




TCIP: Trustworthy Cyber Infrastructure for Power

**Secure and Reliable
Computing Base**

Presenters: Sean Smith, Ravi Iyer, and Carl Gunter



TCIP Year 1 Review, December 11, 2006

University of Illinois • Dartmouth College • Cornell University • Washington State University

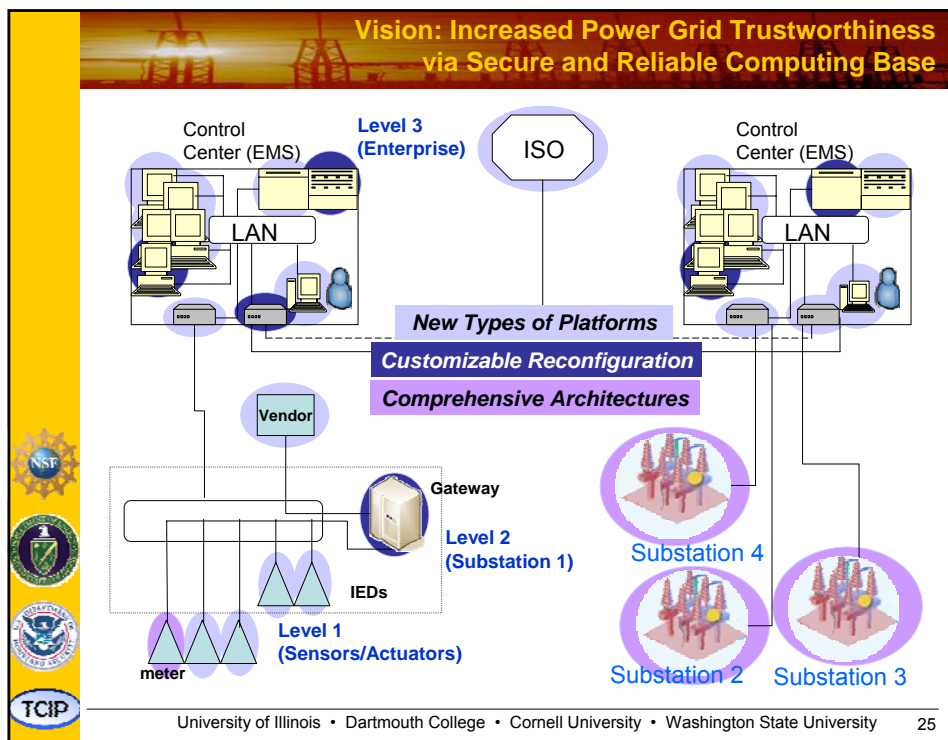
2

Personnel

- **PIs/Senior Staff**
 - George Gross
 - Carl A. Gunter
 - Zbigniew Kalbarczyk
 - Ravi Iyer
 - Pete Sauer
 - Sean Smith
- **Undergraduates**
 - Paul Dabrowski
 - Sanjam Garg
 - Allen Harvey
 - Evan Sparks
- **Graduate Students**
 - John Baek
 - Nihal D'Cunha
 - Reza Farivar
 - Alex Iliev
 - Peter Klemperer
 - Michael LeMay
 - Suvda Myagmar
 - Karthik Pattabiraman
 - Patrick Tsang
 - Jianqing Zhang

University of Illinois • Dartmouth College • Cornell University • Washington State University

24



Area 1 Approach

- **Focus:** Move from *perimeter security* to *platform security* in the power grid cyber infrastructure
- **Focus:** Secure power *infrastructure by ensuring* security of infrastructure *applications*
 - Derive security *requirements* from *application logic*
 - Derive *hybrid solutions* and *constraints* from application context
- **Project Areas:**
 - Build *new types of platforms* to achieve specific security goals for power applications
 - Make these hardened platforms *reconfigurable and customizable*, so one platform secures multiple power applications
 - Integrate hardened platforms into *comprehensive security architectures* for power grid scenarios

Logos on the left side include: NSF, DHS, NIST, and TCIP.

University of Illinois • Dartmouth College • Cornell University • Washington State University 26

Area 1 Projects			
	Hardening Platforms	Reconfigurable Hardening	Application Integration
ISO	DEMO	(future)	(future)
Control Center	poster	poster	(future)
Independent generator	(future)	(future)	(future)
Substation	poster	DEMO	poster
Large customer	(future)	(future)	(future)
Home	(future)	(future)	DEMO

University of Illinois • Dartmouth College • Cornell University • Washington State University 27

Year 1 Accomplishments	
<ul style="list-style-type: none"> • Hardening platforms: <ul style="list-style-type: none"> – Demonstration of automatic tool to secure high-stakes ISO computation against dedicated insiders with physical access <ul style="list-style-type: none"> • Securing large computations with small secure devices. (Kerckhoff's Principle for trusted hardware) • Prototype compiler, host-side code, and secure coprocessor firmware (for now, IBM 4758). – Design and initial prototype of fast, novel crypto for control centers and substations <ul style="list-style-type: none"> • An DSA signing coprocessor that is low-latency, burst-tolerant and physically secure • A Pairing coprocessor that is fast, physically secure and inexpensive – Design and prototype of processor modules: <ul style="list-style-type: none"> • Attack detectors based on information-flow signatures • Error detectors based on selective re-execution of critical instructions • Reconfigurable hardening <ul style="list-style-type: none"> – Customize and implement, into an FPGA, Illinois Reliability and Security Engine (RSE) for substations and control center applications of the power grid infrastructure <ul style="list-style-type: none"> • Configurable hardware framework to deploy application-specific security and reliability modules • Low detection latency, low overhead, and high coverage – Incorporation of attack detectors and error detectors within RSE – Methodology and associated tools for generation of application-specific assertions for runtime detection of malicious and accidental errors in SCADA applications • Application Integration <ul style="list-style-type: none"> – Applied Trusted Computing (TC) and virtualization technologies to develop an attested meter – Analyzed security architecture requirements for relays in substations to understand prospects for individually secured IEDs that can meet timing requirements – Developed a trusted configuration framework and threat analysis for software-defined radios in power grids 	
University of Illinois • Dartmouth College • Cornell University • Washington State University 28	

Project Area: Hardening Platforms

- Example project: How do we protect **high-stakes power computations** against **dedicated adversaries**?
 - Insiders
 - Operator of the machine
 - Physical probing

- Use **Trusted Third Party**

Platform	Hardening Platform	Hardening Platform	Hardening Platform
DEMO	DEMO	DEMO	DEMO
poster	poster	poster	poster
(future)	(future)	(future)	(future)
poster	DEMO	poster	poster
(future)	(future)	(future)	(future)
(future)	(future)	(future)	DEMO

University of Illinois • Dartmouth College • Cornell University • Washington State University

29

Current Platforms Won't Work

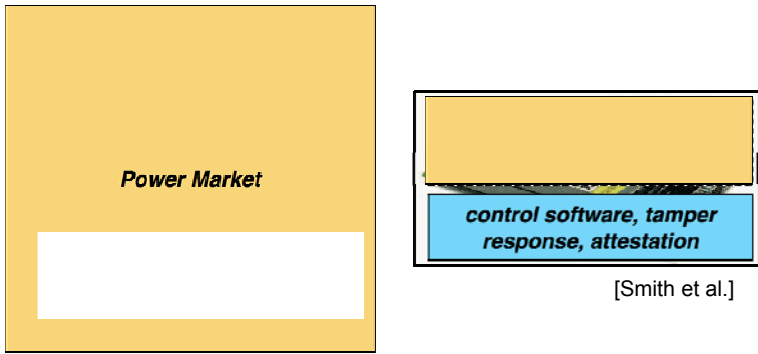
- Standard computer?
- With TPM?

University of Illinois • Dartmouth College • Cornell University • Washington State University

30

Current Platforms Won't Work

- Secure coprocessor?

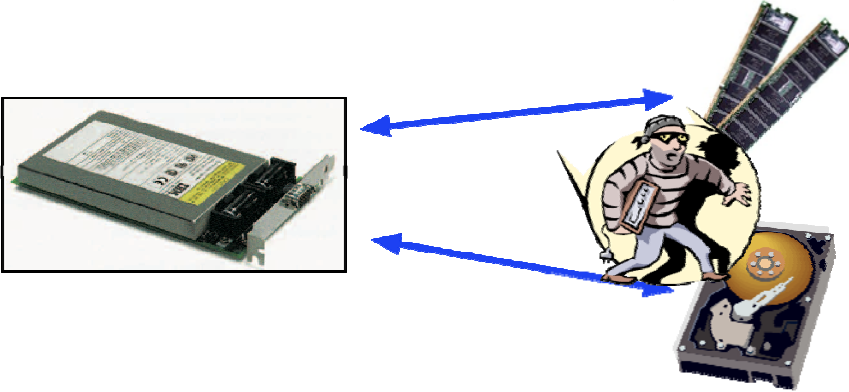


[Smith et al.]

University of Illinois • Dartmouth College • Cornell University • Washington State University 31

Current Platforms Won't Work

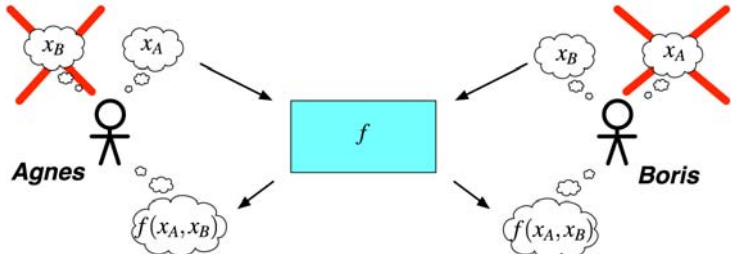
- Secure coprocessor with external resources?



University of Illinois • Dartmouth College • Cornell University • Washington State University 32

Theoretical Techniques Won't Work

- Secure Multiparty Computation




The diagram shows two parties, Agnes and Boris, each with a thought bubble containing their input (x_A and x_B respectively). These inputs are fed into a central function box labeled f . The output of the function is $f(x_A, x_B)$. The inputs x_A and x_B are crossed out with red X's, indicating that the parties do not know each other's inputs directly.

- Fairplay
- Oblivious RAM

University of Illinois • Dartmouth College • Cornell University • Washington State University 33

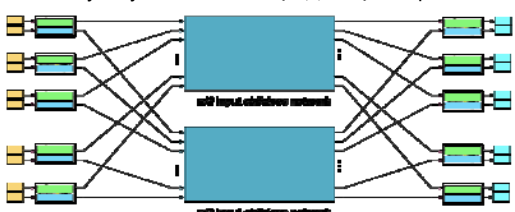
So What Do We Do? Our Previous Tools

- Use **resource-constrained** secure coprocessor in completely new way
 - Like **Kerckhoff's Principle** for computation.
- Encrypted switch.**
 - The adversary only knows: one of $\{C(0), C(1)\}$ was performed



The diagram shows two input boxes on the left connected to a central box. The central box is divided into two sections: 'Our firmware' (green) and 'control software, tamper response, attestation' (blue). The output of the central box is split into two paths, each leading to a different output box on the right.

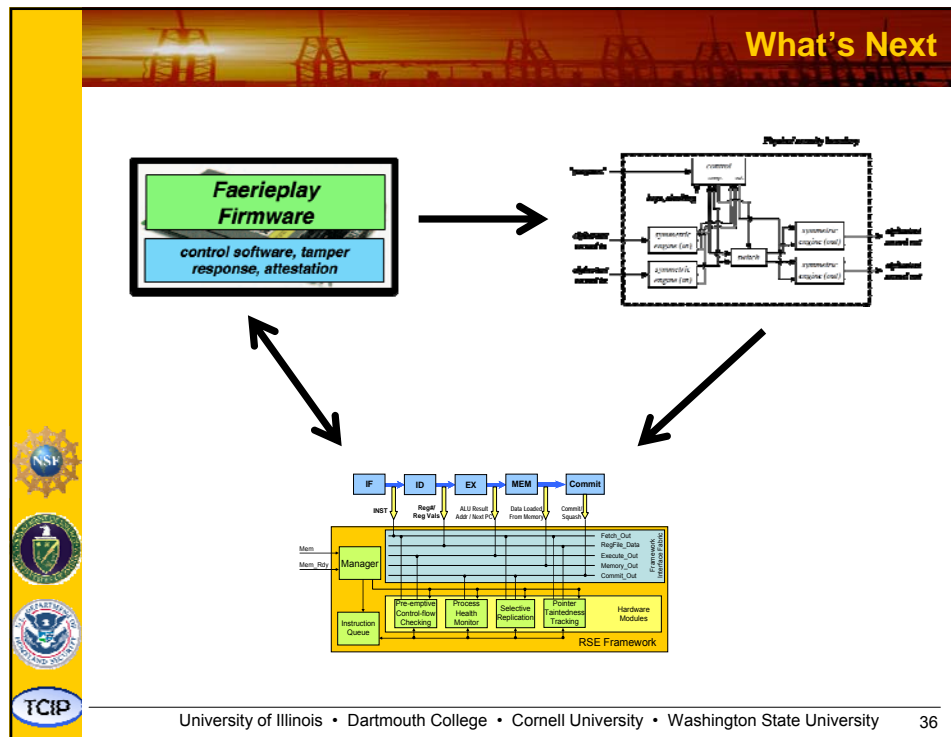
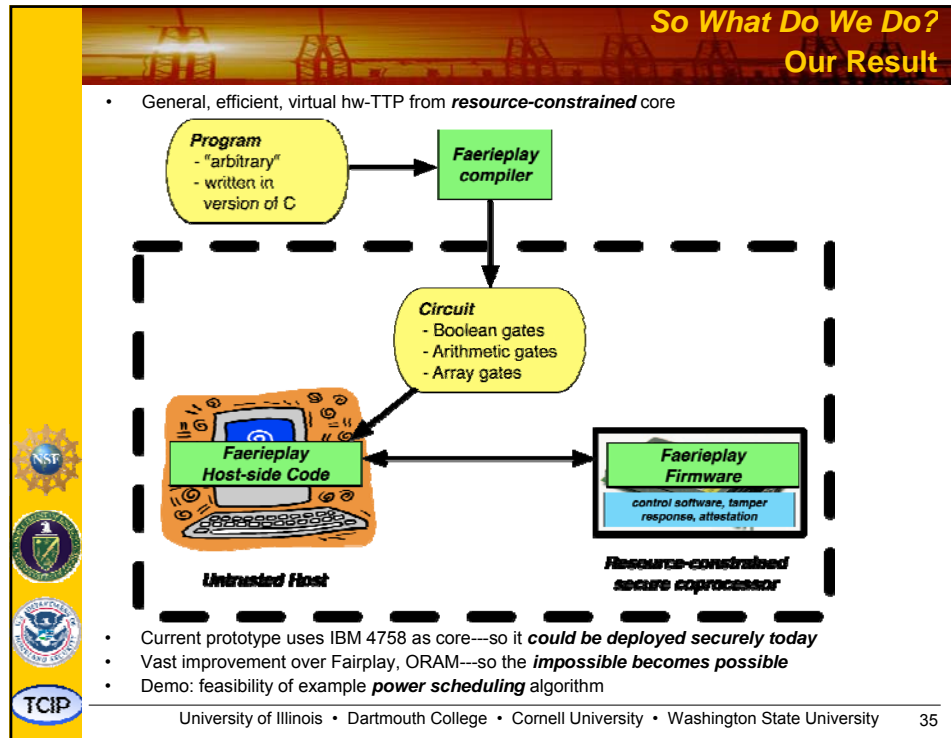
- Opaque Oblivious Networks.**
 - The adversary only knows: one of $\{C(S): \forall S\}$ was performed



The diagram shows a complex network of connections between input and output nodes. The input nodes are on the left, and the output nodes are on the right. The connections are represented by lines that pass through a central area, which is labeled 'opaque oblivious network'.

- Practical Private Information Retrieval**

University of Illinois • Dartmouth College • Cornell University • Washington State University 34








Project Area: Reconfigurable Hardening

- Develop enabling technology to provide customizable level of trust (security and reliability) to a SCADA applications/systems

	Hardware	Software	Application
Control Center	DEMO	(future)	(future)
Gateway	poster	poster	(future)
Substation	(future)	(future)	(future)
IEDs	poster	DEMO	poster
SCADA	(future)	(future)	(future)
Other	(future)	(future)	DEMO



- Explore an integrated approach which involves:
 - A compiler assisted automated generation of application-specific assertions for runtime security protection and error detection
 - Transformation of the derived assertions into runtime checks
 - Implementation of application-specific checks on configurable FPGA-based hardware
 - Demonstration on application scenarios representative of SCADA systems

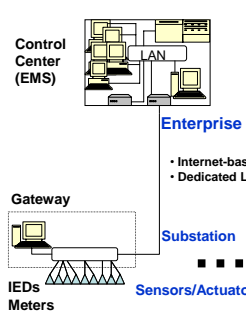
University of Illinois • Dartmouth College • Cornell University • Washington State University






37

Application Scenario

- Goal:** Ensuring integrity of data reflecting current/past system state to enable informed control decisions to be made in the context of the power grid
- Data Source:** Intelligent electronic devices (IEDs) in a substation-level collect/report sensor information on the system status
- Data storage and processing**
 - Gateway (e.g., network terminal unit) acquires, aggregates, and sorts the data for higher level analysis by a SCADA-master
 - Gateway is an electrically hardened industrial computer running Windows XP or Linux and a SQL-like database
- Security protection**
 - Pointer-taintedness** technique to detect malicious tampering with the application which processes the data
 - Reliability and Security Engine**, a hardware framework to integrate and demonstrate developed techniques on SCADA-like systems
 - e.g., computer system with capabilities similar to a gateway in a power grid settings



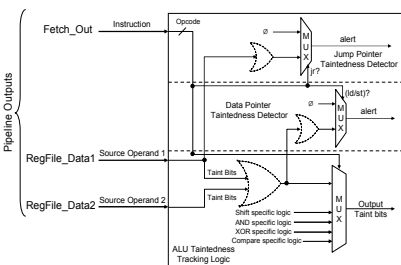






University of Illinois • Dartmouth College • Cornell University • Washington State University

38

Application-Aware Trust: Generation of Security Checks Pointer Taintedness Detection

- Many vulnerabilities (> 66%) due to pointer taintedness
 - a pointer value is derived directly or indirectly from user input
- Pointer Taintedness Tracking and Detection
 - detects malicious memory corruption
 - a **taintedness bit** added to each memory location
 - data received from external sources (e.g., network, keyboard) are marked tainted
 - Performs two operations:
 - tracking the propagation of taintedness bits
 - detecting the dereference of tainted pointers



University of Illinois • Dartmouth College • Cornell University • Washington State University 39

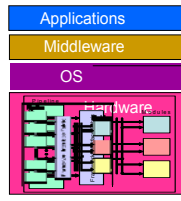
Application-Aware Trust: Generation of Security Checks Information-Flow Signatures






- Use detection of **program data-flow violations** as an indicator of malicious tampering with the system
 - prevent an attacker to exploit disconnect between source-level semantics and execution semantics of the program
- Security critical** variables chosen based on app semantics
- Employ a compile-time static program analysis to
 - extract a backward slice which collates all dependent instructions along each control-path
 - form a signature, which encodes dependences as a set (or sequence) of instruction PCs along each control-path
- Compute runtime signatures for each critical variable
 - trusted bit** associated with each instruction
 - only trusted instructions can update runtime signatures
 - check signatures for instructions with trusted-bit set

University of Illinois • Dartmouth College • Cornell University • Washington State University 40

Application Aware Trust: Support at Architectural Level

- **Illinois Reliability and Security Engine (RSE)**
 - Reconfigurable processor-level hardware framework to support security and reliability
- **Security Support**
 - Pointer Taintedness Module: **protects against malicious tampering with data used by application**
- **Reliability Support**
 - Infinite Loop Hang Detection Module: **protects against infinite program execution hangs**
- **Implementation**
 - FPGA-based **trusted coprocessor** which integrates: **superscalar DLX core**, RSE framework, and RSE hardware modules
 - Communication over PCI Bus with host computing system

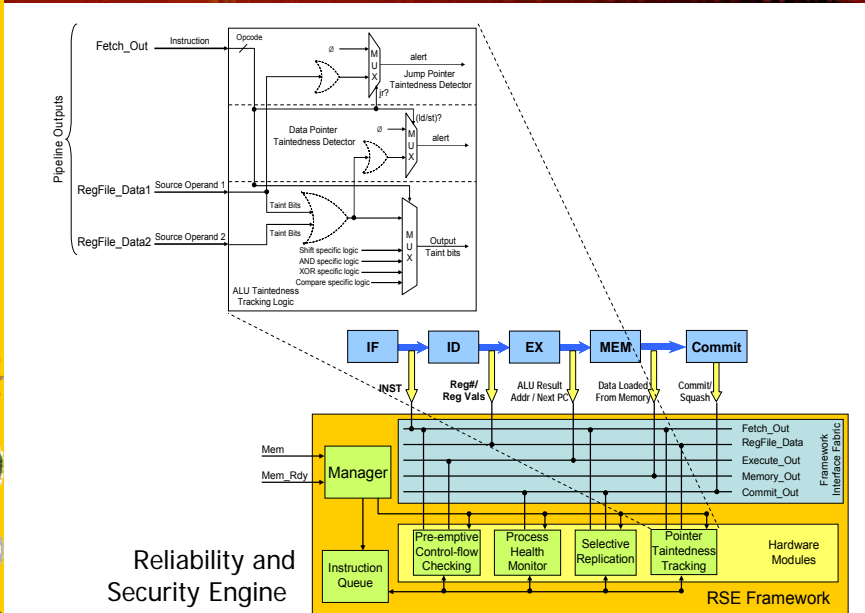













University of Illinois • Dartmouth College • Cornell University • Washington State University

41

Implementation: RSE with Pointer Taintedness Tracking and Detection Module



University of Illinois • Dartmouth College • Cornell University • Washington State University

42

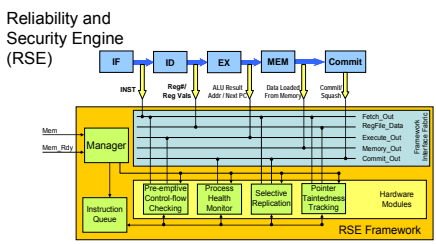
Experimental Testbed

- Part of Power Cyber Infrastructure Laboratory
- Network consisting of computing nodes and power-grid specific devices (e.g., RTUs)
- Develop attack/fault models corresponding to front-end systems (control centers), RTUs, and IEDs
- Experiment and test
 - presence of security vulnerabilities
 - application/system resilience to security attacks and random errors
 - techniques for run-time protection
 - hardware approaches, e.g., programmable hardware
 - software methods, e.g., executable assertions
- Identify services provided by reliable and secure computing base to upper levels, e.g., runtime monitoring, data audit, and secure connection and authentication


University of Illinois • Dartmouth College • Cornell University • Washington State University 43

What's Next

Explore integration of RSE with embedded processors used in low-end devices of the power grid, e.g., ARM microprocessor



Trusted processing








- Advance electronic utility meters
- Intelligent electronic devices
- Network terminal units

University of Illinois • Dartmouth College • Cornell University • Washington State University 44

Project Area: Application Integration


- Important devices in the EMS must be **individually secure**: IEDs, meters, etc.
 - Meters too widely dispersed to protect with security perimeter
 - IEDs in substations may benefit from Internet connections
- Goal:**
 - Develop comprehensive security architectures for power devices
 - Fundamentally advance important areas of operating system and network security
 - Authentication and access control
 - Real-time security
 - Trusted Computing
- Projects:**
 - Advanced Meters
 - Relays

	Hardware	Software	Application
Hardware	DEMO	(future)	(future)
Software	poster	poster	(future)
Hardware	(future)	(future)	(future)
Software	poster	DEMO	poster
Hardware	(future)	(future)	(future)
Software	(future)	(future)	DEMO






University of Illinois • Dartmouth College • Cornell University • Washington State University

45



Project: Attested Meter

- Problem:** *Advanced Meters* exhibit a number of security and privacy vulnerabilities
- Objective:** Create a secure, private, and extensible architecture for future advanced meters
- Approach:** *Attested Metering*: Apply existing *Trusted Computing (TC)* and *virtualization* technology to secure Advanced Metering network communications and computation


University of Illinois • Dartmouth College • Cornell University • Washington State University





46

Advanced Metering Infrastructure (AMI)

Advanced meters are electronic utility meters with bidirectional network connections to a *Meter Data Management Agency* (MDMA)

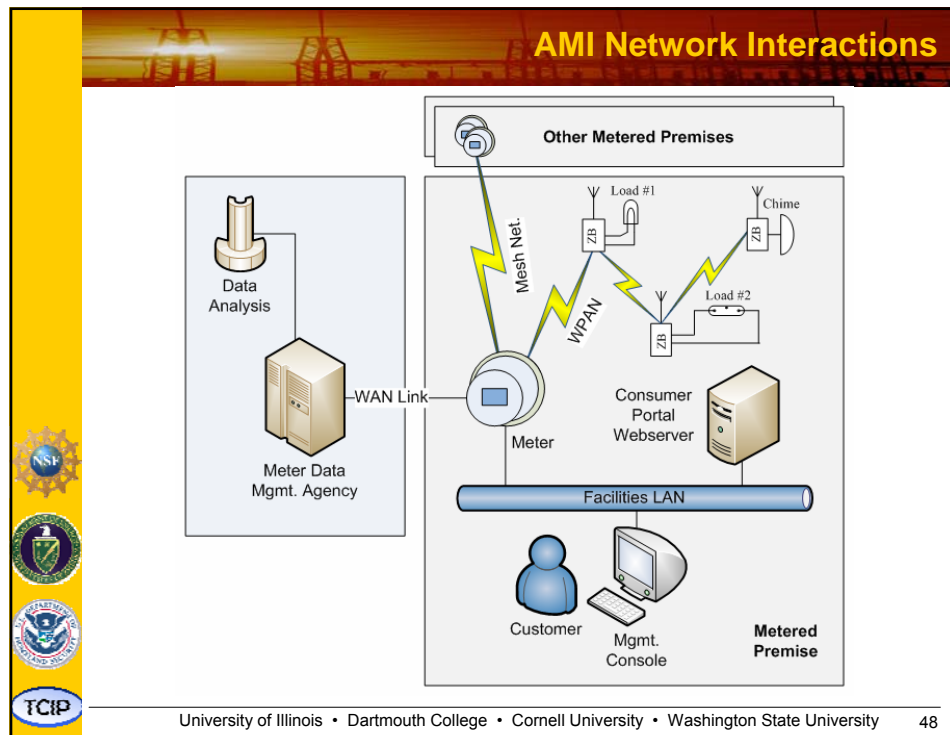
- **Network types:**
 - RF wireless (ZigBee/802.15.4, Wi-Fi/802.11, proprietary)
 - Power-Line Communication (PLC)
 - Broadband over PowerLines (BPL)
 - Cellular (CDMA, GSM)
 - Phone line
- **Benefits:**
 - Reduced cost
 - Improved reliability
 - Demand response
 - Customer control
- **Security state of the art:**
 - Shared key encryption
 - Security by obscurity
 - No security at all.
- **Standards: ANSI C12**







University of Illinois • Dartmouth College • Cornell University • Washington State University

47



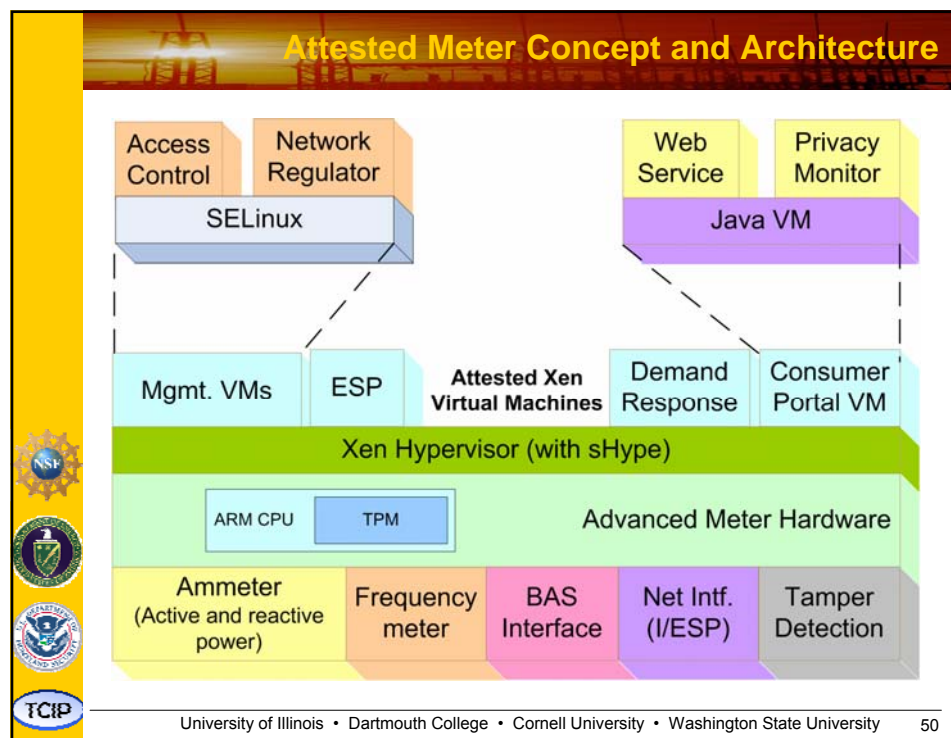
Partial AMI Threat Model


- **Unethical customer**
 - May attempt to modify metering messages to steal service
- **Overly-intrusive MDMA**
 - Could use high-resolution metering data to determine behavior of metered residents
- **Active attacker**
 - Wants to destabilize grid or cause blackout
 - Could directly attack remote disconnect function on many meters to disconnect homes and businesses






University of Illinois • Dartmouth College • Cornell University • Washington State University

49





Research Plan

- Develop C12 prototype implementation with increasingly realistic hardware and feature-rich software based on attested meter concept
- Develop mesh technology for AMI that integrates with platform security objectives and enables new applications
- Target achievements
 - Advanced platform demonstration
 - Model for security developed with parties involved in procurement, sales, and standards development













University of Illinois • Dartmouth College • Cornell University • Washington State University

51



Project: Secure Relay

- Problem:** Relays have limited security currently and rely on perimeters, but this limits convenience and security
- Objective:** Develop a technology for individually secure relays in substations
- Approach:** Real-time Security network architecture and platform


University of Illinois • Dartmouth College • Cornell University • Washington State University






52



Relays


- **Relay IED**
 - Networked computer that detects defective lines or apparatus or other power system conditions of an abnormal or dangerous nature and initiate appropriate control circuit action
- **Security state of the art**
 - Shared passwords for different security levels: user, breaker, administrator
 - Isolation and VPN perimeter protections
- **Standards: IEC 61850**
 - Defines how devices in the substation should interact, and also provides system requirements that support all substation automation functions
 - Extensible set of substation functions



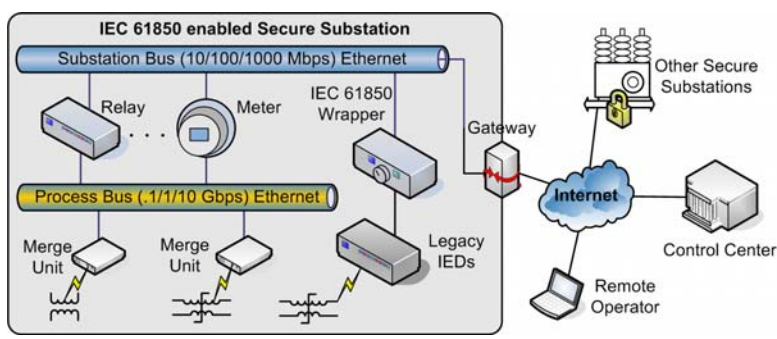






University of Illinois • Dartmouth College • Cornell University • Washington State University






53



Substations




- IEC61850-enabled IEDs get digital power grid condition data via process bus and merge units
- IEDs communicate with each other using substation bus
- Legacy devices use IEC61850 wrapper





University of Illinois • Dartmouth College • Cornell University • Washington State University

54




Secure Relay Concept

- Current IED security is insufficient for internet-exposed devices
- Limits to perimeter defense
 - Often violated by current systems because of complex network topology, convenience, human error, etc.
 - Perimeters lack application knowledge of devices
 - Missed opportunity to provide additional
 - Convenience (e.g. updates)
 - Reliability (e.g. Internet as backup)
 - Defense in depth (protection beyond perimeters)
- Challenges
 - Very high level of individual security required
 - Must provide real-time guarantees beyond current COTS security software thresholds










University of Illinois • Dartmouth College • Cornell University • Washington State University 55



Research Plan

- Develop real-time security
 - Real time (temporal) access control of IEDs
 - Analyze timing constraint issues for secure communication between IEDs
- Develop secure relay platform for advanced substation network architecture based on a simple implementation of IEC 61850
- Target achievements
 - Deploy software patches over network while preserving security and real-time guarantees
 - Intrinsic DoS resistance despite Internet attachment

University of Illinois • Dartmouth College • Cornell University • Washington State University 56