TRUSTED *ILLIAC*: A Configurable Hardware Framework for Reliability and Security

Ravi K. Iyer
(with Wen Mei Hwu, Z. Kalbarczyk, K. Nahrstedt, W Sanders)

Center for Reliable and High Performance Computing
Coordinated Science Laboratory
University of Illinois, Urbana-Champaign

[www.crhc.uiuc.edu/DEPEND](http://www.crhc.uiuc.edu/DEPEND)
The Coordinated Science Laboratory
Leadership in Information Technology
Ravi K. Iyer, Director

Personnel – 500+ Researchers
- 100 professors from 15 academic departments
- 60 senior professional researchers, post-docs & adjunct faculty members
- 350 graduate students
- 70 undergraduate students

CSL Highlights
- Campus “think tank” in IT
- Fundamental research with strong corporate connections
- Successful startups
- Provides leadership to major campus initiatives
- CSL Centers
  - Illinois Center for Wireless Systems
  - Illinois Center for Integrated Microsystems
  - Center for Autonomous Engineering Systems & Robotics
  - Corporate Centers: Motorola, Vodafone, HP.

Multidisciplinary Excellence at the Nexus of Communication, Computing & Control
- Building the next generation air transportation system
- Multi-modal imaging & visualization for healthcare, animation, security & surveillance
- Pervasive & embedded technologies from hand-held devices to large-scale systems
- Making the telecommunications enterprise economical, high-performance & secure
- New parallel technologies for high-end computing applications
- Trusted ILLIAC – a disruptive technology for “rock solid” reliable & secure computing
TRUSTED ILLIAC: Goals

• Create a large, demonstrably-trustworthy computing platform
  – Application aware reliability and security
  – Reconfigurable
  – Prototyping and Benchmarking

• Support for
  – Critical Infrastructures computing platforms
  – Examples: The Power Grid, Financial Databases

• State of the Art: A one-size-fits-all approach
  – Creating a trustworthy environment is complex, expensive to implement. Complex fault management needed (40-60 percent of the code-base) –
  – a lot of wasteful fault detection and recovery!
  – Difficult if not impossible to validate
Present Day Power Grid Cyber Infrastructure

- Present day power grid cyber infrastructure involves the control of areas feed data to a coordinator.
- The coordinator uses this data to create a model from RTUs/IEDs.
- Peer coordinators may exchange information for a broad model.
- The degree of sharing may change over time.

Photos courtesy of John D. McDonald, KEMA Inc.
Approach

• Explore processor/OS/Application level solutions to achieve low-cost, high-performance, scalable security and reliability checking in the same framework

• Provide small footprint solutions that not require large amount of extra hardware or software

• Ensure timely detection and recovery to prevent loss of service or damage to critical infrastructure

• Provide solutions that can coexist with new processing technologies; e.g. multi-core processors
System Architecture

Vision:
• Transform the computing base for application-level security and reliability guarantees

Main idea:
• Derive application-centric checks
• embed them in the HW
• access them with OS/middleware support
• validate them in power-grid cyber infrastructure

Considering:
• Both COTS and new architectures
• technical challenges raised by deployment/management
Current Generation of Low-end Devices (2)

- **NTU-Substation Controller**
  - high-performance
  - large database capacity
  - data concentrator and protocol converter applications
  - ability to process a large amount of data from IEDs,
  - interface a large number of discrete data acquisition and control devices in the substation.

- **Design Features**
  - distributed processing architecture;
  - multiple 32-bit microprocessors,
  - linked using a peer-to-peer type network
  - multiple IED isolated serial communication interfaces

- **Operating Systems**
  - Real Time: RTOS, e.g., Thread X
  - Linux, Windows….
A Secure and Reliable Computing Base

- Reconfigurable operating system-level kernel module to support OS/application aware security and reliability services

**Current features**
- Two level hierarchy:
  - low-level pins interfacing with OS and hardware
  - high-level modules providing application-specific security and reliability techniques

**Available modules**
- Application/OS hang/crash detection
- Transparent application checkpoint

- Reconfigurable processor-level hardware framework to support security and reliability

**Available modules**
- Malicious attack detection
  - Pointer taintedness detection
  - Information-flow signatures
- Transparent hang/crash detection for OS and applications
Automated Design Flow

**Application Source Code**

- Profiling

**Dynamic Execution Profile**

- Fanouts analysis

**Application code annotated with critical variables**

**Trust-Augmented Compiler**

- Application code instrumented with interface to invoke H/W checks

- Path-tracking state machines

- Checking Expressions

- VHDL Translation & synthesis

**General-purpose Processor**

**RSE Interface**

**Reliability and Security Engine (RSE)**
Hardware Implementation: RSE Module

DLX Superscalar with RSE

Path Tracking
- PATH_CHECK Instruction Committed
- Register File

Static-Detector Module

Static-Checking
- EXPR_CHECK Instruction Committed
- Main Memory
- Write Buffer

Runtime Path
Security Partitioned Applications

Intelligent Electronic Device - SEL 3351 Data Aggregator

Main Processor

Database Application

Streaming Video Distribution Application

Secure Coprocessor Protected with RSE

Secure Data

Secured Code Kernels

Access Control Functions
Example of Security Partitioned Applications

Intelligent Electronic Device - SEL 3351 Data Aggregator

Main Processor

Database Application

Streaming Video Distribution Application

Secure Coprocessor Protected with RSE

Secure Data

Secured Code Kernels

Access Control Functions

Main application runs on COTS processor.
Security Partitioned Applications

Intelligent Electronic Device - SEL 3351 Data Aggregator

Main Processor

Database Application

Streaming Video Distribution Application

Secure Coprocessor

Protected with RSE

Secure Data

Secured Code Kernels

Access Control Functions

Coprocessor allows utilization of custom checking hardware.
Security Partitioned Applications

Intelligent Electronic Device - SEL 3351 Data Aggregator

- Main Processor
  - Database Application
  - Streaming Video Distribution Application
  - Secure Coprocessor Protected with RSE
    - Secure Data
    - Secured Code Kernels
    - Access Control Functions

Secure kernels provide high levels of trust
Security Partitioned Applications

Intelligent Electronic Device - SEL 3351 Data Aggregator

Main Processor

- Database Application
- Streaming Video Distribution Application

Clearly Defined Interfaces Support Development

Secure Coprocessor Protected with RSE

- Secure Data
- Secured Code Kernels
- Access Control Functions
Security Partitioned Applications

Intelligent Electronic Device - SEL 3351 Data Aggregator

Main Processor

- Database Application
- Streaming Video Distribution Application

Secure Coprocessor Protected with RSE

- Secure Data
- Secured Code Kernels
- Access Control Functions

Secured Data Remains on Coprocessor
Coprocessor Integration within the Testbed Power Grid Application

- Augment SEL 3351 with FPGA-based coprocessor.
- Nallatech FPGA Card available in PC-104+
- Demonstrate Coprocessor in various applications:
  - Undervoltage Relay
  - Video Streaming Distribution
Power Grid Applications Revisited

Undervoltage Load Shedding Relay:
- Monitor critical power data and take corrective action before system is affected.
- Protect against accidental and malicious data corruption using RSE.
- Integrate FPGA coprocessor into SEL-3351 Data Aggregator using PC-104+ interface.
- FPGA Coprocessor with RSE will execute security critical kernels within protected application with a high degree of Trust.

Streaming Video Distribution:
- Provide protection for distributed distribution of Substation security camera video.
- Prevent malicious tampering with video feed due to bandwidth strangling by limiting each individual users bandwidth usage.
- RSE FPGA Coprocessor will protect small security critical kernels within the streaming application.
Nallatech DIME-II with Xilinx FPGA

Schweitzer SEL-3351 Data Aggregator

Xilinx JTAG Debug Cable

TClP Testbed: Synchrophaser Relay Protected with RSE

Schweitzer SEL-421
Current and Future Development

Initial Cluster

- 256 Linux nodes

FPGA-based hardware

Trusted Illiac Node for advanced hardware development

Reliability and Security Engine

- Application-specific detectors
  - Reliability - process health monitor, data value checking
  - Security - dataflow signature checking, pointer-taintedness checking

- Definition of hardware-software interfaces
  - P2P Streaming application
    - Detection of misbehaving, malicious, or selfish users
  - Model-driven trust management
    - System monitoring and fault/error management

- Integration of hardware accelerators with Linux OS