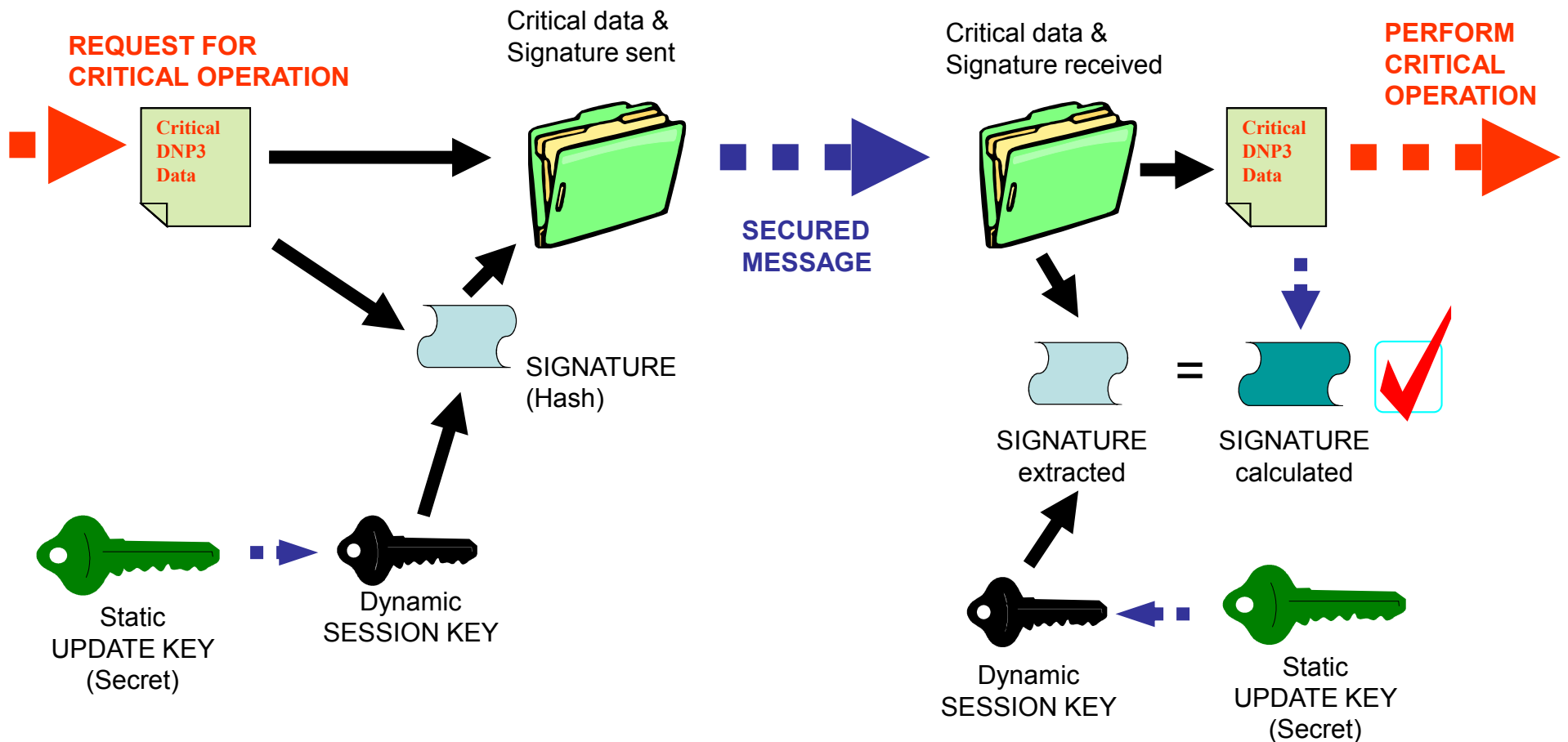
DNP3 Secure Authentication

- Modelled from IEC62315-5 Authentication Standard
- Philosophy based on “AUTHENTICATION” & “CHALLENGE”
 - Prove ‘you are who you say you are’ using Challenges
 - Incorporates security “Key” technology
- Protects actions deemed “critical”
 - uses protocol Application Layer authentication ‘challenge’
 - E.g. Controls, Configuration change (minimum requirements)
 - A “Signature” prevents tampering - but data is not “Encrypted”
 - Bandwidth and processing impact only minor as it applies to protected messages only
- Protocol definitions for remote management of update keys
 - DNP3 security revisions just released (April 2010)
 - Requires a corporate security Authority separate from Master Station




DNP3 Secure Authentication

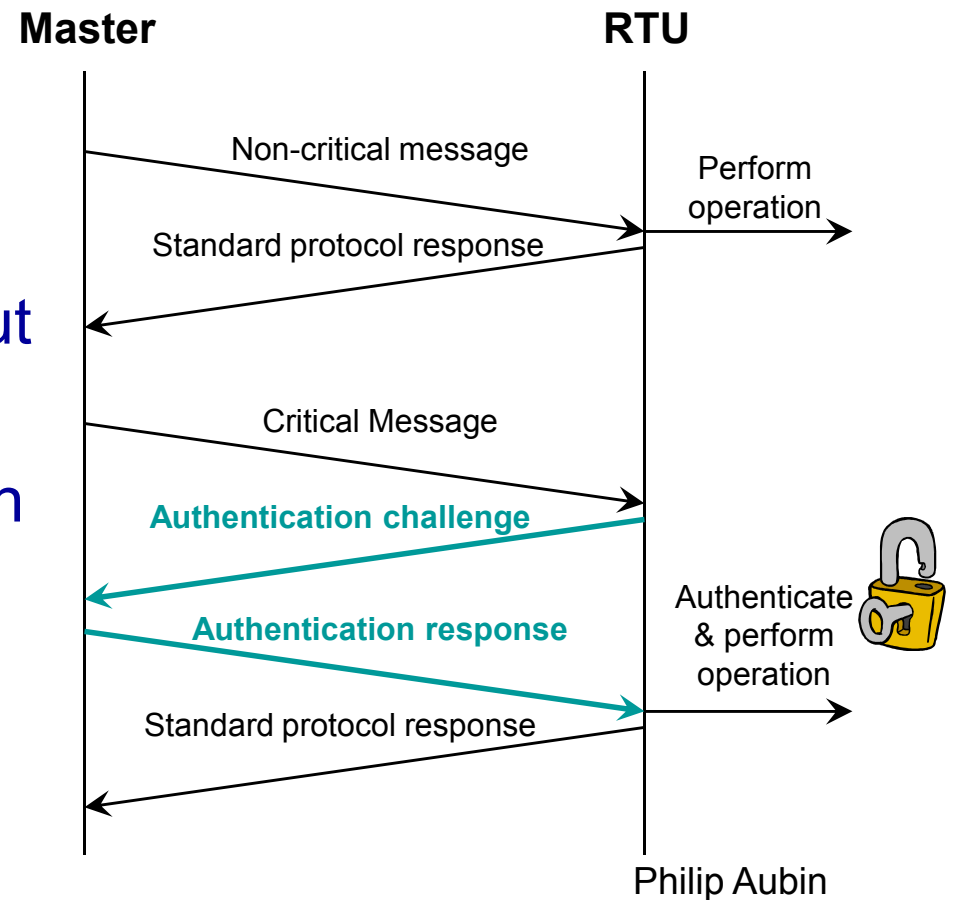
Protecting an operation with a Hash



DNP3

Authentication Challenge

- Non-critical messages operate as usual
- Critical messages are “Challenged”
- Operation is only carried out if Challenge ‘passes’
- Either a Master or RTU can issue a challenge
- Challenge & Response uses Session Key 



DNP3 Security Configuration

- Mandatory minimum security settings & interoperability
- Also provides some choice in security configuration

Security

Challenge data length (4 to 40) bytes

Session key length

Choose which function codes are critical. This determines which requests are sent using aggressive mode and which responses are challenged.

<input type="checkbox"/> Confirm	<input checked="" type="checkbox"/> Warm Restart	<input type="checkbox"/> Get File Information
<input type="checkbox"/> Read	<input type="checkbox"/> Initialise Data	<input checked="" type="checkbox"/> Authenticate File
<input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Initialise Application	<input type="checkbox"/> Abort File
<input checked="" type="checkbox"/> Select	<input checked="" type="checkbox"/> Start Application	<input checked="" type="checkbox"/> Activate Configuration
<input checked="" type="checkbox"/> Operate	<input checked="" type="checkbox"/> Stop Application	<input type="checkbox"/> Response
<input checked="" type="checkbox"/> Direct Operate	<input type="checkbox"/> Save Configuration	<input type="checkbox"/> Unsolicited Response
<input checked="" type="checkbox"/> Direct Operate - No Ack	<input checked="" type="checkbox"/> Enable Unsolicited	
<input type="checkbox"/> Immediate Freeze	<input checked="" type="checkbox"/> Disable Unsolicited	
<input type="checkbox"/> Immediate Freeze - No Ack	<input type="checkbox"/> Assign Class	
<input type="checkbox"/> Freeze-and-Clear	<input type="checkbox"/> Delay Measurement	
<input type="checkbox"/> Freeze-and-Clear - No Ack	<input checked="" type="checkbox"/> Record Current Time	
<input type="checkbox"/> Freeze-at-Time	<input type="checkbox"/> Open File	
<input type="checkbox"/> Freeze-at-Time - No Ack	<input type="checkbox"/> Close File	
<input checked="" type="checkbox"/> Cold Restart	<input type="checkbox"/> Delete File	

DNP3 Device Security

- Configuration for communicating with each Outstation:

The screenshot shows the 'Security' tab in the SCADAPack configuration interface. The 'Enabled' checkbox is checked. Under 'Algorithms', 'HMAC' is set to 'SHA-256 truncated to 16 octets (networked)' and 'Key Wrap' is set to 'AES-128'. Under 'Session Keys', 'Change Interval' is 15M and 'Change Count' is 1000. Under 'Aggressive Mode', 'Accept Requests' and 'Issue Requests' are both checked. 'Maximum Error Count' is set to 2. Under 'Alarm / Event Logging', 'Severity' is set to 'Alarm' and 'High', and 'Area Of Interest' is set to 'World'.

The dialog box is titled 'Set Update Key - DNP3.Outstation'. It contains a 'Key' field with the value '23456789ABCDEF0123456789ABCDEF0' and two buttons: 'OK' and 'Cancel'.

Practical Security

- Securing Master Station to Outstation Communications
 - Controls
 - Configuration changes
 - Firmware changes
 - Optionally encrypting data content
- Securing Outstation to Outstation Communications
 - authenticating Peer to Peer control coordination between devices
- Securing Configuration Application to Outstations
 - Controls
 - Configuration changes
 - Firmware changes
 - Optionally requiring operation behind SCADA firewall

Security Summary

- DNP3 Authentication and AGA12 Encryption ensure:
 - Confidence in who is at the other end of the communication link
 - Protected messages are original (unmodified), and not replayed
- Encryption (AGA12):
 - Protected data can't be eavesdropped (looks random) – preserves the confidentiality of the payload
- The cost of security:
 - “Remote Key Management” – an activity for users to manage
 - Straight forward for small systems now
 - New standards on the way for larger systems
 - Protocol overhead on protected messages, higher for encryption
 - Take care to choose the “right” security methodology to suit the criticality of the operation of your system and your SCADA data

PHILIP AUBIN

PAubin@controlmicrosystems.com

www.controlmicrosystems.com