AGA 12 Cryptography Can Reduce SCADA Cyber-Attack Risk At Low Cost

A Presentation To The
DOT PHMSA Conference
By
Chris Ziolkowski
Gas Technology Institute
February 7-8, 2007
New Orleans, Louisiana

gti

THE GAS TECHNOLOGY INSTITUTE (GTI) IS -

- 300 People
- Non-Profit Energy R&D Institute formed from IGT and GRI
- Perform $50,000,000 of contract research annually

Chris Ziolkowski

- With GTI Since 1982
- Electrical Engineer
- Currently R&D Manager, Sensors & Automation
- Has worked in standards and automation area with:
  - Dr. Bill Rush
  - John Kinast
  - Aakash Shah

For A System To Be At Risk, Three Factors Must Exist

- Vulnerability – Exploitable Weakness
- Threat Agent With
  - Motivation To Attack
  - Capability To Exploit Vulnerability
- Consequence - Significant Damage

gti

Pipelines & Other Facilities Are Prime Terrorist Target

- Targeting Theory Focus: Infrastructure
- Exploit Interdependencies
- Damage Economy, War Fighting
- Genetic Algorithms, Selective Annealing, and other sophisticated methods to choose targets

gti

Aerial Photo Of City C Site

Skilled Attackers Exist

- Hackers – Patience, Some Skill
- Insiders – Special Knowledge, Access
- Criminals – Can Buy Expertise, Access
- Terrorists – Have Significant Resources
- Governments – Resources, High Skill

gti

Cyber Attacks Can Do Damage

- Malevolent Code Can
  - Change Set Points, Safety Limits
  - Lie To System Host
- Open/Close Valves
- Turn Equipment On/Off
- Damage Turbines? (*Critical Question*)

Physical Attack Requires High-Skill Help

AGA 12 Is An Industry Recommended Practice

- Passed In March 2006
- "Cryptographic Protection Of SCADA Communications"
- Applies To Gas, Water, Electric & Oil
- An Open Standard
- Available For Free
- Supported By Manufacturers
- Being Field Tested

AGA 12 Protects Against Many Risks

- Real Attacks
- Liability And Negligence
- Government Legislation
- Insurance Premium Increases
- Loss Of Customer, Investor Confidence

AGA 12 Is Actually A Series Of Documents

- Part 1: Overall Recommendations - ***Passed***
- Part 2: Retrofit Technical Spec. - ***Ready***
- Part 3: Network/IP Technical Spec.
- Part 4: New (Embedded) Design
- Key Management
- Forensics

AGA 12 Is The General Document

- Part 1 Final Ballot Passed March 2006
- Policy Guidelines
  - Focus On “How To Develop”
  - Complements Checklist Policy Documents
- Problem Background
- Testing Program For Equipment

Part 2 Has Specific Goals

- Cryptographic Communication Protection
- Retrofit To Existing Systems
- Gas, Water, Electric & Oil
- Reasonable Cost
- Tolerable Message Delays
- Reliable Certification Methods
- Interoperability Among Manufacturers

gti

AGA 12 Protects SCADA Communication Privacy

> Technical Approach: Attackers can't read

Even Intercepted SCADA Commands Are Secure Until They Reach Their Destination

AGA 12-1 Is A Gas Industry Recommended Practice

- Part 1 Was Passed March 2006
- Part 2 Technically Complete
- Field Tests Started Last January
- Commercial Prototypes Available
- Evaluated By National Labs
- Work Now Stalled

AGA 12-2 Is A RETROFIT Solution

- **Strong** Industry Message: Retrofit FIRST
- BUT Difficult To Do
  - 150 Protocols
  - Radio, Phone, Microwave, Fiber, Leased Line
  - Many Different Speeds
- Easy To Install “Bump In The Cord”
- Two Manufacturers Now Supply Hardware For Under $600

It Is Time To Start Deploying AGA 12

- Commercial Products Available
- Provides Good Protection
- Low Prices
- Fast Enough For Gas And Electric

AGA 12 Would Benefit From A Forensic Upgrade

- Products Can Detect Attempted Attacks
- BUT, Products Do Not Notify Operators
- Should Add Notification For
  - Operators
  - Emergency Responders
- Ran Out Of Time And Funds Before These Forensic Capabilities Were Added
- This Capability Should Be Added

gti

And AGA 12 Needs A Certification Test

- The Standard Tells What The Products Must Do
- BUT, Purchaser Must Trust Manufacturer
- There Is No Objective Pass/Fail Third Party Conformance Test
- For Now, It Is “Buyer Beware”

Adopting AGA 12 Can Reduce SCADA Risks At Low Cost

- Now Gas Industry Standard
- Offered To Electric Industry
- Protects Against Many Risks
- Retrofits Many Systems
- Upgrades For Forensics And Certification Would Improve AGA 12 Usefullness

gti