CS&IIR/IOC Overview

Cyber Security & Information Infrastructure Research
Information Operations Center
Computational Sciences and Engineering Division
Oak Ridge National Laboratory

December 12, 2005
Mission and Objectives

• The CS&IIR and IOC conduct basic and applied research to develop leading-edge end-to-end integrated core capabilities and solutions to:

  - Influence, disrupt, corrupt, or deny adversaries the opportunity to exploit friendly information systems for their own purpose;

  - Providing the advanced technologies necessary to protect, defend, and preserve friendly information systems with timely, accurate, and relevant information access and real-time situation awareness.

• Discover, evaluate, and understand existing and emerging threat;
• Advance the state-of-the-art in detection, deterrence, mitigation, and destruction of the threats;
• Protect our data from insider threats and external attacks;
• Ensure the continuing security, survivability, and dependability of our national critical infrastructure.
Research Staff

- CS&IIR and IOC staff consist currently of 15 organic and 7 matrix staff.

  Ph.D.    4
  Ph.D.(*) 6
  MS       7
  MS (*)   1
  BS       3

(*) Matrix Staff
CS&IIR/IOC ORNL Expertise

Components
- Algorithms
- Agents
- Fusers
- Knowledge Discovery

Systems
- Intrusion Detection
- OS Security
- Standards

System of Systems
- Frameworks
- System Architectures
- Integration of Systems
- Cyber Strategy & Tactics
- Vulnerability Assessment
- Threat Assessment
- Large Scale Simulation
Focus Areas

- **Situational Awareness**: Knowing the current state of the network. Current Attacks. Source of Attacks, Goal of Attacks.
- **Insider Threats**: How to identify/detect and protect the network from insider attacks.
- **Data Protection**: How to protect sensitive data from insider corruption and exfiltration.
- **Software Assurance**: How to assure software do not contain malicious and sleeper codes.
- **Response**: The ability to rapidly respond at machine speed. This includes network reconfiguration, set filters, move software sensors and probes all bounded by policy requirements.
Dimensions of Security Factors

Vulnerability

Data confidentiality

Data Integrity

Authentication

Survivability

Non-repudiation

Criticality

Critical Assets

Threat with Vulnerabilities

CA with Vulnerabilities

CA with Vulnerabilities and Threat

Critical Assets with Threat

Threat Environment

RISK
Emerging and Evolving Cyber Threats Require Sophisticated Response and Protection Capabilities

- Advanced Algorithms
- Cyber Attack Detection and Machine Speed Response
  - Distributed Intrusion Detection and Attack Containment (DIDAC) for Organizational Cyber Security
  - Distributed Zero-Day Attack Detection
- Cyber Security Management (CSM) Framework
- Stand-off Brain Scan Authentication and Identification
- Data and Identity Integrity and Protection
  - Preventing Ex-Filtration and Corruption of Stored Data
  - Protection of Data (Secure, Trusted, Protected Information Sharing)
  - Digital Watermarking & Traceback
  - SNORT Plus
  - Keystroke Biometric
ORNL Partners in New NSF Science & Technology Center

Trust Center Partners

Industrial Partners
- Cisco Systems
- ESCHER
- Hewlett Packard
- IBM
- Intel
- Microsoft
- Oak Ridge National Laboratory
- Qualcomm
- Sun
- Symantec

Academic Partner Institutions
- Carnegie Mellon University
- Cornell University
- Mills College
- San Jose State University
- Smith College
- Stanford University
- University of California, Berkeley
- Vanderbilt University

Academic Partner Research Centers
- Center for Information Technology Research in the Interests of Society (CITRIS)
- Center for Hybrid and Embedded Software Systems (CHESS)

The Team for Research in Ubiquitous Secure Technology (TRUST) is devoted to the development of a new science and technology that will radically transform the ability of organizations (software vendors, operators, local and federal agencies) to design, build, and operate trustworthy information systems for our critical infrastructure.
• Design & Validation of Trustworthy Systems
  - Trust – a holistic combination of security, correctness, dependability, privacy, and survivability
  - Building and Validating Trustworthy Systems, Software, and Networks from the ground up
  - Assessment-Driven Design for Trust

• Combining University, Industry, & Government Expertise
  - Campus-Wide Effort
  - National, State, and Industry Funding
  - Taking Application-centric approach; close industry-academic partnerships
  - Including Research, Education, and Workforce Development

Real-world Inputs
  - Problem identification

Information Trust Institute
  - Application-specific research & development
  - Deployment

Outcomes
  - Education/Workforce Dev.
  - Trusted System

Defense Applications
  - Boeing, SAIC, BBN, TCS+

Critical Infrastructures
  - Honeywell, GE, OSI, ORNL...

Trusted Enterprise Networks
  - HP, SUN, ORACLE, CISCO

Synthesis of common elements

Generic Architectural Constructs
Generic Validation & Design Tools
Workforce Development

Outcomes
  - Skilled & knowledgeable workforce
  - New technology spin-offs, new services
  - New trust-based reworked COTS products
NSF Cyber Trust Center: Cyber Infrastructure for Power

Address technical challenges motivated by power grid problems in

- Ubiquitous exposed infrastructure
- Real-time data monitoring and control
- Wide area information coordination and Information sharing

By developing science in

- Secure and Reliable Computing Base
- Trustworthy infrastructure for data collection and control
- Wide-Area Trustworthy Information Exchange
- Quantitative Validation

www.iti.uiuc.edu
Current CS&IIR/IOC Projects

- **Situation Awareness**
  - ICETECH-I
- **Data Protection**
  - Digital Watermarking & Trace back and anomaly Detection
- **Insider Threat Detection & Mitigation**
  - SNORT Plus
- **DHS Cyber Threat Assessments**
  - Cyber Security Management (CSM) Framework
- **DHS Motivation & Intent Thrust**
  - PsyGAPS (Predicting Terrorist Strategies and Target Selection)
- **Steganography**
- **Weigh-in-Motion**
- **Mobile Automated Distributed Support System (MADSS)**
- **Integrated Safety and Security Enforcement Information System**
- **Identification and Monitoring of Radiation In Commerce Shipments**
- **Trusted Corridor**
Situational Awareness Framework Issues

• Ability to integrate applications from multiple sources into a single system. Eliminates stovepipes and allows best of breed integration.
• Real-Time Operation
  – Reduce time to complete task by Parallel/Distributed Operation
• Scalability
• High Security Architecture
• Collaboratory Environment
• Recoverability/Regeneration
• Synchronous Operation
• Minimizing network bandwidth utilized for Cyber Security.
• Operates in a mobile ad hoc network environment.
**IAVA Compliance Enabling Technology (ICETECH)**

- **Goal:** Large Scale Situation Awareness and Information Assurance Vulnerability Assessment (IAVA).
- **Teamed effort with EigenSoft.**
- **Tightly coupled agent framework to monitor and control network.**
  - Map the topology in near real-time including all hidden machines.
  - Assess vulnerabilities.
  - Patch vulnerabilities.
- **Current Sponsor:** Joint U.S. STRATCOM and DISA effort.
- **Demonstration Site:** U.S. Army Space Command, Colorado Springs, CO.
Threat Assessments

- Electric power generation, transmission, and distribution
- Oil and gas pipelines
- Water treatment and distribution
- Transportation systems
- Refineries
Next-Generation Validation and Response Tools for Critical Protection Mechanisms

- Large-Scale Cyber Security and Network Test Bed
  - Software Verification and Validation
  - Vulnerability Assessments
- Software Assurance
- Software Reliability
- IAVA Compliance Enabling Technology (ICETECH)
Intrusion Prevention, Detection, and Response at the Granular Level (SNORT Plus, CSM)

- Multi-Level Evidence Based Intrusion Detection System Using Bayesian Network to Detect Insider Threats (SNORT Plus)

- Threat Assessment Risk Analysis (TARA) Management Framework – Algorithm and Tool for Threat/Vulnerability assessment and risk analyses
Nonlinear Analysis of Complex Time-Serial Data

Projects:

• Forewarning of Epileptic Seizures from Scalp Brain Waves
• Forewarning of Heart Attacks and Fainting from Surface Heart Waves
• Detection of Sepsis from Surface Heart Waves
• Detection of Increasing Breathing Difficulty from Chest Sounds
• Forewarning of Failure in Motors and Motor-Driven Components

Recent Publications:


Domestic Integrated Inter-modal Safety & Security Monitoring Pilot Program (ISSEIS)

State Operated Web-Based Service Interface

Weigh Station (Mobile & Virtual) Sensors

Critical National Database
- Nuскаfе RРМ
- Handheld Rad Detector (Spectroscopy)
- LРR Camera
- Digital Camera (DOT #)
- Video Camera (Environment + Truck)
- Scale (Static & WIM)
- Scanner (Manifest)
- Weather
- Systems Diagnostics
- Government Encryption/Decryption

Non-Critical National Database
- Laser Axle Counter
- Thermal Camera
- Chemical Detector
- RFID

State Operated Web-Based Service Interface

State Weigh Station Central Database

State Operated Web-Based Service Interface

State Operated Web-Based Service Interface

Protected Secure Infrastructure Shell Service Interface (PSISSI)

DOT
- Law Enforcement
- Emergency Response
- State Level Reach Back

ORNL Secure Trusted Weigh Stations National D3C Center

FBI
DHS
EPA
DOT
ACADEMIA
SCIENCE COMMUNITY
National Reach Back

ORNL SENSORNET

OAK RIDGE NATIONAL LABORATORY
U. S. DEPARTMENT OF ENERGY
Logistics Transformation

Next Generation Portable Weigh-In-Motion (WIM) System

TC-AIMS II (TIS) AALPS

Unit ID and Vehicle ID with planned weights via AIT:
- RFID
- MSL: 2D and/or 1D barcodes

Unit ID and Vehicle ID with actual weights:
- Weight (total)
- Individual axle
- Axle spacing
- Center of balance

Actual Weight and Center of Balance Data

Updated Actual Movement Information

- Portable
- Fully automated—no operator error
- Wireless technology and load-planning
- Determines weight, center of balance, axle weight and spacing
- 500% productivity increase, save 40 minutes per plane
- Enhances safety of the vehicle/cargo weighing process and safety of deployments

Contacts: Robert K. Abercrombie, 865-241-6537, abercrombie@ornl.gov