TCIP: Trustworthy Cyber Infrastructure for Power

Predictive YASIR: High Security with Lower Latency in Legacy SCADA

Rouslan V. Solomakhin, Patrick P. Tsang, Sean W. Smith
Dartmouth College
rouslan@solomakhin.net

IFIP WG 11.10 4th ICCIP
March 15, 2010
• Power grid networks
• Example attacks
• Existing solutions
• Our solution
• Evaluation results
• Power grid networks
• **Example attacks**
• Existing solutions
• Our solution
• Evaluation results
Attacks

- Modify message
- Replay message
Replay Message

Front End Processor

I am Fine

Data Aggregator

I am on Fire
• Power grid networks
• Example attacks
• **Existing solutions**
• Our solution
• Evaluation results
Insert Bump-in-the-Wire Devices

Front End Processor

Bump-in-the-Wire

Bump-in-the-Wire

Data Aggregator

Message

Message, Counter, Digest

Message
• SEL-3021-2
  – Schweitzer Engineering Laboratories
• AGA SCM
  – American Gas Association SCADA Cryptographic Module
• YASIR
  – Our lab, previously
SA

V

R
Bump-in-the-Wire Devices

- SEL-3021-2
  - Schweitzer Engineering Laboratories
- AGA SCM
  - American Gas Association SCADA Cryptographic Module
- YASIR
  - Our lab, previously
• Message format novel use
  – Random errors in legacy device
  – Malicious error → random error

Modbus / ASCII

Start | Message | CRC | End

AES-CTR : Counter mode

AES-ECB : Electronic Code Book mode
• SEL-3021-2
  – Schweitzer Engineering Laboratories
• AGA SCM
  – American Gas Association SCADA Cryptographic Module
• YASIR
  – Our lab, previously
• PE-inspired error conversion
  – Malicious → random
• Standard authentication technique
  – HMAC-SHA-1-96 digest
• Stronger security
  – 80 vs. 32 bits
• Lower latency
  – 16 vs. 32 byte-times
Outline

• Power grid networks
• Example attacks
• Existing solutions
• **Our solution**
• Evaluation results
• Reduce YASIR latency
  – Prediction
  – Compression
  – Pre-sending
Predictive YASIR

S
A
V
R

S | Message | E

| D | + | S | T |
Outline

• Power grid networks
• Example attacks
• Existing solutions
• Our solution
• Evaluation results
• Scalable Simulation Framework
  – David M. Nicol
  – Discrete-event simulation of large, complex systems
    [http://www.ssfnet.org/homePage.html]

• Varying unique messages
  – Hard to predict rare, unique events
  – Real-world SCADA repetitive, few events, e.g., temperature

• Modbus / ASCII
  – Common message format in power grid networks

• Trace from Paul Myrda of EPRI
  – Electronic Power Research Institute
Results

![Graph showing the relationship between the number of unique messages and byte-time latency for different systems. The graph includes lines for YASIR, P-YASIR, and Minimum, with YASIR showing a slight decrease in latency as the number of unique messages increases.]
Conclusions

- Security
  - Other BitW devices ≤ YASIR = Predictive YASIR
- Performance
  - Other BitW devices < YASIR < Predictive YASIR
- Implementation
  - Predictive YASIR in C++ (YASIR in HDL)
- Future improvements
  - More real data
  - Move BitW devices closer to end-points

Thank you! Questions?
rouslan@solomakhin.net