

2014 Cyber and Information Security Research (CISR'14) Conference (The 9th Annual Cyber Security Conference at ORNL, formerly CSIIRW)

8-10 April 2014

Oak Ridge National Laboratory, Oak Ridge, Tennessee, USA

<http://www.cisr.ornl.gov/cisrc14/index.html>

Important Dates

All deadlines are 23:59:59 EST

Submission Deadline 24 February 2014

Author Notification 10 March 2014

Early Registration Deadline..... 14 March 2014

Registration Deadline..... 28 March 2014

Submission and Registration

Submission and registration information can be found at:

<http://www.cisr.ornl.gov/cisrc14/index.html>

(Not currently active)

About

Cyberspace is fundamental to our national prosperity, as it has become critical to commerce, research, education, and government. Realizing the benefits of this shared environment requires that we are able to properly balance the risks and rewards, understand and communicate threats to security and privacy, and rapidly adapt any resulting approach to a changing adversarial environment.

Recognizing this, we seek original paper submissions in the following general areas derived from the Federal Cybersecurity R&D agenda¹.

- (1) **Tailored Trustworthy Spaces** – Provides flexible, adaptive, distributed trust environments that can support functional and policy requirements arising from a wide spectrum of activities in the face of an evolving range of threats, recognizing the user's context and evolves as the context evolves.
- (2) **Moving Target** – Enables us to create, analyze, evaluate, and deploy mechanisms and strategies that are diverse and that continually shift and change over time to increase complexity and cost for attackers, limit the exposure of vulnerabilities and opportunities for attack, and increase system resiliency.

1

http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf

- (3) **Designed-In Security** – Builds the capability to design, develop, and evolve high-assurance, software-intensive systems predictably and reliably while effectively managing risk, cost, schedule, quality, and complexity.
- (4) **Cyber Economic Incentives** – Develops effective incentives to make cybersecurity ubiquitous, including incentives affecting individuals and organizations.
- (5) **Science of Security** – Provides a more fruitful way to ground research efforts, and to nurture and sustain progress.

Keynote Speakers

- **Gregory Neal Akers**, Senior Vice President for Advanced Security and Chief Technology Officer for TRIAD Group, Cisco Systems, Inc.
- **Lt. Gen. Michael Basla**, Chief Information Dominance and Chief Information Officer, US Air Force
- **Richard Bejtlich**, Chief Security Strategist, FireEye, Inc.
- **Lt. Gen. Edward Cardon**, Commanding General, US Army Cyber Command
- **Dr. Mica Endsley**, Chief Scientist, US Air Force
- **Dr. Carol Hawk**, Program Manager for Cyber Security for Energy Delivery Systems in the Office of Electricity Delivery and Energy Reliability, US Department of Energy
- **Nate Lesser**, Deputy Director, National Cybersecurity Center of Excellence, NIST
- **Michael Pozmantier**, Program Manager for Transition to Practice, Cyber Security Division, Science & Technology Directorate, US Department of Homeland Security

Related Events

1. DOE Cybersecurity for Energy Delivery Systems (CEDS) Program for the office of Electricity Delivery and Energy Reliability in the Department of Energy (DOE) - Several CEDS performers will present and demonstrate results of their R&D efforts. Open to all.
2. DHS Transition To Practice Program – Technologies selected by DHS from DOE labs will be presented and demonstrated. Open to all.
3. DOE Cyber Sciences Lab (CSL) – CSL is a virtual integrated cyber defense R&D activity that spans 8 DOE National Labs and 1 DOE Test Site. Selected technologies proposed for Signature Programs will be presented and demonstrated. Open to all.
4. DOE Cyber Defenders 2nd Annual Symposium. Restricted access.

Specific Topics of Interest

The following more specific topics are of special interest. Many of these are also taken from the Federal Cybersecurity R&D agenda.

- Security and trustworthiness of information in motion and at rest, especially in a shared (“cloud”) environment.

- Understanding the risks and tradeoffs in deploying solutions, in terms that are measurable and quantifiable.
- Fusion of cyber data such as netflows with other data from non-cyber sources, such as geographic and economic data to discover connections and highlight activity of interest.
- Discovery of trends, especially in malware design and use.
- Trust negotiation tools and data models to support negotiation of policy.
- Data protection tools, access control management, monitoring and compliance verification mechanisms to allow for informed trust.
- Hardware mechanisms that support secure bootload and continuous monitoring of critical software.
- Application and operating system elements that can provide strong assurance that program semantics cannot be altered during execution.
- Control theory to abstract the complexity of moving target systems and enable sound, resilient system management.
- Models and techniques to support on-the-fly evidence creation during a systems engineering process.
- Mathematically sound techniques to support combination of models and composition of results.
- Analysis techniques (based on model checking, abstract interpretation, semantics-based testing, and/or verification) to enable traceable linking among diverse models and code.
- Team and supply chain practices to facilitate composition of assurance in the supply chain.
- Psychology and human factors for how to build software specification, implementation, verification, analysis, and testing tools that are easy to use and provide positive feedback to users.
- Methods to model adversaries; especially co-modeling of attackers and defenders.
- Control theory for maintaining security in the presence of ongoing and even partially successful attacks.
- Formal and stochastic modeling techniques in security modeling.
- Comprehensive, open, and anonymized data repositories.

Organization

General Co-Chairs:

- Joseph P. Trien, Oak Ridge National Laboratory
- Dr. Stacy J. Prowell, Oak Ridge National Laboratory
- Dr. John R. Goodall, Oak Ridge National Laboratory

Program Co-Chairs:

- David Manz, Ph.D., Pacific Northwest National Laboratory
- Sean Peisert, Ph.D., Lawrence Berkeley National Laboratory
- Sven Leyffer, Ph.D., Argonne National Laboratory

- Carl Kutsche, Ph.D., Idaho National Laboratory
- Michael Grimaila, Ph.D., Air Force Institute of Technology
- Marco Carvalho, Ph.D., Florida Institute of Technology
- Sun-il Kim, Ph.D., University of Alabama, Huntsville
- Todd R. Andel, Ph.D., University of South Alabama

Proceedings Co-Chairs:

- Robert Abercrombie, Ph.D., Oak Ridge National Laboratory
- Todd McDonald, Ph.D., University of South Alabama

Sponsorship and Exhibition

If you are interested in becoming a sponsor contact Kevin Jackson at Federal Training Partnership

Kevin Jackson

Kevin.jackson@federaltrainingpartnership.com

1-844-325-0341

Sponsorship Levels:

Platinum: \$7500

Gold: \$5000

Silver \$3000