Cryptographic Protection for Serial SCADA Communications

Andrew Wright

Critical Infrastructure Assurance Group
Cisco Systems

© 2005, Cisco Systems, Inc. All rights reserved.

in collaboration with

Bill Rush, John Kinast, Joe McCarty, Aakash Shah
Gas Technology Institute (GTI)

and many other contributors to AGA 12

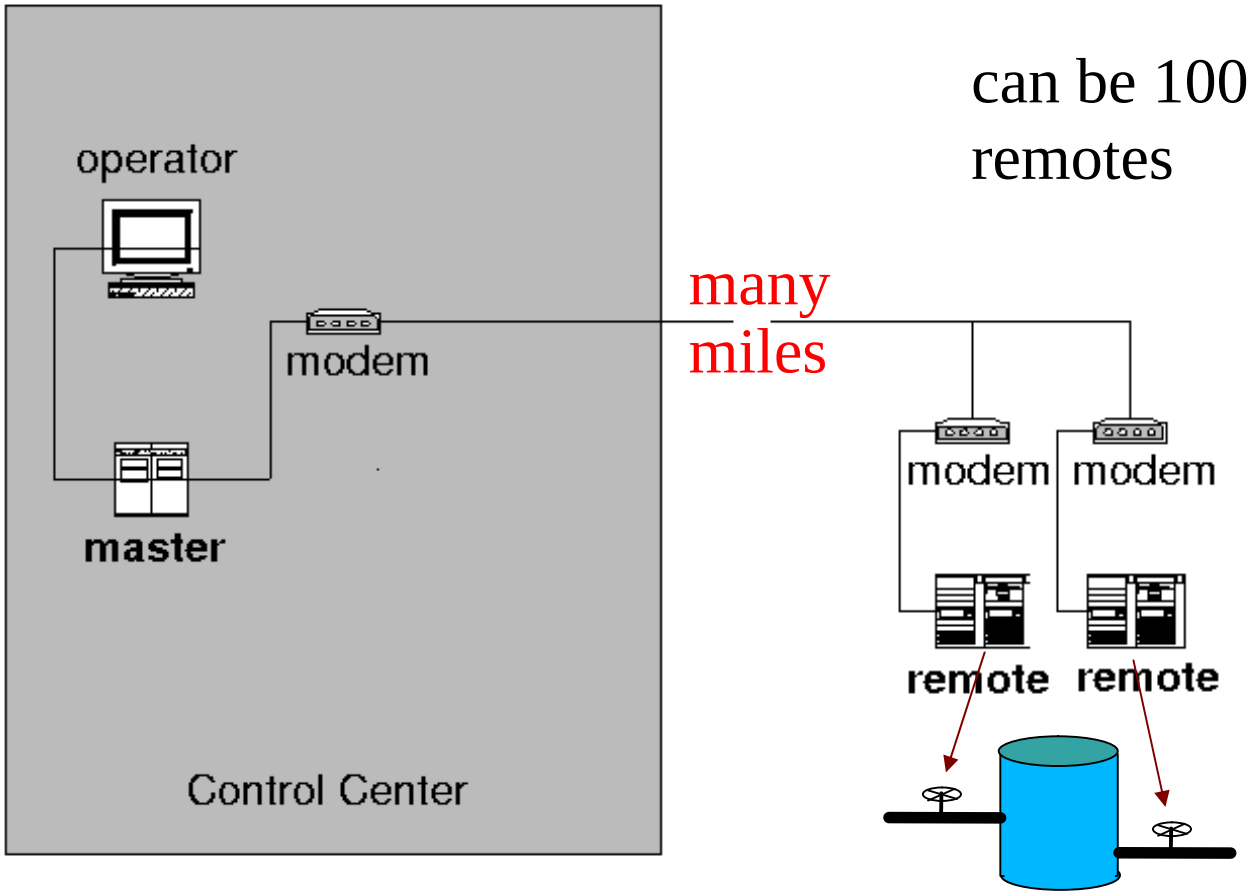
© 2005, Cisco Systems, Inc. All rights reserved.

SCADA

- **SCADA: Supervisory Control And Data Acquisition**
- **used in gas, power, oil, water, waste water, …**
- **to monitor and control remote field devices**
  - **eg. sensors for temperature, pressure, flow, voltage, current, frequency**
  - **eg. valves, breakers**

© 2005, Cisco Systems, Inc. All rights reserved.

Typical SCADA System



can be 1000's of remotes

© 2005, Cisco Systems, Inc. All rights reserved.

SCADA Operation

Cisco.com

- typical modes of operation:
  - master polls each remote in succession
  - remote configured with “set-points” and will “report-by-exception” when set-points triggered
- short messages, typically 8-64 bytes
  - cmd: “read remote 23 status registers”
  - resp: “remote 23 status is 55 66 77”

    => temp 104F, pressure 80psi, flow 3.4 cu ft/min
  - cmd: “write remote 23 control register 1 value 5”

    => open valve #1 to 50%

© 2005, Cisco Systems, Inc. All rights reserved.

SCADA Communications

Cisco.com

- communications are mostly low-speed serial
  - RS232 dialup or leased, 300 – 9600 baud
  - RS485 multidrop, 1200 – 19.2k baud
  - radio, microwave, 1200 – 56k baud
- most protocols use 8- or 16-bit checksum to address accidental communications errors
  - 16-bit CRC is common
  - damaged messages are usually discarded
  - master uses timeout and retry

© 2005, Cisco Systems, Inc. All rights reserved.

SCADA Physical Security

Cisco.com

- **SCADA master located in a secure facility**
  - **barbed wire perimeter**
  - **guards with guns**
- **SCADA remotes in unmanned stations**
  - **barbed wire and padlocks at best**
- **SCADA communications links unprotected**
  - **links are often outside physical control of utility**
    - **dialup, leased-line, radio, …**

© 2005, Cisco Systems, Inc. All rights reserved.

SCADA Communications Security

Cisco.com

- **SCADA communications security relies on:**
  - **secrecy of dialup phone ports**
  - **difficulty of tapping comm lines**
  - **passwords sent in clear, seldom changed, widely known**
  - **obscurity of proprietary protocols**
- **these are all very weak!**

© 2005, Cisco Systems, Inc. All rights reserved.

AGA 12

Cisco.com

- **American Gas Association working group 12**
  - **formed Oct. 2001 after 9/11**
- **developing recommendations for retrofit cryptographic protection of existing SCADA communications**
  - **communications are most vulnerable**
  - **existing systems will be with us for many years**
  - **modification of existing devices largely infeasible**

© 2005, Cisco Systems, Inc. All rights reserved.

AGA12 Recommendations

Cisco.com

- **Part 1: policies and requirements**
  - **done**
- **Part 2: an encryption protocol for serial communications**
  - **almost done**

- **Part ?: authentication for management ports**
- **Part ?: embedding cryptographic protection into newer SCADA masters/RTUs/PLCs/IEDs**
- **Part ?: protection for IP-based SCADA**

© 2005, Cisco Systems, Inc. All rights reserved.

AGA12 Part 2

Cisco.com

- **SSPP – Serial Scada Protection Protocol**
  - **retrofit: applies to existing serial SCADA**
  - **protocol-agnostic: applies to a wide variety of SCADA protocols, systems**
  - **open (public) protocol**
  - **supports interoperability between SSPP devices built by different vendors**

© 2005, Cisco Systems, Inc. All rights reserved.

Why Retrofit?

Cisco.com

- **hardware is environmentally hardened**
  - **more expensive than similar commodity components**
- **hardware often has 20+ year lifetime**
  - **amortization already budgeted**
- **remote device processors computationally challenged**
- **Þ require a retrofit solution that requires minimal modifications to existing systems**

© 2005, Cisco Systems, Inc. All rights reserved.

Why Protocol Agnostic?

Cisco.com

- **thousands (millions?) of SCADA systems deployed throughout US, world**
- **dozens of SCADA hardware manufacturers**
  - **none with majority market share**
- **100's of different protocols**
  - **many proprietary protocols**
  - **a few open protocols: Modbus, DNP**
- **Þ must accommodate most protocols in order to ensure a viable market for protection devices**

© 2005, Cisco Systems, Inc. All rights reserved.

Why Open?

Cisco.com

- **open development of cryptographic solution ensures**
  - **no “security by obscurity”**
  - **security depends only on secrecy of the cryptographic keys**
  - **no proprietary crypto**
  - **open to examination by anyone**

© 2005, Cisco Systems, Inc. All rights reserved.

Why Interoperable?

Cisco.com

- **interoperability ensures utilities do not become locked into one security vendor's products**
  - **promotes competition, lower prices**
  - **protects utility from vendor going out of business**
  - **encourages smaller vendors to compete**

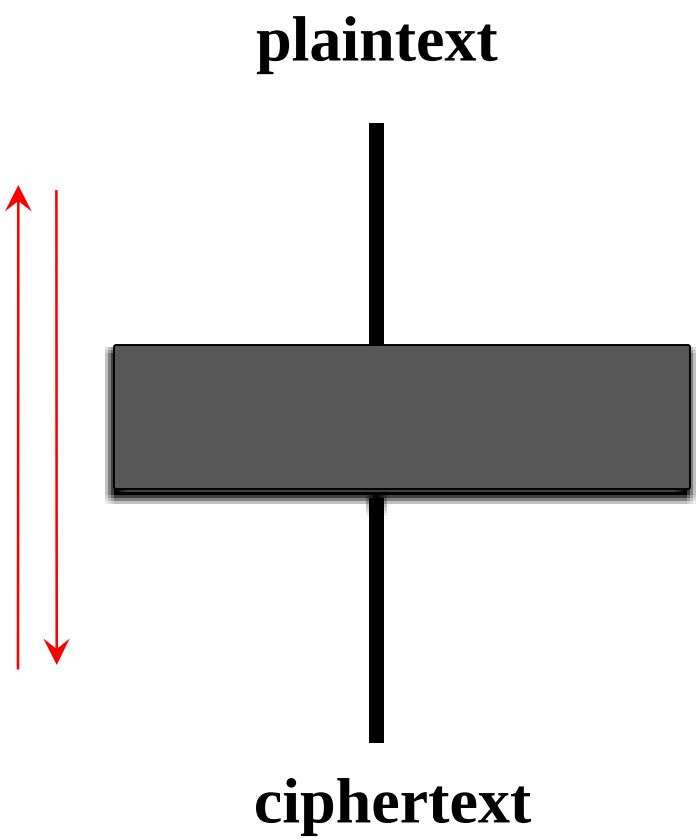
© 2005, Cisco Systems, Inc. All rights reserved.

SCADA Cryptographic Module (SCM)

Cisco.com

SCM:

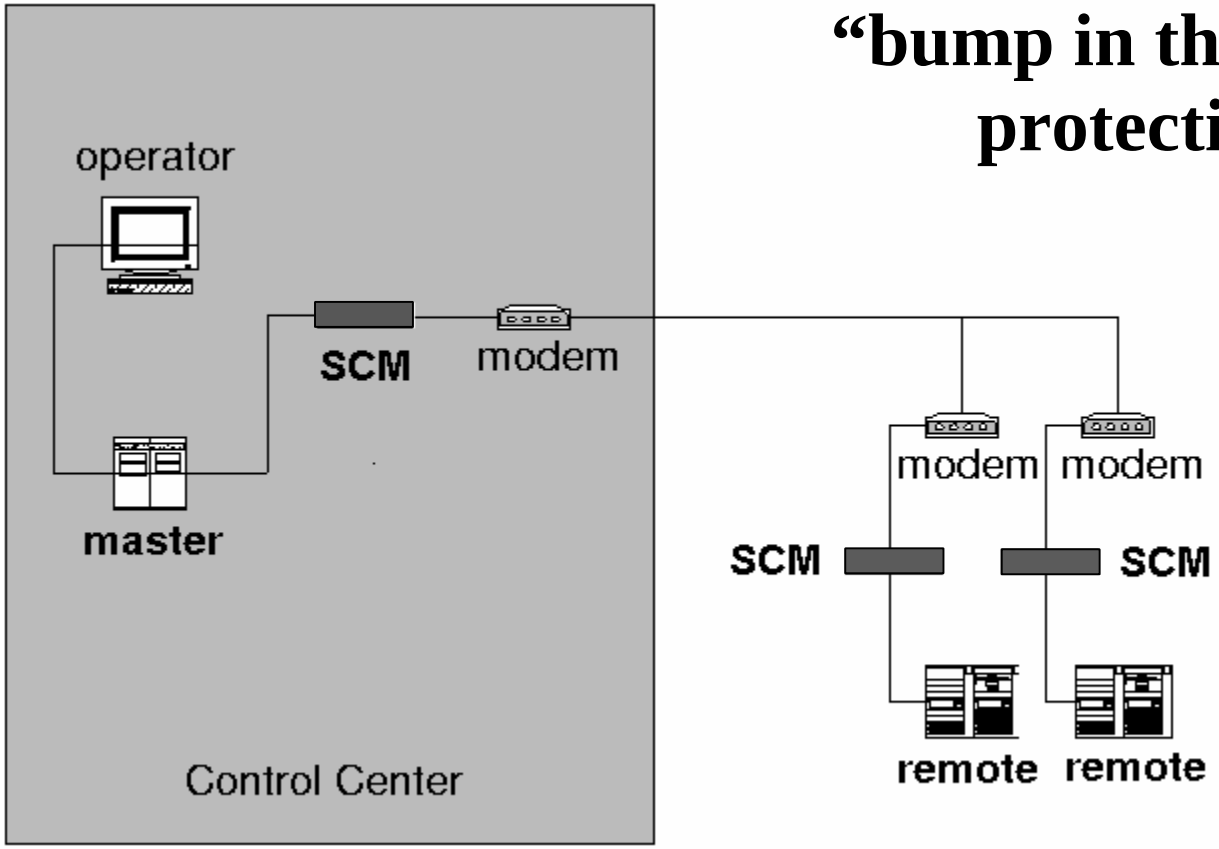
Scada Cryptographic Module



© 2005, Cisco Systems, Inc. All rights reserved.

AGA 12 Cryptographic Module Deployment

“bump in the wire” protection



© 2005, Cisco Systems, Inc. All rights reserved.

Attack Model and Protection Goal

Cisco.com

- **Attack Model**
  - **adversary has access to communications link(s)**
  - **adversary may compromise some remote sites, but few without detection**
  - **compromise of master station is less likely**
  - **adversary may corrupt insiders**
- **protection goal**
  - **protect integrity (or message authenticity) of SCADA traffic between uncompromised stations**
  - **confidentiality is of secondary importance**

© 2005, Cisco Systems, Inc. All rights reserved.

AGA 12 Solution Requirements

Cisco.com

- **introduce minimal additional latency**
- **accommodate as many protocols as possible**
  - **be as independent of protocol as possible**
- **cheap to manufacture**
- **easy to deploy and operate**
- **must not interfere with safety!**

© 2005, Cisco Systems, Inc. All rights reserved.

AGA 12 Solution Constraints

Cisco.com

- **low communication rate**
  - **extra bytes of header/trailer add to latency**
  - **cannot afford to buffer entire message**
- **must not introduce jitter**
  - **some SCADA protocols timing sensitive**
- **noisy communication lines**
- **high predictability of plaintext**
  - **known plaintext attacks likely**
  - **chosen plaintext attacks not a concern**

© 2005, Cisco Systems, Inc. All rights reserved.

Challenges in Protocol Design

Cisco.com

- **unique solution constraints lead to unique challenges in protocol design**
  - **integrity with low latency and little buffering**
  - **accommodating channel errors**
  - **avoiding channel collisions**
  - **ensuring timely delivery**
  - **supporting “mixed mode”**
  - **supporting broadcast & multicast**
  - **key management**

© 2005, Cisco Systems, Inc. All rights reserved.

Challenge: Integrity with Minimal Latency

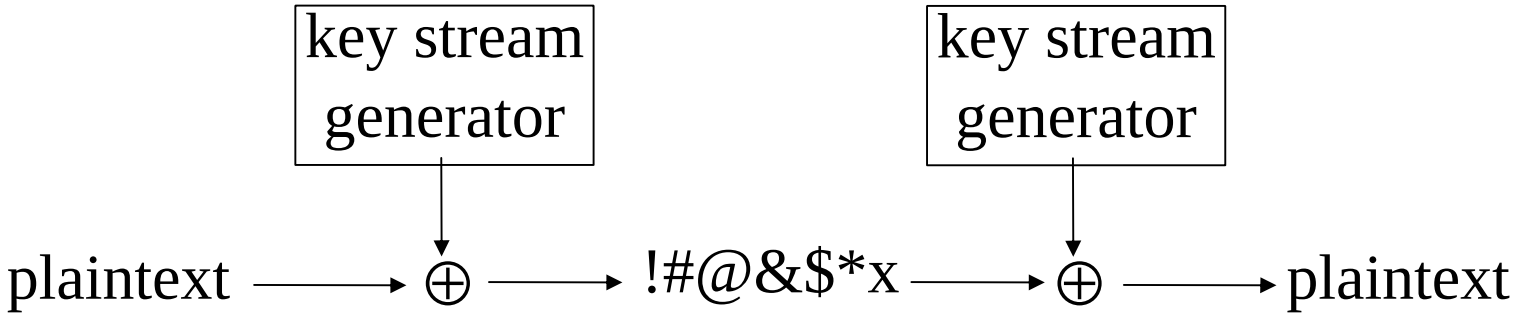
Cisco.com

- **SCADA message integrity**
  - **with minimal buffering**
  - **minimizing latency**
  - **despite known plaintext**

© 2005, Cisco Systems, Inc. All rights reserved.

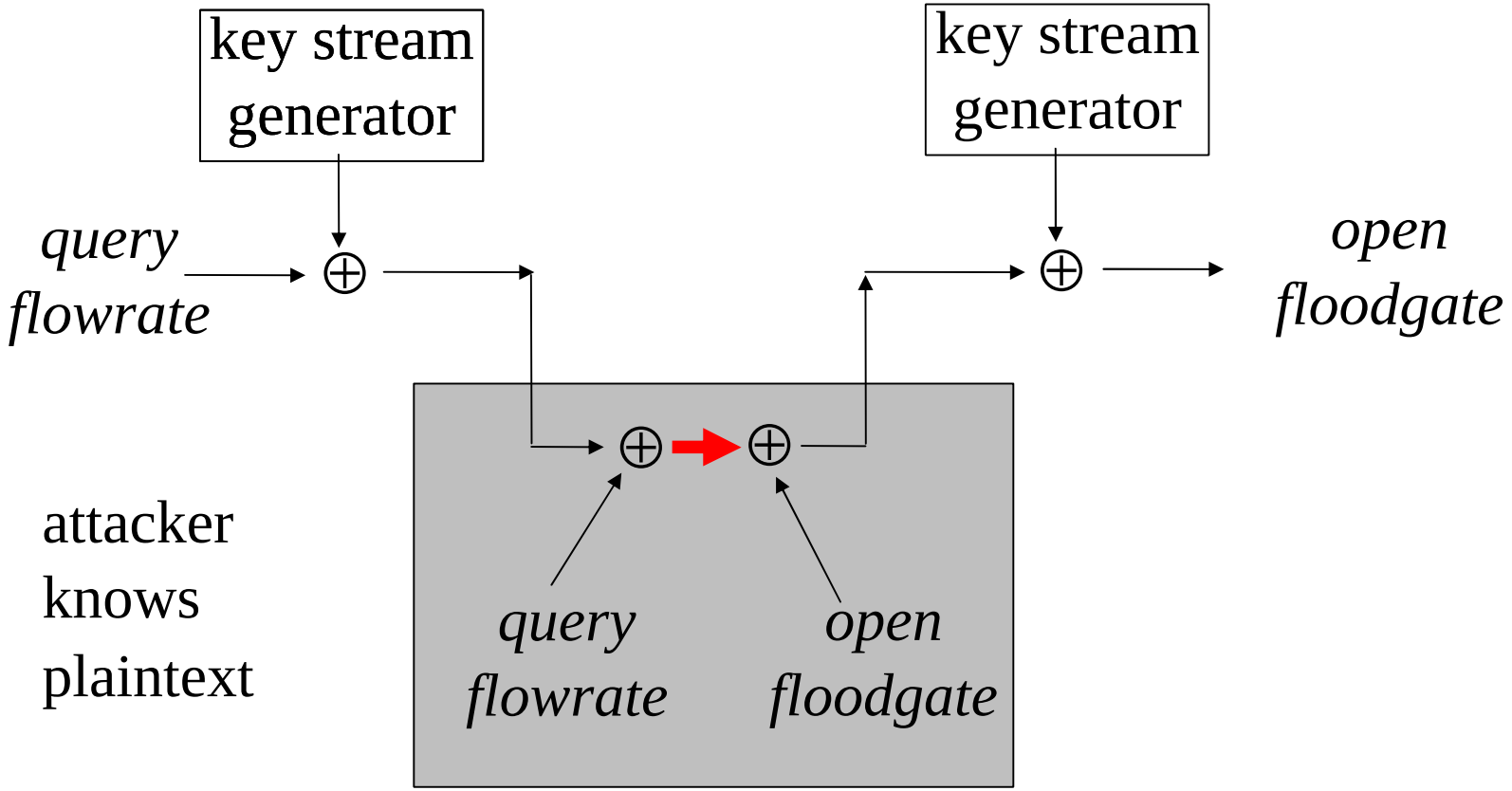
Encryption: NOT a Solution!

- **stream cipher minimizes latency and jitter**
  - **key stream generator emits deterministic stream of pseudo-random bits**



© 2005, Cisco Systems, Inc. All rights reserved.

Encryption Does Not Provide Integrity



© 2005, Cisco Systems, Inc. All rights reserved.

WEP Encryption

- **WEP (802.11b) uses stream cipher plus a CRC**
- **attacker with known plaintext can patch up CRC "underneath" encryption**
- **attacker with *partial* known plaintext can still patch CRC**
  - **CRC is not keyed and is linear:**

    CRC(M+E) = CRC(M) + CRC(E)

© 2005, Cisco Systems, Inc. All rights reserved.

CBC-mode Block Encryption

Cisco.com

- block encryption works on blocks of bits
  - 128 bits for AES, 64 bits for 3DES
  - diffuses plaintext bits across entire cipher block
  - attacker cannot directly flip bits
- CBC-mode chains blocks together
  - decryption of block depends on preceding block
  - but can be vulnerable to splicing attacks
    - Stubblebine & Gligor [IEEE 1992]

© 2005, Cisco Systems, Inc. All rights reserved.

Encryption Does Not Provide Integrity

Cisco.com

- **integrity is not assured by**
  - **stream cipher**
  - **stream cipher with CRC**
  - **block cipher with CBC and CRC**

encryption does not assure integrity!!

© 2005, Cisco Systems, Inc. All rights reserved.

Message Authentication Code

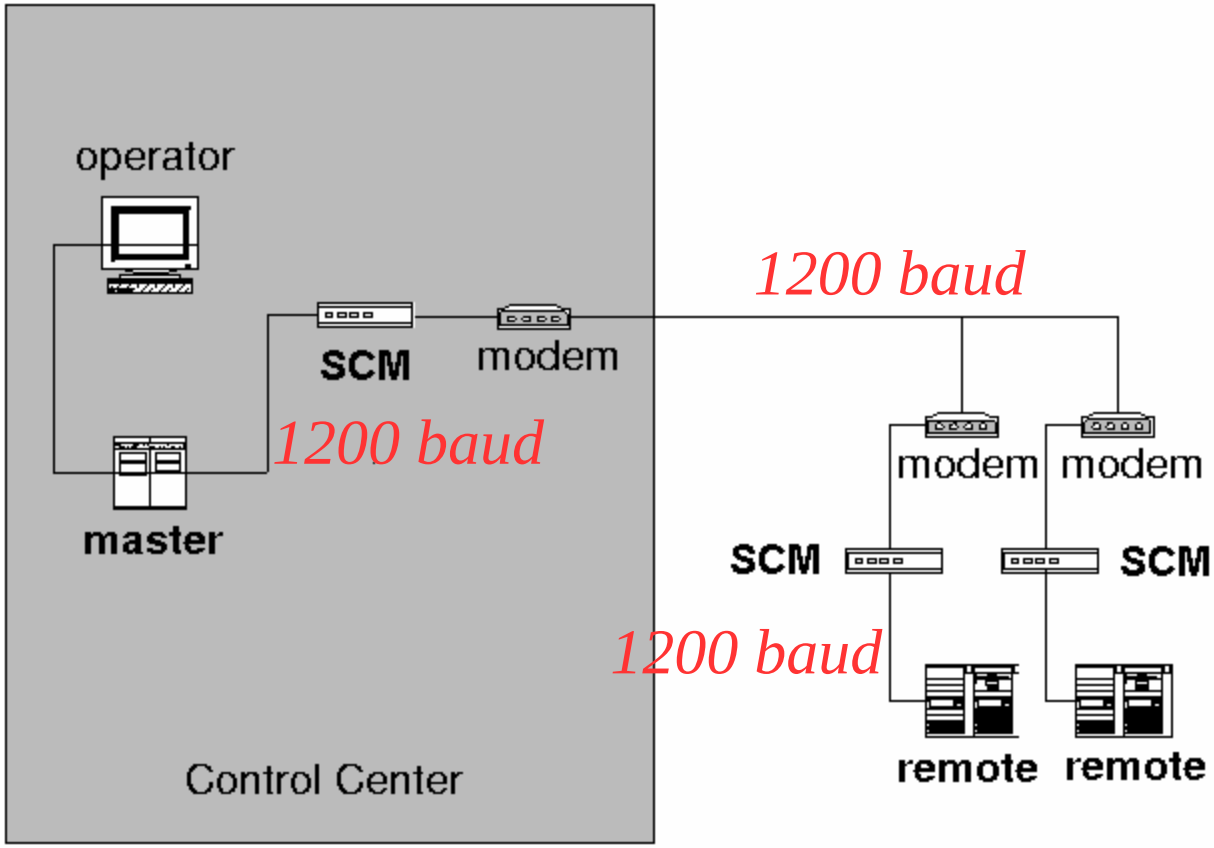
Cisco.com

- **MAC is a keyed hash**
  - **MAC(key, msg) = HASH[key || msg]**
- **sender sends**

  msg || MAC(key, msg)
- **transmitted message is longer than plaintext**
  - **adds latency = length of MAC**
- **receiver must buffer message to verify MAC**
  - **buffering adds latency = length of msg**

© 2005, Cisco Systems, Inc. All rights reserved.

AGA 12 Cryptographic Module Deployment



© 2005, Cisco Systems, Inc. All rights reserved.

Integrity by Leveraging SCADA CRC

Cisco.com

- **PE-mode – a new Position Embedding block encryption mode**
- **forward decrypted block to SCADA device as soon as decrypted**
- **rely on SCADA device to check CRC**
- **PE mode ensures adversary cannot reliably:**
  - **construct a specific unauthentic message**
  - **forge any unauthentic message with valid CRC**

© 2005, Cisco Systems, Inc. All rights reserved.

Position Embedding (PE) Mode

Cisco.com

- **consider messages as 2D "matrix" of blocks:**

m1:	b1,1	b1,2	b1,3	
m2:	b2,1	b2,2	b2,3	b2,4
m3:	b3,1	b3,2		

- **encrypt blocks as follows:**

$$E_k[\, b_{i,j} \,] = E_k[\, b_{i,j} \oplus E_k[\, i\ j\ 0 \ldots \,] \,]$$

© 2005, Cisco Systems, Inc. All rights reserved.

PE Mode

$$E_k[\, b_{i,j} \,] = E_k[\, b_{i,j} \oplus E_k[\, i\ j\ 0 \ldots \,] \,]$$

- $E_k[\, i\ j\ 0 \ldots \,]$ is encryption of **i** and **j**, ie. position
- $b_{i,j} \oplus E_k[\, i\ j\ 0 \ldots \,]$ diffuses position thru $b_{i,j}$
- $E_k[\, b_{i,j} \oplus E_k[\, i\ j\ 0 \ldots \,] \,]$ diffuses plaintext and position thru encrypted block

© 2005, Cisco Systems, Inc. All rights reserved.

PE Mode

- every cipher bit depends on every plaintext bit (within a block)
  - flip 1 or more bits Þ entire block decrypts to random bits
- every cipher block depends on position
  - wrong position Þ entire block decrypts to random bits
- any attack leads to at least 1 randomized block

© 2005, Cisco Systems, Inc. All rights reserved.

PE Mode with CRC

- **PE mode with CRC**

mi:	ci,1	ci,2	ci,3 CRC

- **damaging a block randomizes B consecutive bits (where B is cipher block size)**
- **for B ³ N, probability of unauthentic message containing valid N-bit CRC is 1 in 2^N** (see proof in ACNS '04 paper)

© 2005, Cisco Systems, Inc. All rights reserved.

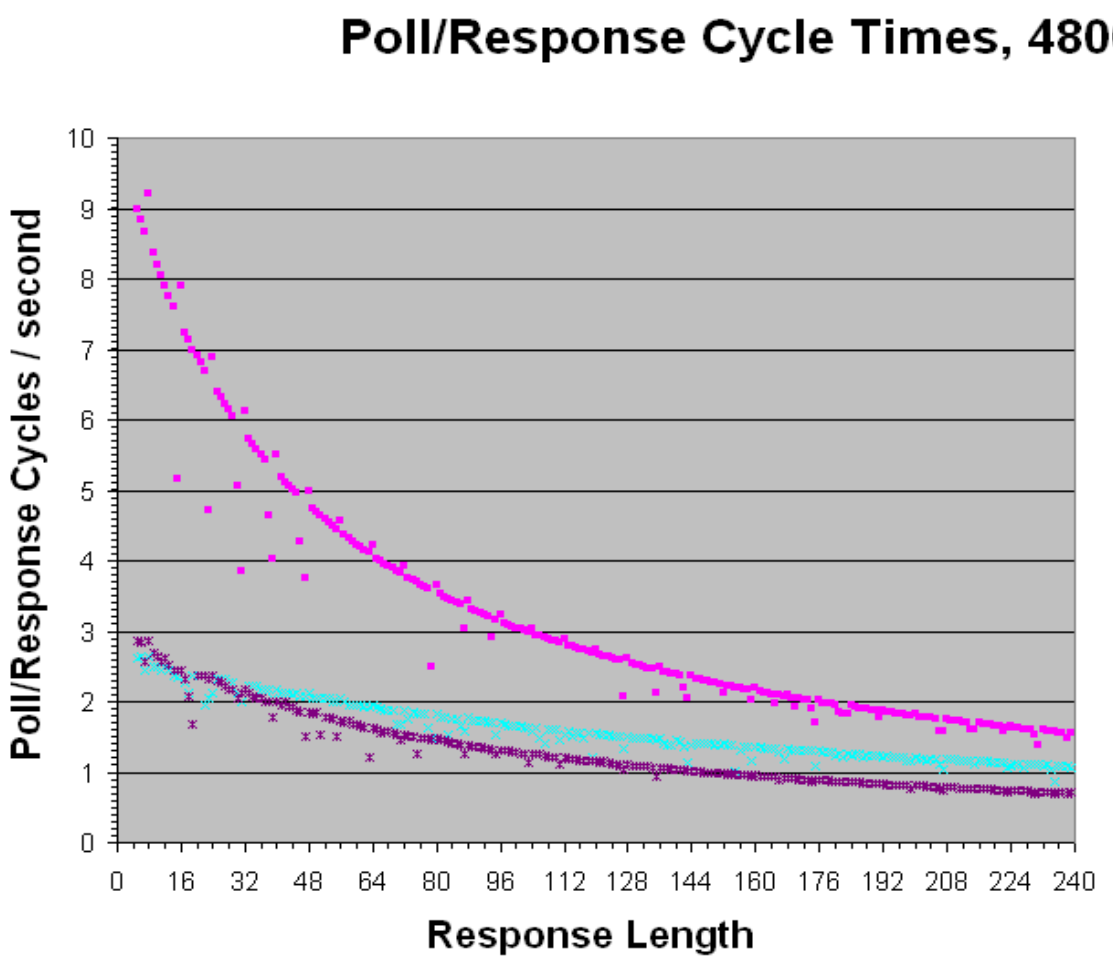
PE mode Properties

Cisco.com

- **latency = 1 cipherblock at sender**
  + 1 cipherblock at receiver
- **two encryptions per block**
  - **but $E_k[\ i\ j\ 0...\ ]$ can be precomputed**
- **works with any block cipher**
- **1 in 2^{16} is sufficient security for SCADA**
  - **attacker must make many trials at low speed**
  - **attacker cannot forge a specific message**
- **latency including header = 44 characters**

© 2005, Cisco Systems, Inc. All rights reserved.

Poll/Response Times

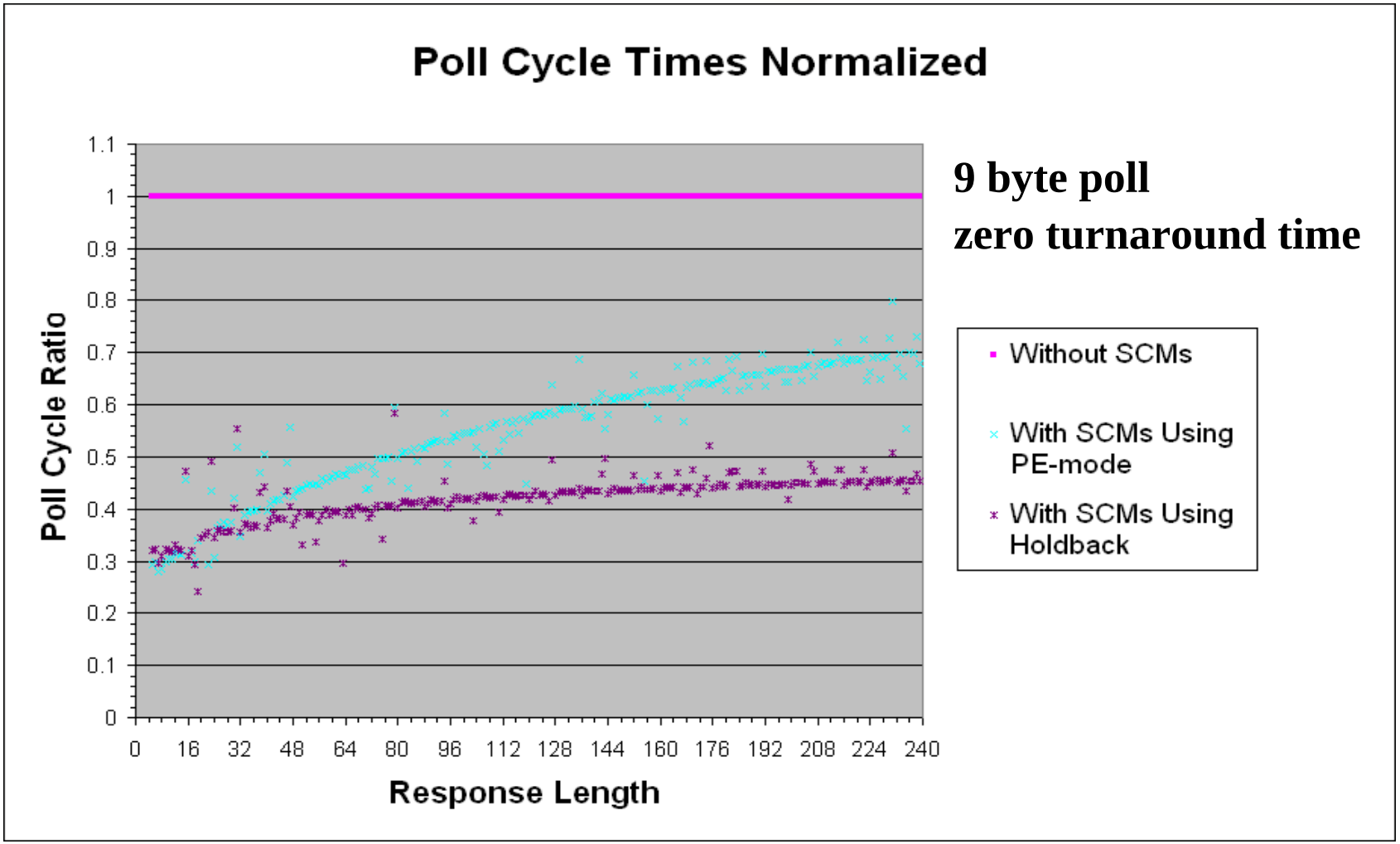


9 byte poll
zero turnaround time

- Without SCMs
- With SCMs Using PE-mode
- With SCMs Using Holdback

© 2005, Cisco Systems, Inc. All rights reserved.

Poll/Response Times (normalized)

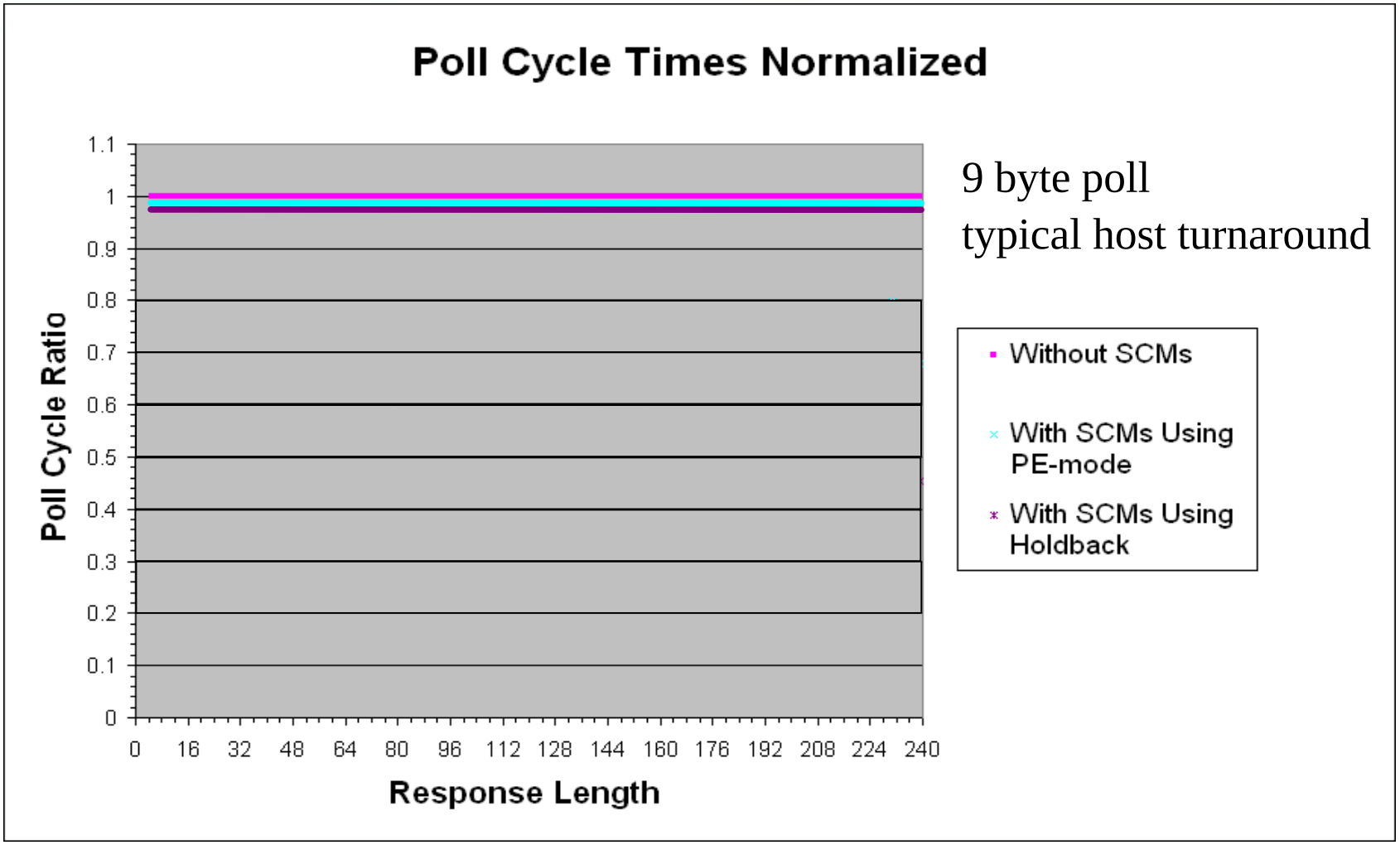


9 byte poll

zero turnaround time

© 2005, Cisco Systems, Inc. All rights reserved.

Poll/Response Times (typical)



9 byte poll
typical host turnaround

© 2005, Cisco Systems, Inc. All rights reserved.

Challenges in Protocol Design

Cisco.com

- **unique solution constraints lead to unique challenges in protocol design**
  - **integrity with low latency and no buffering**
  - **accommodating channel errors**
  - **avoiding channel collisions**
  - **ensuring timely delivery**
  - **supporting “mixed mode”**
  - **supporting broadcast**
  - **key management**

© 2005, Cisco Systems, Inc. All rights reserved.

Challenge: Channel Collisions and Errors

Cisco.com

- **SCADA protocols handle errors by retry**
  - **SCMs depend on SCADA system to retry**
- **SCADA protocols by design avoid collisions**
  - **SCMs talk only when SCADA system does** (almost)
  - **SCM protocol does not use ACK/NACK, retry, windowing, etc. like TCP**
    - **no guaranteed delivery, reordering, fragmentation & reassembly, etc.**
    - **more like UDP**

© 2005, Cisco Systems, Inc. All rights reserved.

Challenges in Protocol Design

Cisco.com

- **unique solution constraints lead to unique challenges in protocol design**
  - **integrity with low latency and no buffering**
  - **accommodating channel errors**
  - **avoiding channel collisions**
  - **ensuring timely delivery**
  - **supporting “mixed mode”**
  - **supporting broadcast**
  - **key management**

© 2005, Cisco Systems, Inc. All rights reserved.

Challenge: Ensuring Timely Delivery

Cisco.com

- **SCADA messages contain information about system state at a point in real time**
- **messages must be delivered in a timely way**
- **ordered delivery, freshness alone are *not* sufficient!**

© 2005, Cisco Systems, Inc. All rights reserved.

Ensuring Timely Delivery

Cisco.com

- **messages include time stamps representing relative time since beginning of session**
- **time stamps must be within tolerance of current session clock**

  tolerance = 2EC + A

  E = session expiry

  C = clock accuracy, eg. 50×10^{-6} (50 ppm)

  A = ack timeout during session negotiation
- **typical tolerance is 10 sec for E = 1 day**

© 2005, Cisco Systems, Inc. All rights reserved.

Challenges in Protocol Design

Cisco.com

- **unique solution constraints lead to unique challenges in protocol design**
  - **integrity with low latency and no buffering**
  - **accommodating channel errors**
  - **avoiding channel collisions**
  - **ensuring timely delivery**
  - **supporting “mixed mode”**
  - **supporting broadcast**
  - **key management**

© 2005, Cisco Systems, Inc. All rights reserved.

Challenge: Supporting Mixed Mode

Cisco.com

- **mixed mode: some SCADA remotes with SCMs, some without (multidrop link)**
  - **some SCADA remotes are low value**
  - **some unprotected during phased deployment**
- **master SCM must send ciphertext to remotes with SCMs, plaintext to remotes without SCMs**
  - **must parse SCADA addressing**
- **encrypted messages must not confuse SCADA remotes without SCMs**

© 2005, Cisco Systems, Inc. All rights reserved.

Challenge: Supporting Broadcast & Multicast

Cisco.com

- some SCADA systems use broadcast commands
  - for “set time” or “emergency shutdown”
  - not ack'ed, but often repeated multiple times
- for mixed mode, send both protected and in clear
  - adversary sees plaintext
- symmetric broadcast key shared amongst all SCMs
  - broadcast key is dynamically generated
  - distributed during session establishment
  - use two broadcast sessions with overlapping expiry and rolling key renegotiation

© 2005, Cisco Systems, Inc. All rights reserved.

Challenge: Key Management

Cisco.com

- **symmetric keying**
  - **pairs of shared keys between SCMs**
  - **not N^2 for SCADA!**
- **public keying**
  - **better security**
  - **peer discovery simplifies field maintenance**
  - **must address certificate revocation/renewal**
  - **could enable role-based access control**

© 2005, Cisco Systems, Inc. All rights reserved.

Status

- **draft protocol almost ready for ballot**
  - **see www.gtiservices.org/security**
- **prototype SCM implemented in Java**
  - **open source: scadasafe.sourceforge.net**
  - **runs on Arcom VIPER embedded linux controller**
  - **lab tested at Cisco, GTI, PNNL, anon. gas co.**
  - **undergoing security evaluation at SNL**
  - **undergoing preformance evaluation at INEL**
  - **beginning field tests at utilities**
  - **used as GTI standard for interoperability testing**
- **several vendors starting to build products**

© 2005, Cisco Systems, Inc. All rights reserved.

Future Work

Cisco.com

- further testing with various SCADA systems
- independent verification of security
- more analysis for use in power, oil, water, ...
- add key management, especially public key
- improve encryption modes for lower latency
- investigate embedding in RTUs, modems
- user authentication and authorization
- IP-based SCADA protection

© 2005, Cisco Systems, Inc. All rights reserved.

OT-ERA

- PE-mode does not work with XOR-based checksum
  - some SCADA protocols use LRC
- OT-ERA: One Time Encryption with Redundancy for Authentication
  - joint with Steve Wang, James Madison (JMU)
  - uses different key for each block
  - chains blocks
  - to appear in ACNS05

© 2005, Cisco Systems, Inc. All rights reserved.

Conclusion

Cisco.com

- **AGA 12 Part 2 is likely to become an important standard for protecting SCADA communications**
- **we invite comments and critique!!**
  - **problems**
  - **improvements**
  - **extensions**
  - **applications**

© 2005, Cisco Systems, Inc. All rights reserved.

References

- www.gtiservices.org/security
- scadasafe.sourceforge.net
- A. Wright, J. Kinast, and J. McCarty. Low-Latency Cryptographic Protection for SCADA Communications. Proceedings ACNS '04, Springer-Verlag LNCS 3089.
- akwright@acm.org
- bill.rush@gastechnology.org

© 2005, Cisco Systems, Inc. All rights reserved.

CIAG

Cisco.com

- Cisco's Critical Infrastructure Assurance Group
  - Mission: conduct and sponsor research to improve the security of network and computing technology used by critical infrastructures
  - research is security-related, but not tied to Cisco products
    - respond to PDDs for greater collaboration between industry, govt, academe
    - find new product directions, markets
    - improve market perception of Cisco as security conscious
    - promote greater use and diversity of internet technologies
    - altruism

© 2005, Cisco Systems, Inc. All rights reserved.