J. B. Speed
School of
Engineering

Hardening the Active Perimeter of Industrial Control Networks

James H. Graham
Intelligent Systems Research Lab.
University of Louisville

J.B. Speed School of Engineering

Overview

- Project Background
- ICS Cyber-security Threat
- Case Study – Water Sector Cyber-security Vulnerabilities
- Research Directions
  - Field Intrusion Detection
  - Hardened RTU and Security Preprocessor
- Collaborations and Partnerships

Background – SCADA Cyber-Security

- 5-year SCADA security research project funded by Dept. of Homeland Security through Natl. Inst. of Hometown Security
- Conducted by Univ. of Louisville – Intelligent Systems Research Laboratory
- Project started January 1, 2006 and now continuing with second phase initiated in June 2010 (water sector focus)

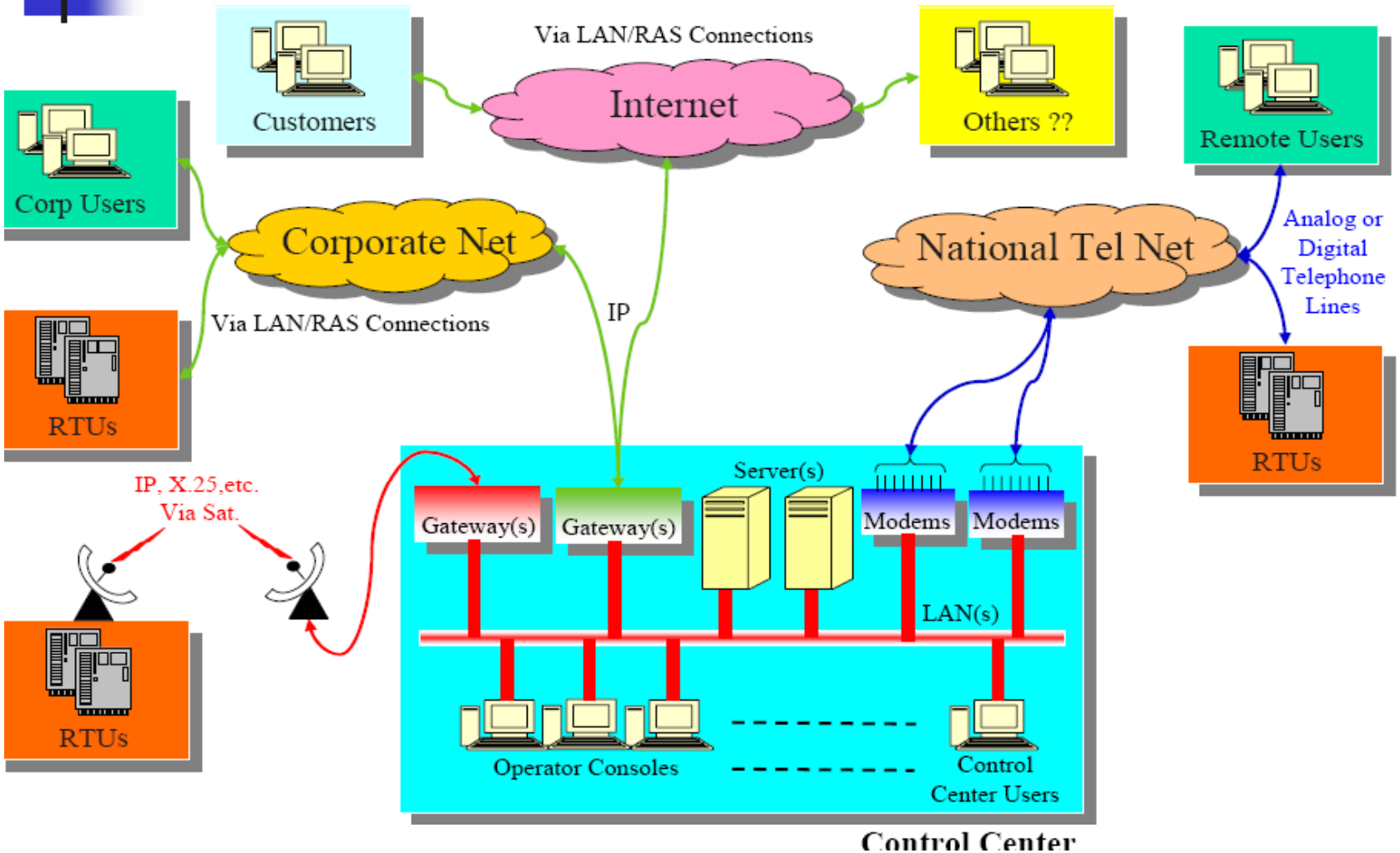
Project Relevance to DHS and Nation

- SCADA systems control much of our industrial infrastructure
- These systems are currently very vulnerable to cyber attack, despite recent attempts to improve security
- This research has created approaches which can significantly enhance the cyber security of these networks

Industrial Collaborators

- Hexion Specialty Chemicals
- LG&E and Kentucky Utilities
- Louisville Water Company
- Eastman Chemical
- EWA NAC-MAST (ARL)

High Level SCADA



ICS Security Vulnerabilities

- Insider threats are always a concern
  - Valid user intentionally or accidentally creates an incorrect setting
  - BCIT study indicated that insiders accounted for 78% of all incidents where costs exceeded $100K
- External threats are increasing
  - More open pathways to RTU lead to increasing ICS reconnaissance
  - Attacks can be direct or incremental
  - Spoofing, man in the middle, DOS, and many other traditional cyber attacks possible
- COTS components have increased ICS vulnerability
  - Flaws and vulnerabilities in COTS hardware and software make RTUs vulnerable to common cyber security attacks, by allowing attackers to use commonly available attack tools.

J.B. Speed
School of
Engineering

Case Study:
Water Sector Cyber-Security Vulnerabilities

Major Technical Vulnerabilities

- Poorly Secured Legacy System
- Lack of Trained Cyber Security Specialists
- Delayed Application of Patches
- Lack of cyber-security situational awareness (Event monitoring / Audit)
- Communication Security
- Remote Access

J.B. Speed School of Engineering

Component Compliance Summary

Component Category	Percent of Questions meeting target SAL	Percent of Questions 1 SAL below target SAL	Percent of Questions 2 SAL below target.
Modem	100%	0%	0%
HMI	74%	14%	12%
Router	65%	10%	25%
Database Server	61.9%	23.8%	14.3%
Firewall	40.7%	25.9%	33.3%
Switch	38.1%	19%	42.9%
Serial Radio	33.3%	8.3%	58.3%
Terminal Server	29.4%	35.3%	35.3%
RTU	27.8%	27.8%	44.4%
PLC	27.8%	22.2%	50%

J.B. Speed School of Engineering

Technical Vulnerability:
Poorly Secured Legacy System

- Little or no cyber security features
- Long replacement cycle – 25 years or more
- Difficult to incorporate new cyber security technologies
- Related Research
  - AGA 12 SCADA cryptographic modules
  - UofL ISRL Hardened RTU using reduced kernels
  - CMU and Purdue investigating the general problem of legacy systems in IT.

Technical Vulnerability:
Lack of Trained Cyber Security Specialists

- Most personnel expertise in either control or security
- Training for new ICS security different from legacy systems
- No secure Water Sector ICS definition
- Relevant Research
  - University of S. Australia is developing SCADA security program for their engineering program
  - Sandia and INL ICS cyber-training

Technical Vulnerability:
Delayed Application of Patches

- Patches not applied or delayed
- Patch incompatibility
- Security Patches difficult to install
- Relevant Research
  - Patch management research at Purdue, CMU, and others aimed at traditional IT
  - CSSP Guidance documents (best practices only)
  - No specific technical solution for ICS systems is currently being researched (to our knowledge)

Technical Vulnerability:
Lack of cyber-security situational awareness

- Lack of event generation
- Lack of event correlation
- Lack of audit trail analysis
- No integration with control system view (operator HMI)
- Related Research
  - LOGIIC
  - Portaledge and Quickdraw (Digital Bond)
  - ISRL field intrusion detection

Technical Vulnerability:

Communication Security

- Unsecured protocols
- Unsecured links
- Poor isolation
- Relevant Research
  - AGA-12 SCADA encryption
  - UofL ISRL: secure SCADA communications
  - University of Tulsa (Secure Modbus)
  - DNP3: Secure Authentication

J.B. Speed School of Engineering

Technical Vulnerability:
Remote Access

- Weak authentication scheme for employee and vendors
  - Simple password or no/shared password
- Lack of restrictive default values
- Devices do not support multiple roles with least privilege.
- Related Research
  - Some ISRL Hardened RTU technology can be applied to Remote Access vulnerabilities.

Business/Operational Vulnerabilities

- Lack of Business Case for Cyber Security for control systems
- ICS security not integrated into overall Risk Management policies
  - Lack of model and awareness
- Two Cultures Problem
  - Different goals for IT and Control Engr.

J.B. Speed School of Engineering

Vulnerability Priority Levels

Vulnerabilities	Prevalence	Impact severity	Exploit Difficulty
Legacy Systems	Very High	Very High	Low
Lack of Trained Cyber-security Specialists	High	High	N/A
Delayed Patches	High	High	Medium
Lack of Cyber-security Situational Awareness	High	Medium	Medium
Communication Security	Medium	High	Medium
Remote Access	Medium	High	High

Research Directions

Enhanced ICS Security

- The University of Louisville Research Team has identified several promising approaches:
  - Enhanced authentication
  - Field intrusion detection systems
  - Security-hardened field devices
  - Security preprocessor for ICS

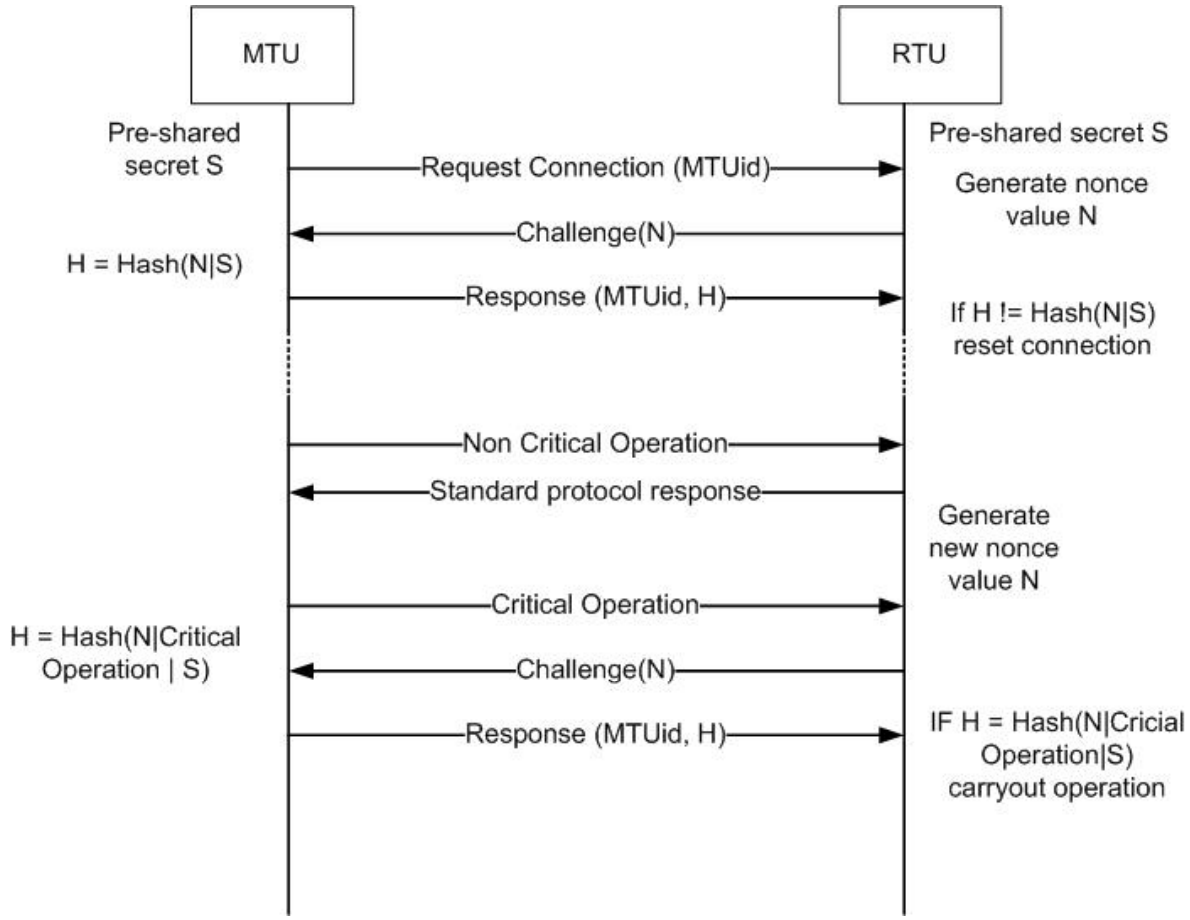
Enhanced Authentication

- Message integrity and authentication is usually more important than data confidentiality in ICS
- Many IT authentication approaches are too computationally expensive for ICS
- We have developed and evaluated several low overhead authentication schemes

Challenge-Response

- High impact operations can be challenged by the field device
- MTU responds with a hashed secret, and the field device then checks the hash against a table of hashed secrets
- N-Secrecy enhancement adds multiple levels of authentication for use when attack is detected

Challenge Response



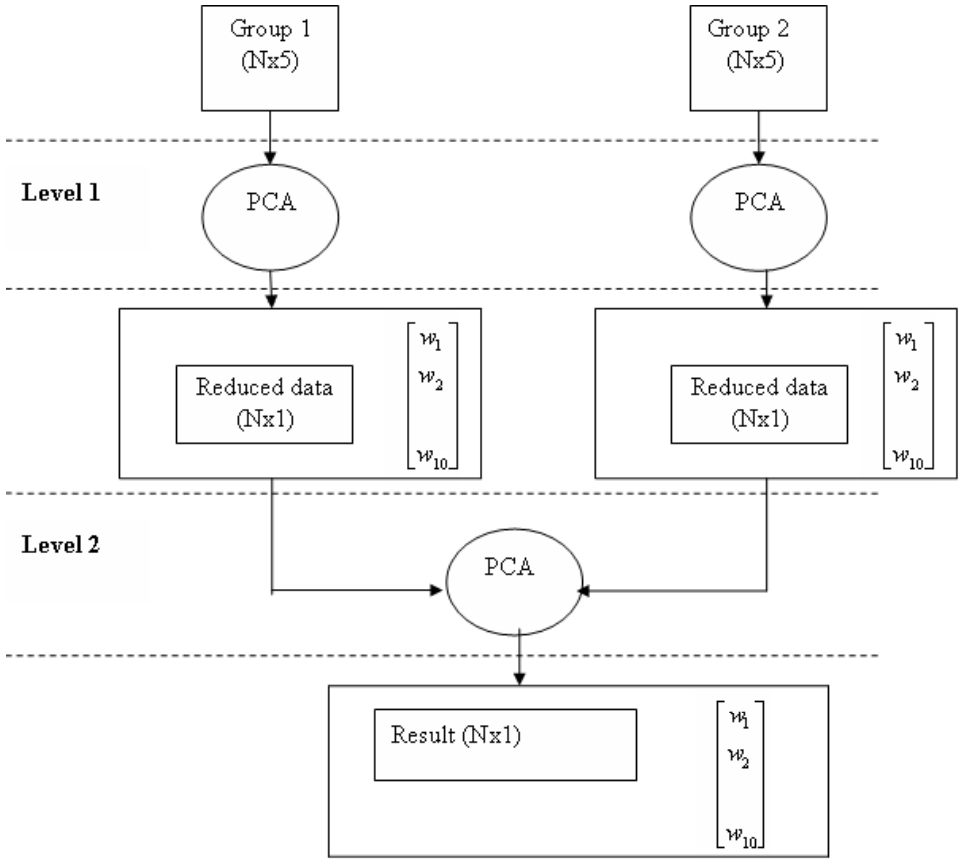
N-Secrecy Enhancement

- The idea is to keep two (or more) private keys, two secrets, and a hash table at each unit
- One general purpose private key (GPK) between the Master Terminal Unit (MTU), and all the Remote Terminal Units (RTUs) that can communicate with MTU
- Another key between the MTU and each RTU, a specific private key (SPK)
- Two secrets between the MTU and each RTU, or each pair of sender-receiver (SSEC1 and SSEC2)
- A hash table containing Key-Value pairs list that corresponds to a list of SSEC1-(SPK, SSEC2), i.e. Key is SSEC1, and value is (SPK,SSEC2)
- **Security level can be increased as threat level increases**

Field Intrusion Detection Systems

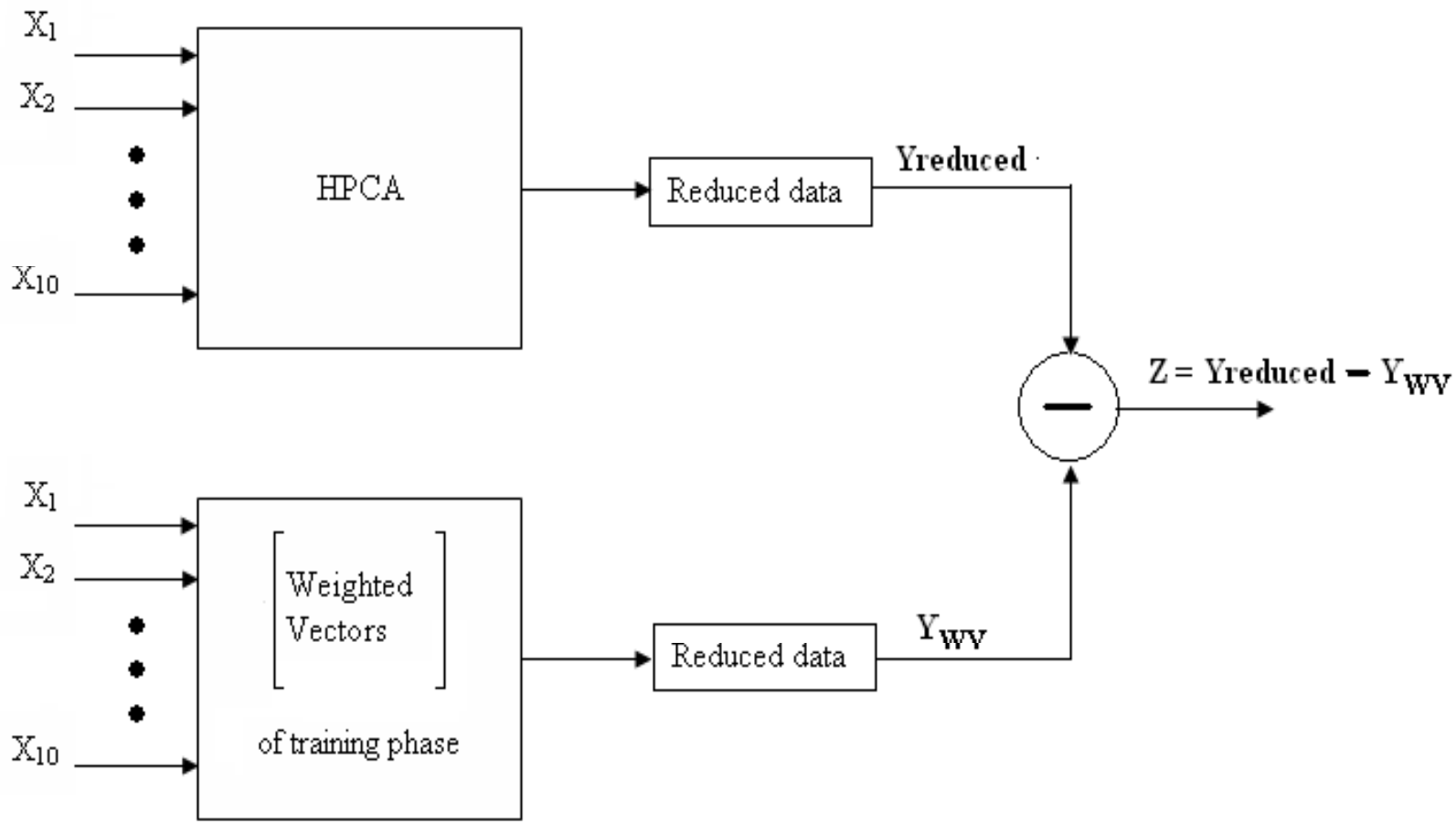
- Traditional network intrusion detection systems focus on “signatures” of suspicious network traffic
- For ICS we have additional information available in the form of systems data from the controlled process
- We have implemented a FIDS for chemical plants and integrated it with traditional Network IDS

HPCA (Hierarchical PCA)



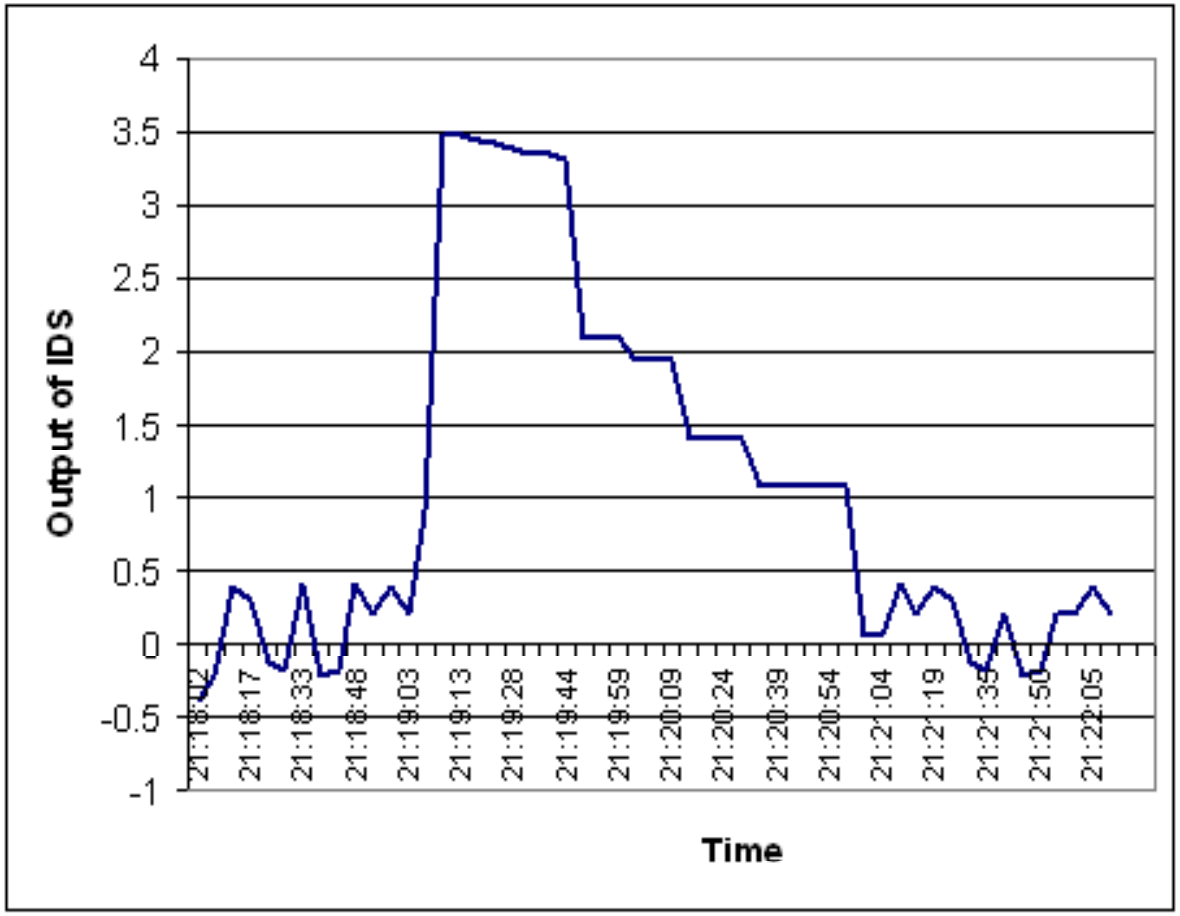
J.B. Speed
School of
Engineering

Operational phase – Intrusion Detection



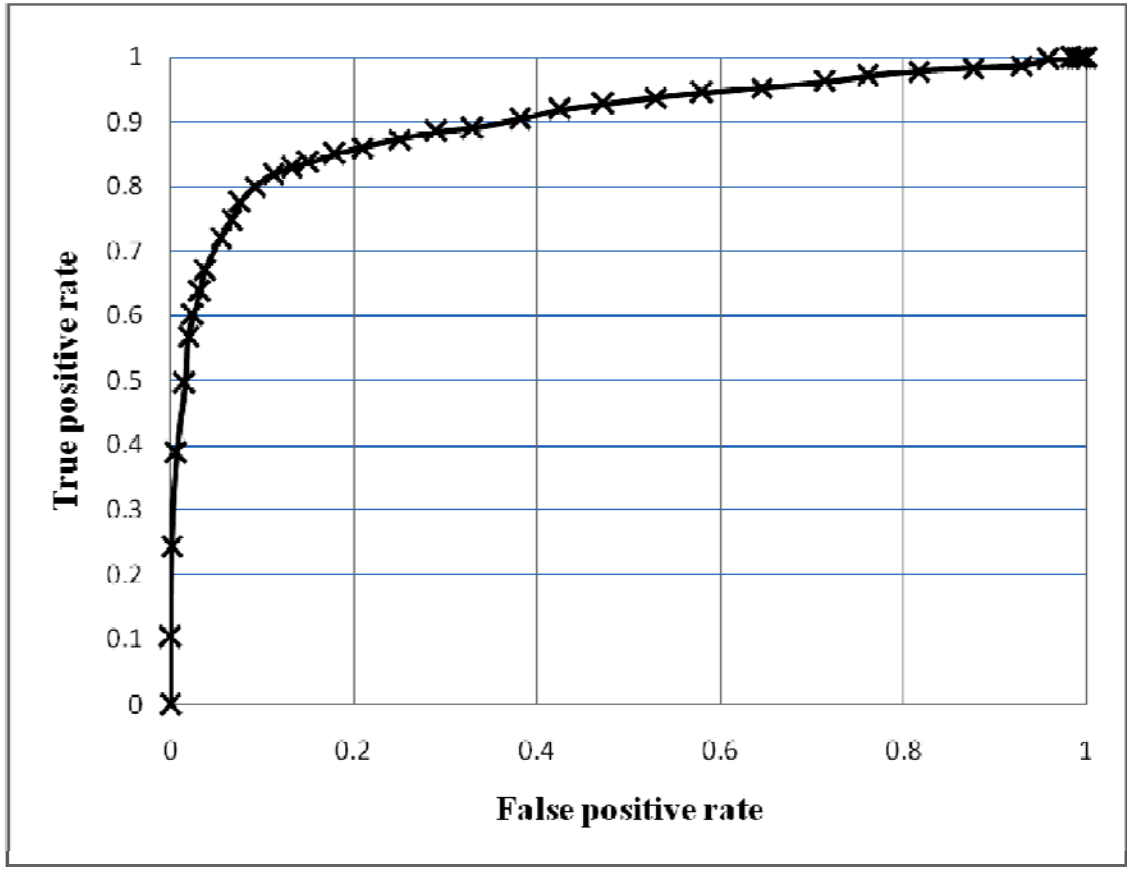
J.B. Speed School of Engineering

IDS Output for Simulated Intrusion



J.B. Speed School of Engineering

ROC Curve for Field-IDS

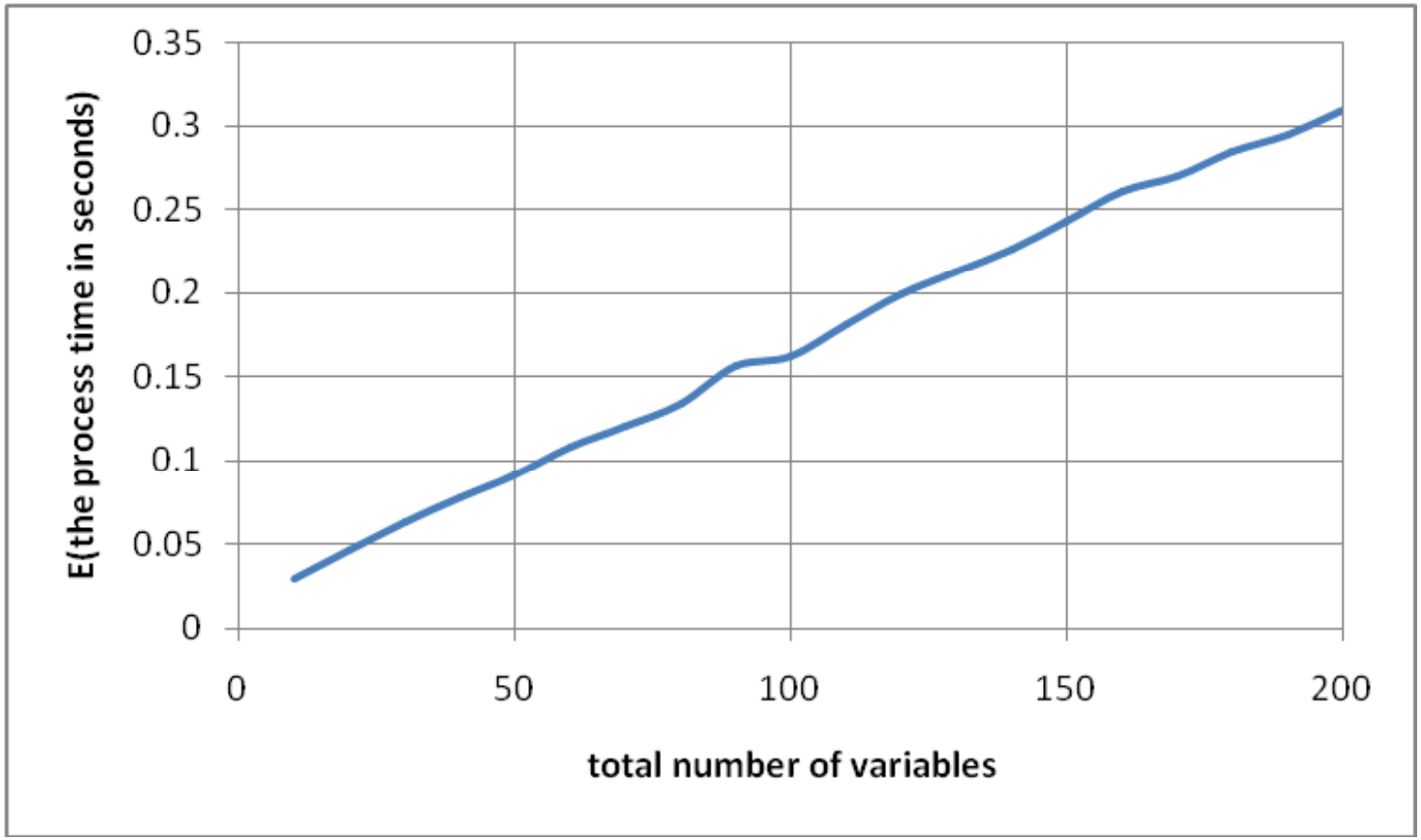


Scalability of FIDS

- FIDS process time depends on the hierarchical structure of levels and groups of process variables.
- For scalability testing purposes, the input data was extended from ten variables to 200 variable.

J.B. Speed School of Engineering

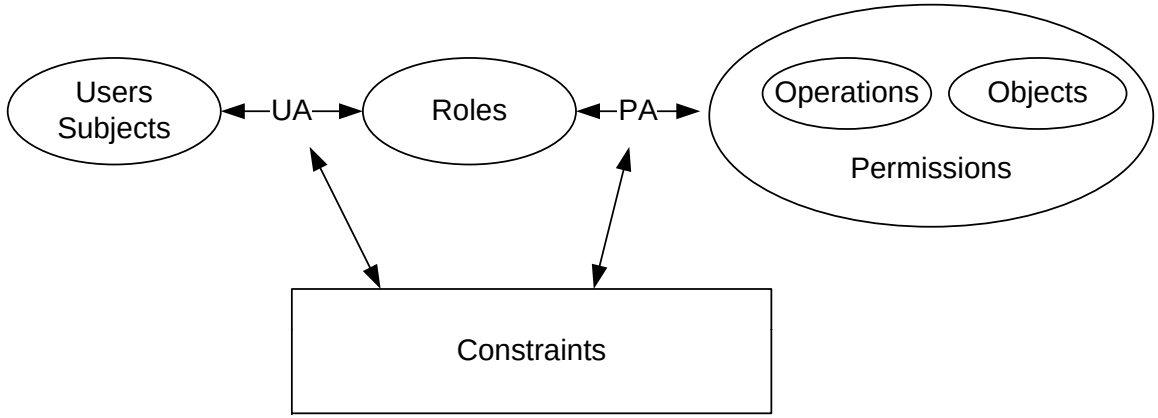
Detection time vs. system size



Security-hardened Field Devices

- Since the control activity takes place as a result of signals sent from the field devices (RTUs, IEDs, etc) it seems reasonable to harden these devices to cyber-attacks
- "Hiding" field devices behind firewalls, encrypted communications, etc. does not solve the security problem for these devices as demonstrated by Stuxnet

Role Based Access Control (RBAC)

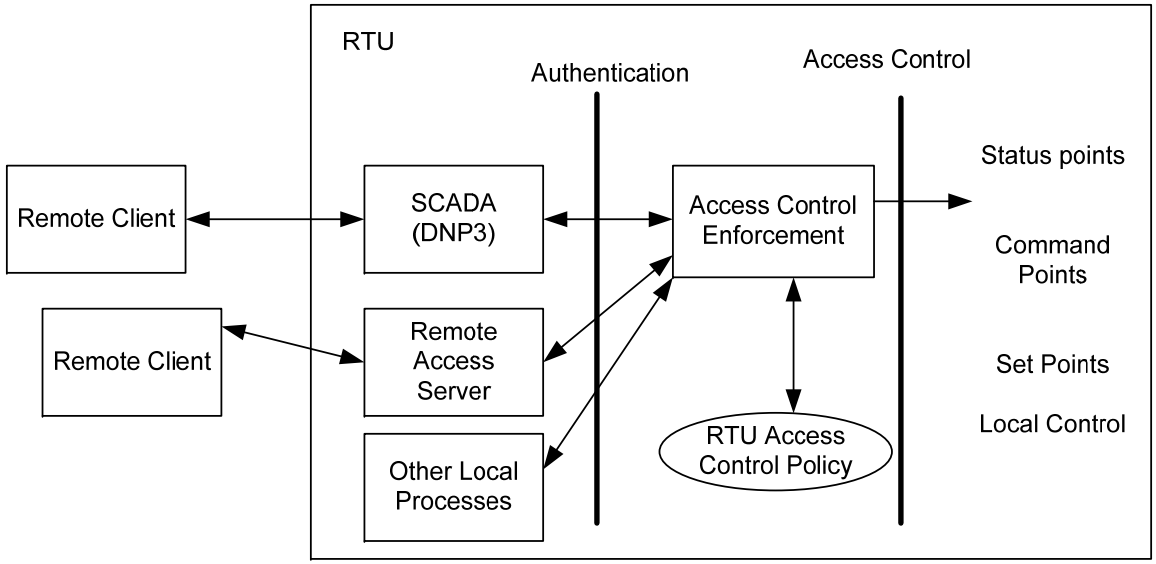


- Sets: Users, Roles, Permissions (operation X object)
- Relations: UA (user assignments), PA (permission assignment).
- Constraints place restrictions on UA and PA
- Types of constraints
  - Static Constraints vs. Dynamic Constraints
  - Endogenous vs. Exogenous
  - Authorization vs. Assignment

J.B. Speed School of Engineering

RTU Access Control: Enforcement

- Security hardening can be achieved by placing enforcement mechanism between all RTU software components and protected resources.
- Operating system mitigates all access to resources
- Most operating systems lack support for RBAC
- Can be implemented in middleware between OS and all RTU software components.



Microkernel Architecture: Hardened RTU

- Isolate critical resource, specifically analog and digital I/O and control algorithms into their own partitions
- Place security enforcement module(s) between "untrusted" network components and isolated critical resources
- Prevent unwanted and undesirable interaction between functional components

Evaluation

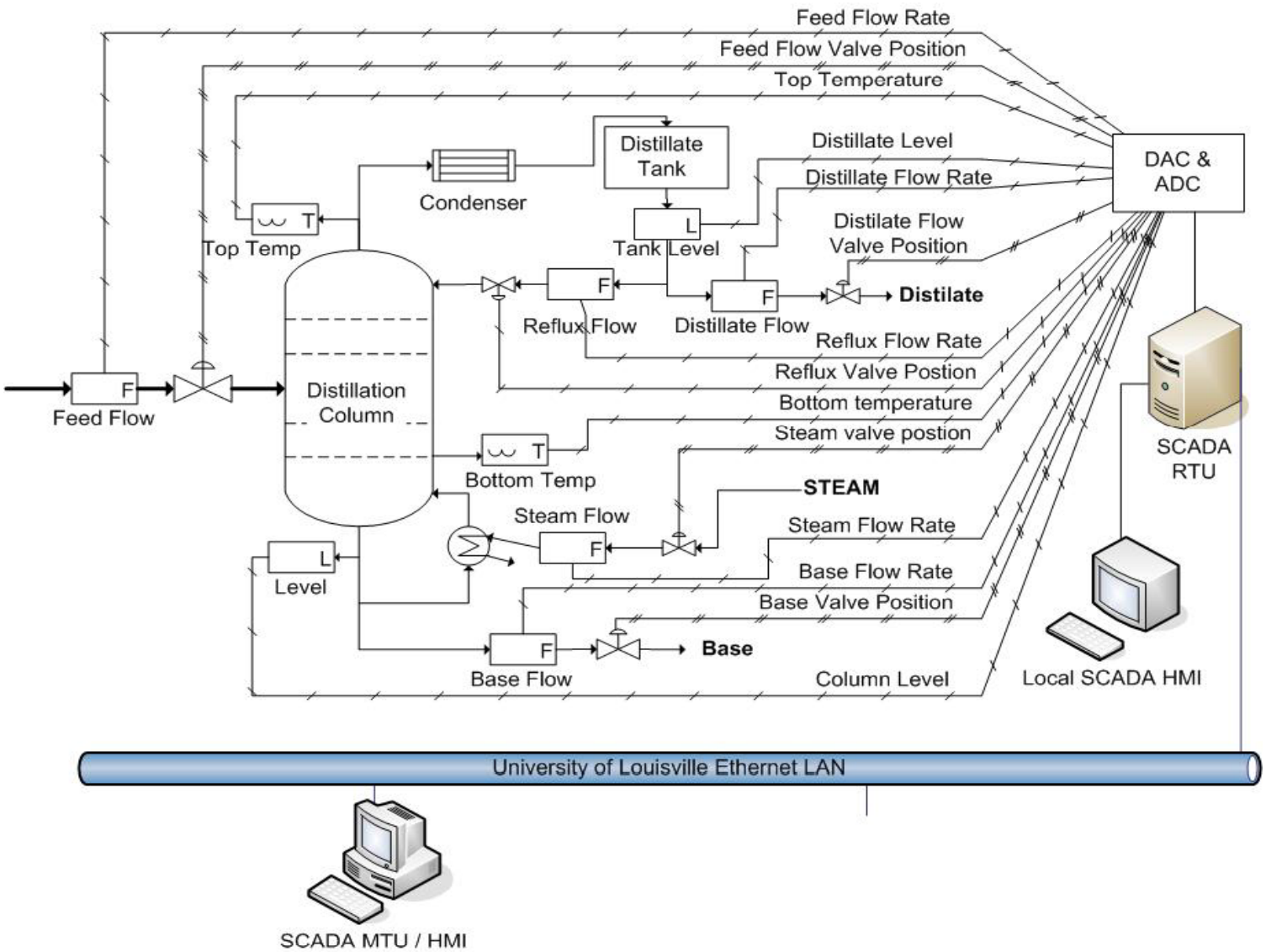
- Used laboratory SCADA implementation to evaluate challenge response authentication and hardened RTU
- Timing results were acceptable for most chemical and water sector applications
- Max of 14% additional overhead for C-R authentication

Unit Operations Lab

SCADA Controlled Distillation Column

J. B. Speed School of Engineering
University of Louisville

J.B. Speed School of Engineering



J.B. Speed School of Engineering

Performance Testing Results

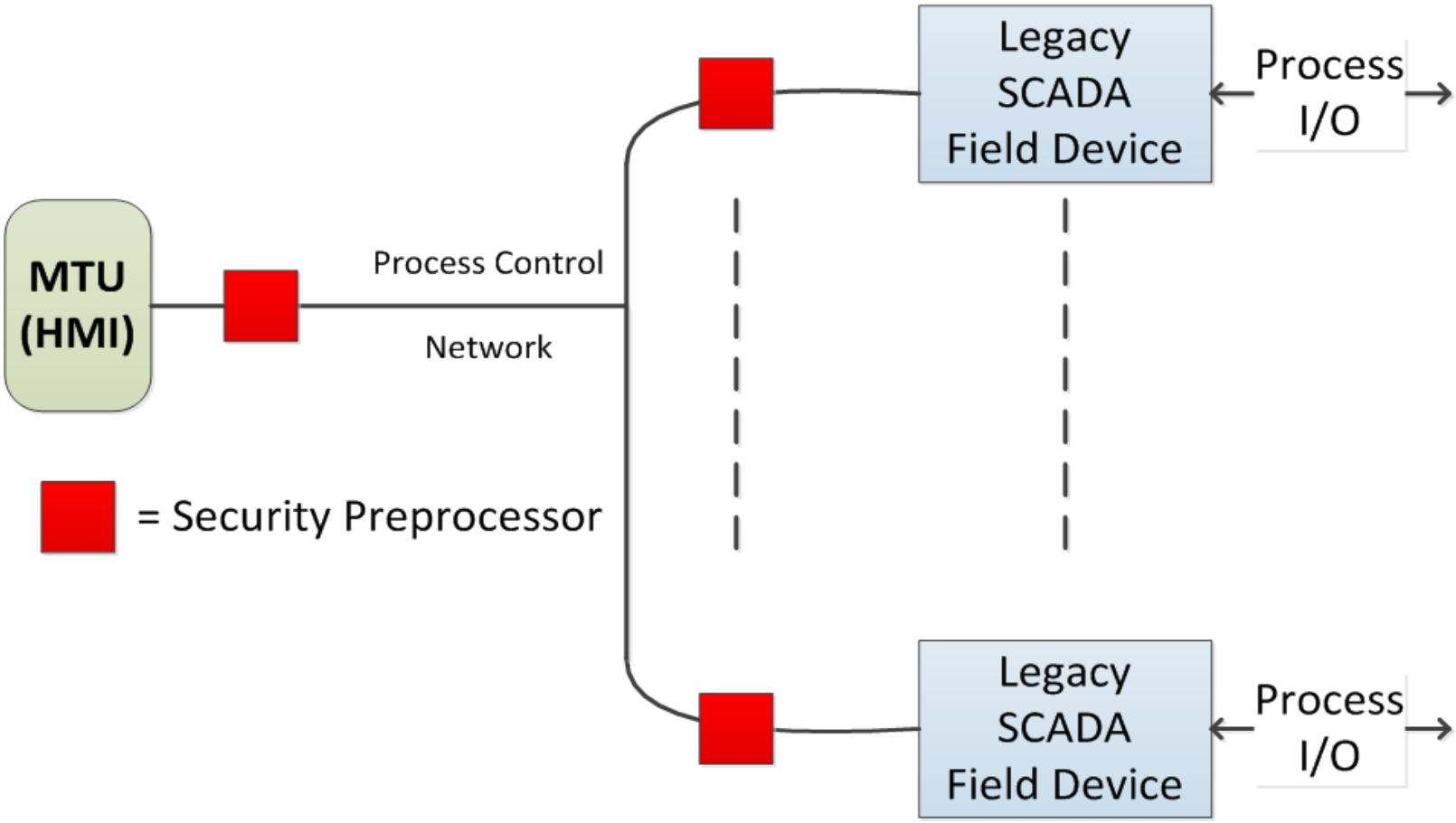
Operation	Response time (ms)
Simple Read (read one analog input point)	49
Simple Write (write one analog output point)	399
Static Data Poll (read all RTU points)	379
Closed Loop (read 1 point write 1 point)	499

Security Pre-processor for ICS Field Devices

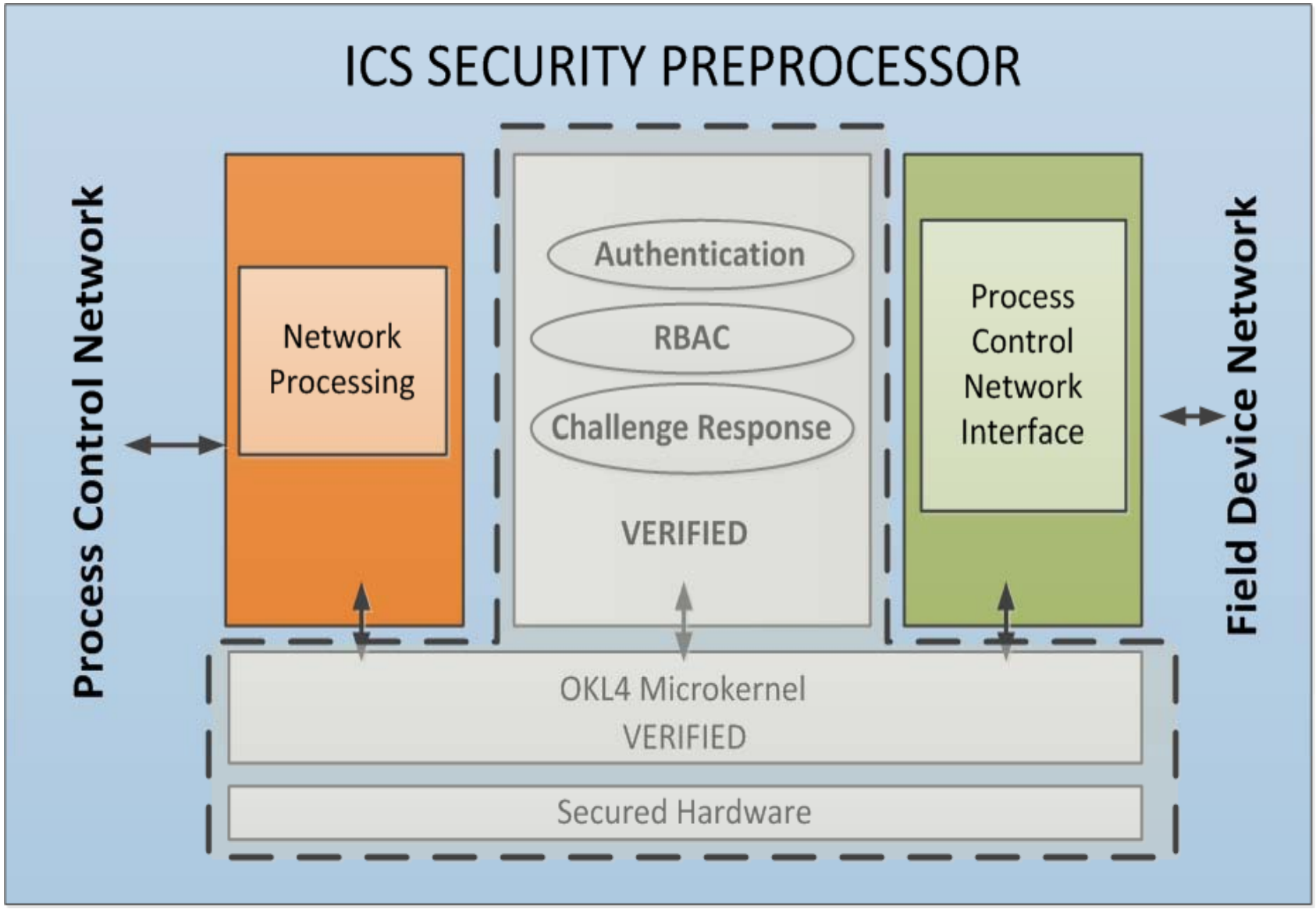
- The hardened field device approach has limitations in legacy systems
- We are currently working to utilize the same technology as an add-on security preprocessor for SCADA systems
- We plan to be forward compatible with the Sandia OPSAID/LEMNOS reference architecture

J.B. Speed School of Engineering

High Security Architecture



J.B. Speed School of Engineering



Security Preprocessor - Features

- Critical components are mathematically verified (EAL-7). All input-output combinations conform to specification – No undefined actions!
- All communications are through the verified microkernel
- Authentication module will be verified as a follow-on to current project

Collaborations and Partnerships

- Developing collaborative proposal with Sandia Laboratories to create enhanced LEMNOS prototypes
- Submitting proposal to Ky Comm. Fund to develop Security Preprocessor brass-board prototypes
- Have also discussed this technology with Honeywell, Microsoft Research, PNNL and Idaho Natl. Laboratories

Conclusions - General

- Despite heightened awareness of cyber-security risks, significant vulnerabilities continue to exist in ICS
- Water systems are an attractive target for terrorist or nation state attacks due to the societal disruption factor
- We should not make the mistake of assuming our enemies will not patiently plan and then attack us at our weakest points

J.B. Speed School of Engineering

Conclusions - Specific

- Increased use of COTS components makes SCADA systems more vulnerable to many common cyber threats as well as SCADA specific threats.
- Network security approaches provide some outer perimeter hardening, but enhanced authentication, field IDS and RTU hardening are needed to add defense in depth
- The prevalence of legacy control systems will continue to be a significant vulnerability in the water sector
- Initial evaluation results of the security preprocessor approach are promising

J. B. Speed
School of
Engineering

Questions ?

Please feel free to contact me at
jhgrah01@louisville.edu
for more information