Focus Area: Secure and Reliable Computing Base

Presenter: Sean Smith, Dartmouth College

TCIP Industry Day
October 17, 2007

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

Personnel

- PIs/Senior Staff
  - Sergey Bratus (Dartmouth)
  - George Gross (UIUC)
  - Carl A. Gunter (UIUC)
  - Zbigniew Kalbarczyk (UIUC)
  - Ravi Iyer (UIUC)
  - Pete Sauer (UIUC)
  - Sean Smith (Dartmouth)
- Alumni
  - Nihal D'Cunha (M.S., Dartmouth)
  - Allen Harvey (B.A., Dartmouth)
  - Evan Sparks (B.A., Dartmouth)
- Graduate Students
  - John Baek (Dartmouth)
  - Paul Dabrowski (UIUC)
  - William Healy (UIUC)
  - Alex Iliev (Dartmouth)
  - Peter Klemperer (UIUC)
  - Michael LeMay (UIUC)
  - Suvda Myagmar (UIUC)
  - Karthik Pattabiraman (UIUC)
  - Ashwin Ramaswamy (Dartmouth)
  - Patrick Tsang (Dartmouth)
  - Jianqing Zhang (UIUC)
- Undergraduates
  - Justin Deinlein (UIUC)
  - Alex Latham (Dartmouth)
- High School
  - Axel Hansen (Dartmouth)

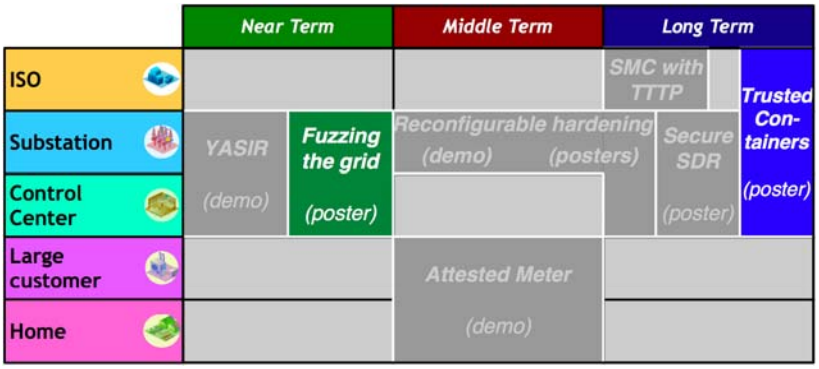
University of Illinois • Dartmouth College • Cornell University • Washington State University

Base Area 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***
- *Project Approach*:
  - ***Identify***: security problems in near-term, middle-term, long-term power grid cyber infrastructure
  - ***Secure***: apply ***current security technology*** into base devices, as well as ***developing new security technology*** and applying it
  - ***Deploy***: evaluate solutions in testbed grid scenarios
- *New Thrust (from last year):*
  - Develop vertical links into protocols group

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

Base Area Projects



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

1. Fast Crypto for SCADA

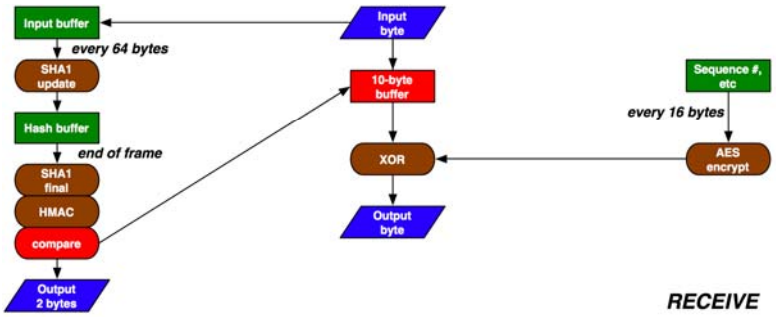
(near-term deployability)

- ***Identify:***
  - Communications between SCADA devices susceptible to ***eavesdrop, modification, replay***
  - …but need to have ***low latency***
  - A ***bump-in-the-wire (BITW)*** approach adds security without replacing entire infrastructure
  - Existing BITW approaches do not provide high security ***integrity*** with low latency
- ***Secure:***
  - YASIR: a BITW with high security integrity and low latency, for legacy SCADA
  - (and some public key results too)
- ***Deploy:***
  - Initial proof-of-concept hw

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

YASIR: Yet Another Security Retrofit

- ***BITW*** for legacy SCADA
- High security
  - ***Data integrity***, optional data confidentiality
  - ***80-bit*** security level
  - ***Strong attacker model***
- Prototype:
  - Modbus/ASCII, Modbus/RTU, DNP3
  - IEC 60870-5
- ***Low latency***:
  - ≤ 18 byte-times,
  - irrespective of message length
- Builds on Wright et al's trick:
  - BITW receiver transforms integrity failure
  - …to CRC error, flagged by SCADA
- NIST-standardized, patent-free crypto
  - HMAC, SHA-1, AES-CTR
- Formal security analysis



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

Our Contribution

Approach	Bump-in-the-wire?	Confidentiality?	Integrity?	Security Level	Latency (byte-times)
SEL 3021-1	Yes	Yes	*No* ☹	High	Low (5)
SEL 3021-2	Yes	Yes (option)	Yes	High	*High* ☹
AGA12/Cisco, PE-mode	Yes	Yes (option)	Yes	*Low* ☹	Low (~32)
AGA12/Cisco, other modes	Yes	Yes (option)	Yes	High	*High* ☹
PNNL SSCP BITW	Yes	Yes (option)	Yes	High	*High* ☹
PNNL SSCP embedded	*No* ☹	Yes (option)	Yes	High	Low (<10)
YASIR (our approach)	Yes ☺	yes (option) ☺	Yes ☺	High ☺	Low (≤18) ☺

- Part of research into more general problem of securing communications despite resource constraints
  - Batch paring delegation (e.g., for ECC public key)
  - Secure crypto precomputation with insecure memory (e.g., for DSA signatures)

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

2. Attested Meters: Security Architecture for Advanced Meters

(middle-term deployability)

- ***Identify:***
  - ***Advanced Meters*** enable advanced functionality
    - Remote measurement
    - Demand response and demand control
    - Improved monitoring and control for the grid
  - But computation leads to ***security and privacy vulnerabilities***
- ***Secure:***
  - Create a secure, private, and extensible architecture for future advanced meters
  - ***Attested Metering***:
    - Apply ***trusted computing (TC)***
    - and ***virtualization***
    - to secure Advanced Metering network communications and computation (ANSI C12, ZigBee)
  - …and develop new, lightweight trusted computing technology for the special case of meters
- ***Deploy:***
  - Initial prototypes, industry discussions

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

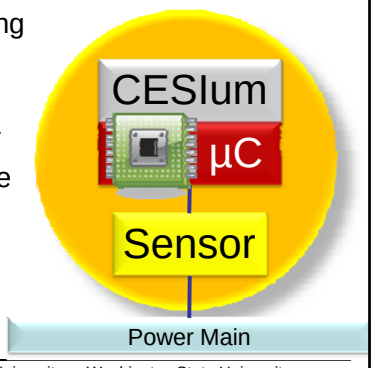
New Architectures

- New functionality: ***emergency-response networking over mesh-connected advanced electric meters***
  - After Katrina, surveillance camera mesh was only network infrastructure to survive.
  - It was retasked to carry municipal communications.
  - Advanced meters with mesh networks will soon be widely deployed, why not use them?
    - Use secure distributed consensus protocol to determine when network should switch into emergency-response mode
  - Meters already include battery backup for outage notification…
- Our previous results: countermeasures against…
  - ***Unethical customer***
    - May attempt to modify metering messages to steal service
    - Has legitimate physical access to meter, could modify it
  - ***Overly-intrusive MDMA:*** Could use high-resolution metering data to determine behavior of metered residents
  - ***Publicity seeker:*** Cracker or virus author seeking physical disruption to garner publicity

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

New Platforms

- Hardware-assisted ***embedded attestation*** scheme:
  - ***Continuous Embedded System Integrity Using Remote Firmware Attestation (CESIum)***
  - Much simpler than TPM
  - Maintains a log of all firmware revisions installed on a microcontroller
  - Provides the complete log during remote attestation operations
  - Main advantages:
    - Simplicity = low cost, power
    - Complete record of firmware revisions, not just current firmware like TPM
    - Not heavily dependent on OS correctness



University of Illinois • Dartmouth College • Cornell University • Washington State University 10

3. Reconfigurable Hardening

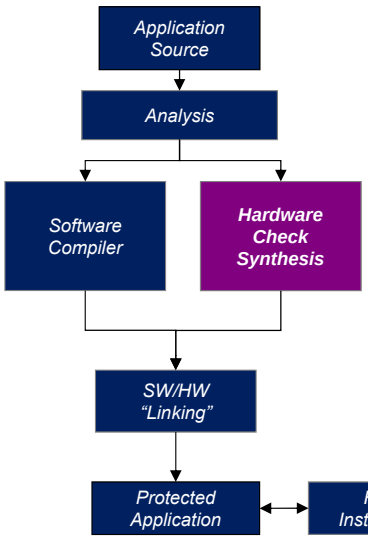
(middle-term and longer)

- ***Identify:***
  - Security vulnerabilities due to hardware or software flaws pose a significant hazard to power grid applications.
  - Application and OS sw has long history of vulnerabilities
  - Patching applications and OS (or replacing hardware) difficult in power grid settings
- ***Secure:***
  - Build application-aware security and reliability solutions ***into the underlying hardware itself***
  - Make it ***reconfigurable***, to allow evolution and customization
  - Result: ***intrusion tolerance for critical infrastructure***
- ***Deploy:***
  - SEL 3351 Data aggregator and SEL 421 Relay.

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

Approach

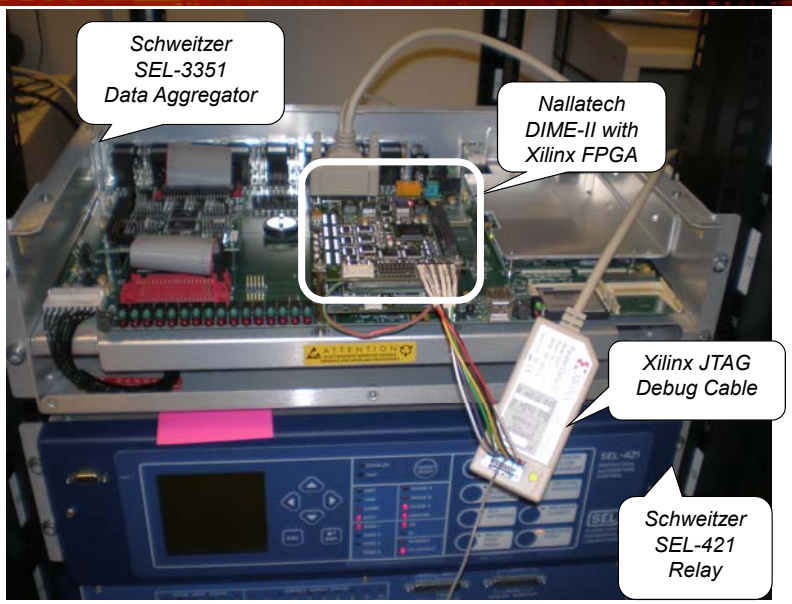
(Automated Design Flow)



- Explore ***processor level solutions*** to achieve low-cost, high-performance, scalable security and reliability checking in the same framework
  - ***small footprint techniques*** that do not require large amount of extra hardware or software
- Automated End-to-End Compilation Framework for checks derivation – from *C-program* to *FPGA Hardware*
- Enhanced compiler transforms checks to VHDL hardware description for synthesis
- Integration with **Reliability and Security Engine (RSE)**:
  - RSE in the pipeline of the DLX and LEON3 processors (poster)
  - Prototyped on FPGA-based hardware
  - Low performance overhead (2%) demonstrated on embedded benchmarks

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

Demo: Real SCADA Protected with RSE

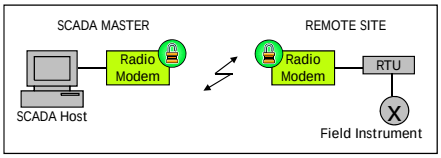


University of Illinois • Dartmouth College • Cornell University • Washington State University

4. Secure Software-Defined Radio in Power Grids

(long-term deployability)

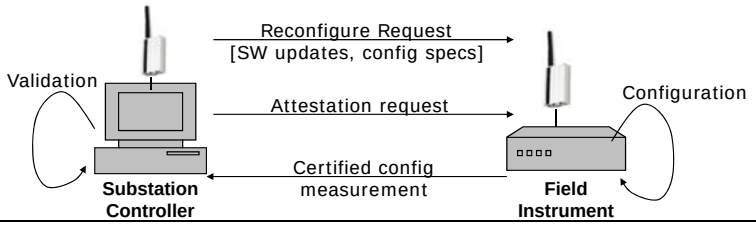
- ***Identify:***
  - ***Communication lines*** needed for SCADA, special protection schemes
    - Installing fixed lines is expensive, time-consuming
    - Preferred wireless technologies may change over time
  - ***Software Defined Radio (SDR)*** can address these problems
    - ***Interoperability*** among various wireless technologies
    - ***Over-the-air download*** of new protocols
    - Fast, ***seamless transition*** between technologies
  - But ***configurability*** leads to security and reliability problems!
- ***Secure:***
  - ***Automated reliable configuration***: policy-driven configuration of specs into an executable code of radio modules
  - ***Conformance:*** verify the conformance of the radio configuration with regulatory policies (FCC regulations, network provider policies, HW specs)
  - ***Integrity, Validity:*** attest validity and integrity of software configuration to a remote party (Substation controller validate field instruments)
- ***Deploy:***
  - Initial framework completed



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

Approaches to Main Challenges

- **Mapping configuration specs** into an executable component composition
  - Provides ***automated, correct reconfiguration***
  - 2 step graph mapping: high-level requirement policies to functional graph, functional graph to executable graph of components (DSP modules)
- **Verifying the conformance** of the radio configuration with regulatory policies
  - Ensures the device is ***operating within allowed frequency band, at acceptable power level***
  - Check input parameters and output properties of DSP modules, against regulatory policies
- **Attesting the validity and integrity** of radio configuration
  - Proves configuration performed by an ***authorized process***, the configuration hasn't changed without permission (***Integrity***)
  - Radio device bootstrapped with the device's public/private key pair
  - Bottom up certify hardware, OS, radio software using TPM



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

5. Fuzzing the Power Grid

(new project; near-term)

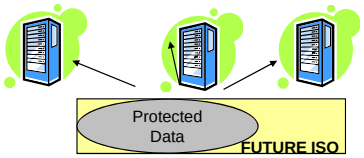
- ***Identify:***
  - Embedded devices in power SCADA implement complex protocols
  - Current and emerging network connectivity increases risks of exposing these interfaces to adversaries
  - Generically… embedded networked devices, protocols and implementations have holes
- ***Secure:***
  - Adapt standard ***fuzzing*** (and other hacker techniques) to automatically probe for these holes
    - Modbus, 61850, DNP, GOOSE, QNX…
  - ***Requirement discovery*** for new Base Area work
  - Help evaluate solutions
- ***Deploy:***
  - Initial framework

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

6. Scalable, Auditable, High-Assurance Containers

(emerging research, new to TCIP; long-term)

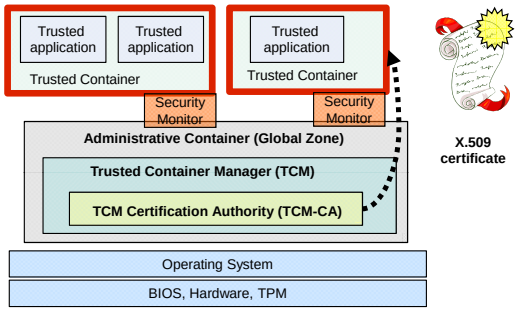
- ***Identify:***
  - The need for ***high assurance*** computing environment for information sharing and dissemination at ISO during power emergency
  - How can we meet different security and information flow policies of different control centers at the same time in a scalable manner?
  - Is it possible to create and attest a trusted environment ***with minimal overhead and constraint?*** And do ***fine-grained auditing?***
- ***Secure:***
  - Design and implement secure computing base for on-demand provisioning of scalable, high assurance, auditable, trusted environments
- ***Deploy:***
  - Implement a prototype for future ISO emergency data dissemination



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

Approach

- Implement **Trusted Containers on Demand** using fast OS-level "paenevirtualization" containers ***based on remote requirements of control centers***
- Implement fine-grained dynamic monitoring (intrusion prevention) and auditing (intrusion detection) of containers using Solaris Dtrace
- Implement outbound authentication for fast verification using TPM and X.509 certificate



- http://www.opensolaris.org/os/project/tpm

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

7. Base Area Accomplishments Last Year

Theory:
- CESIum theory of operation
- Network provisioning protocol for emergency-response networks based on retaskable network infrastructure
- Proof of security properties for YASIR
- Proof of security properties for precomputation memory proxy
- Proof of security properties for batch pairing delegation
- Threat model for SDR

Protocols:
- YASIR low-latency, high-security BITW
- Batch pairing delegation
- Precomputation with insecure memory
- Designed a new protocol for scalable, on-demand trusted computing using Solaris zones, dtrace, ZFS, and TPM
- Trusted configuration framework for SDR

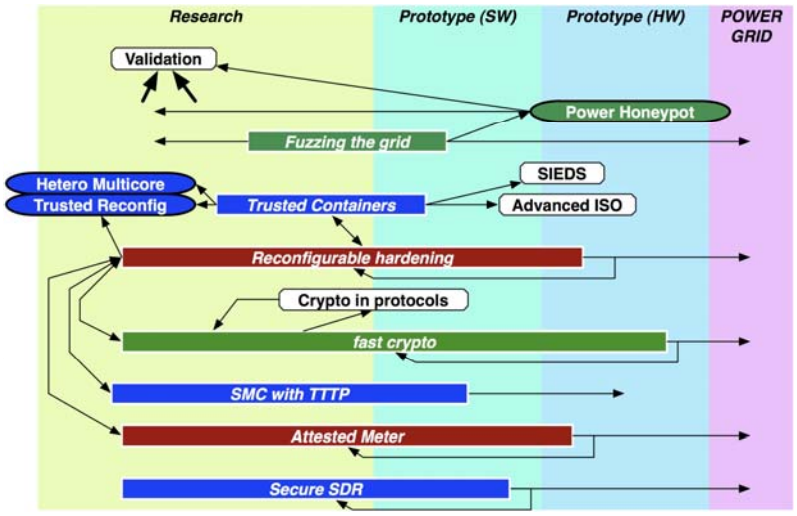
Software:
- Java prototype program for simple 802.15.4 emergency-response networks
- AVR firmware for programmable thermostat, for demand-response purposes
- Java demand-response control and monitoring testbench
- RSE End-to_end compilation framework
- RSE Enhanced compiler to VHDL
- SW/HW interfaces for runtime RSE invocation
- Faerieplay tools and documentation
- YASIR sw prototype
- Batch pairing delegation prototype
- Precomputation memory proxy prototype
- Prototypes for generative and mutative fuzzing for power SCADA protocols
- Implemented TPM driver, user-level and kernel-level software stack for OpenSolaris
- SDR Trusted Configuration Framework (GNU radio package)

Hardware:
- Attested meter hardware prototype
- Price-responsive demand-response controller
- YASIR hardware prototype
- Integration of new checks into RSE
- Integration of RSE into SEL3351, SEL421
- Integration of RSE into DLX and LEON pipelines
- SDR tuning experiments with Universal Software Radio Peripheral

Evaluation:
- Performance evaluation of RSE against embedded benchmarks
- HICSS paper evaluating price-responsive demand-response strategies
- Security analysis of SDR
- Performance measurement for batch pairing delegation
- Performance measurement for precomputation memory proxy
- Performance analysis of SDR TCF radio package
- User testing for Faerieplay tools
- SCADA MITM test harness
- Breaking TCG with a 3" piece of wire

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

What's Next



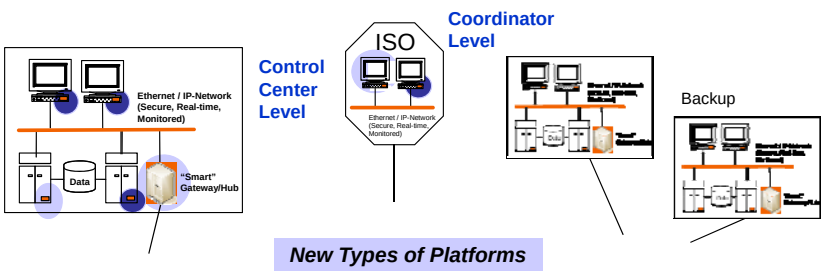
University of Illinois • Dartmouth College • Cornell University • Washington State University

Questions

Backup Slides

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

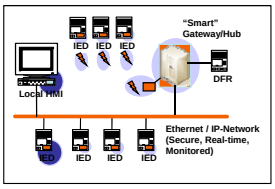
Vision: Increased Power Grid Trustworthiness via Secure and Reliable Computing Base



New Types of Platforms

Customizable Reconfiguration

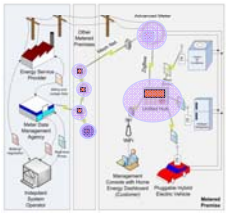
Comprehensive Architectures



Substation Level

Sensor/Actuator Level

Metering and Load Control



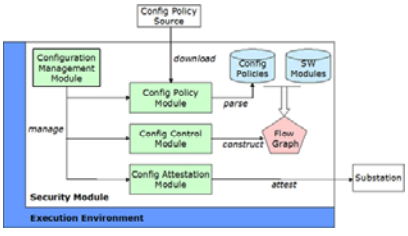
University of Illinois • Dartmouth College • Cornell University • Washington State University

SDR Achievements

- Security analysis, threat model formulation
  - Configuration of a malicious device
  - Violation of regulatory constraints
  - Invalid configuration
  - Insecure software download
  - Exhaustion of system resources
  - Improper Software Functionality
  - Unauthorized access to configuration data

…configure as eavesdropping or jamming device. Transmit at high power level to force other devices to higher power level, drain batteries; communications disruption…

- Design & implementation of trusted configuration framework
  - Provides ***automated radio configuration*** while **preventing malfunctioning or malicious device**
  - Implementation platform: open source GNU Radio software, experiments with prototype SDR hardware



- Published paper, book chapter

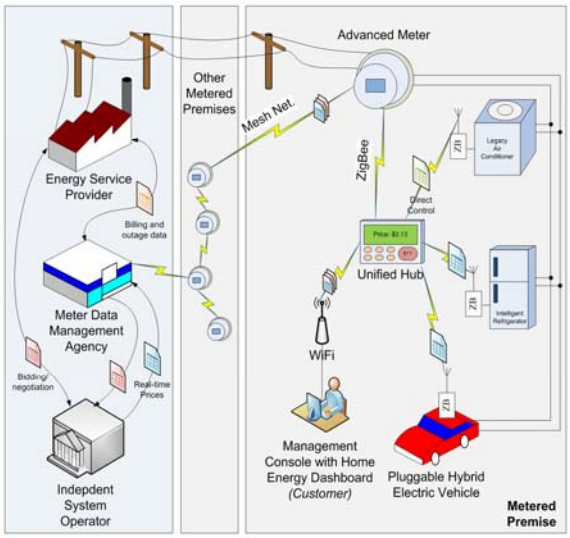
University of Illinois • Dartmouth College • Cornell University • Washington State University

Advanced Meter Functions

- Read data such as kWh consumption
- Disconnect/reconnect power remotely
- Request demand response from premise
- Reset meter (change season mode)
- Set date/time
- Clear tables
- Log in (username/password)
- Log out

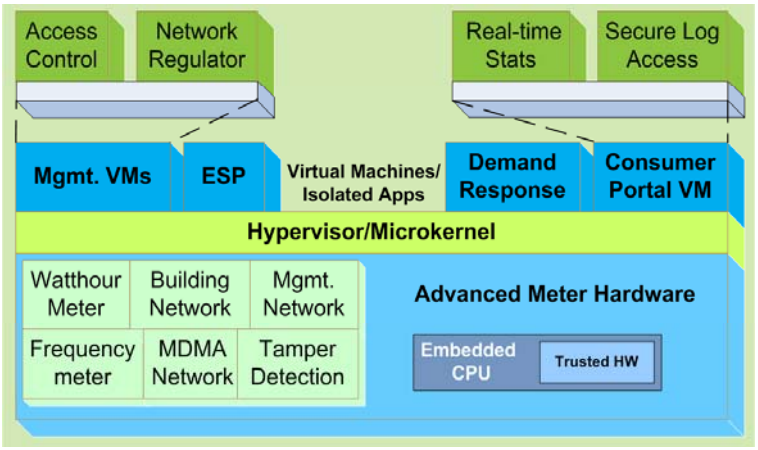
University of Illinois • Dartmouth College • Cornell University • Washington State University

Metering Interactions

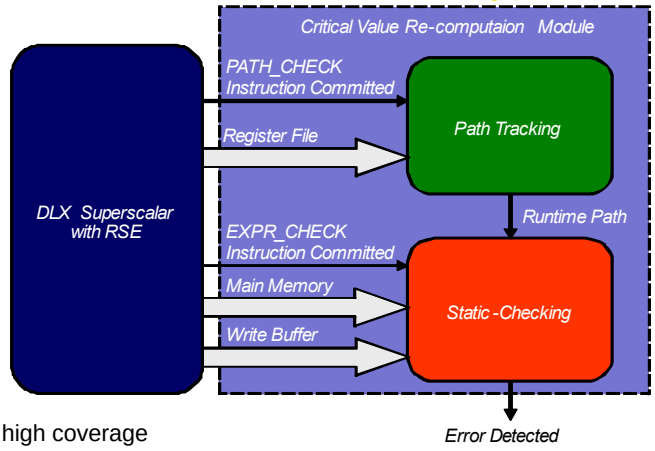


University of Illinois • Dartmouth College • Cornell University • Washington State University

Security Architecture Layers



Example: Critical Value Re-computation Module



- high coverage
- low benign error detection rate
- low performance overhead
- implemented using end-to-end compilation framework

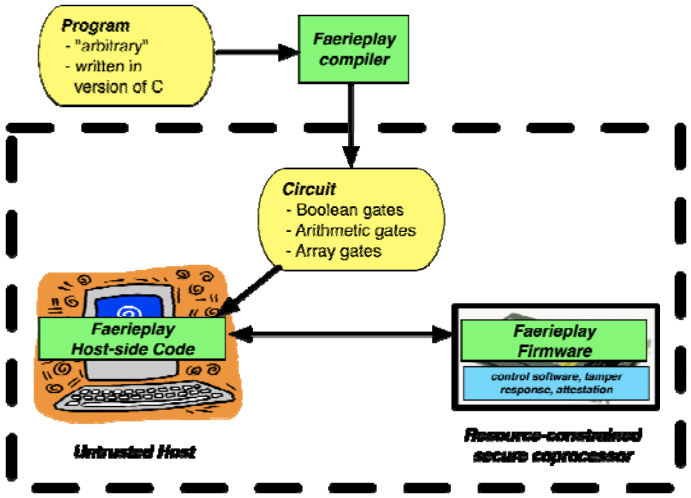
Fuzzing Research Plan

- Reproduce typical attacker's tool chain and investigate its capabilities
  - E.g.: cross-compilation kits for embedded platforms vs. core penetration testing (L2 & L3 injection, IDS evasion & man-in-the-middle attacks) libraries & tools.
- Reproduce known network attacks on unhardened Ethernet network from embedded platforms.
- Explore protocol models based on generative Markov chains and random fields derived from actual packet traces.
- Develop and test fuzzing tools on the Testbed
- Develop visualization tools for analysis of packet traces and crafted traffic
- Explore feasibility of upstream attacks from compromised devices on the Control Center:
  - Direct exploitation of CC software vulnerabilities via crafted upstream traffic,
  - Disruption via fake data injection (Phasor measurement project connection?)

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

Securing Power Market Computation

- General, efficient, virtual TTP from ***resource-constrained*** hardware core



- Current prototype uses IBM 4758 as core---so it ***could be deployed securely today***
  - But we're working on a core that's ***smaller, faster, cheaper***
- Vast improvement over Fairplay, ORAM---so the ***impossible becomes possible***

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

Security Analysis of TPM-base Architectures

Evan Sparks' senior thesis (2007)

TPM reset attack
- Kauer was first to Usenix, but
- We were first to YouTube

Good

Interposers possible

"Good"

Side-channel attacks possible
- Boney-Brumley RSA
- Countemeasure: slowness of TPM

www.cs.dartmouth.edu/~pkilab/sparks/

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