SCIENCE OF SECURITY VIRTUAL ORGANIZATION

http://sos-vo.org

KATIE DEY

VANDERBILT UNIVERSITY

VANDERBILT UNIVERSITY Berkeley UNIVERSITY OF CALIFORNIA Massachusetts Institute of Technology INFORMATION & COMPUTER SCIENCES UNIVERSITY of HAWAI'I at MĀNOA

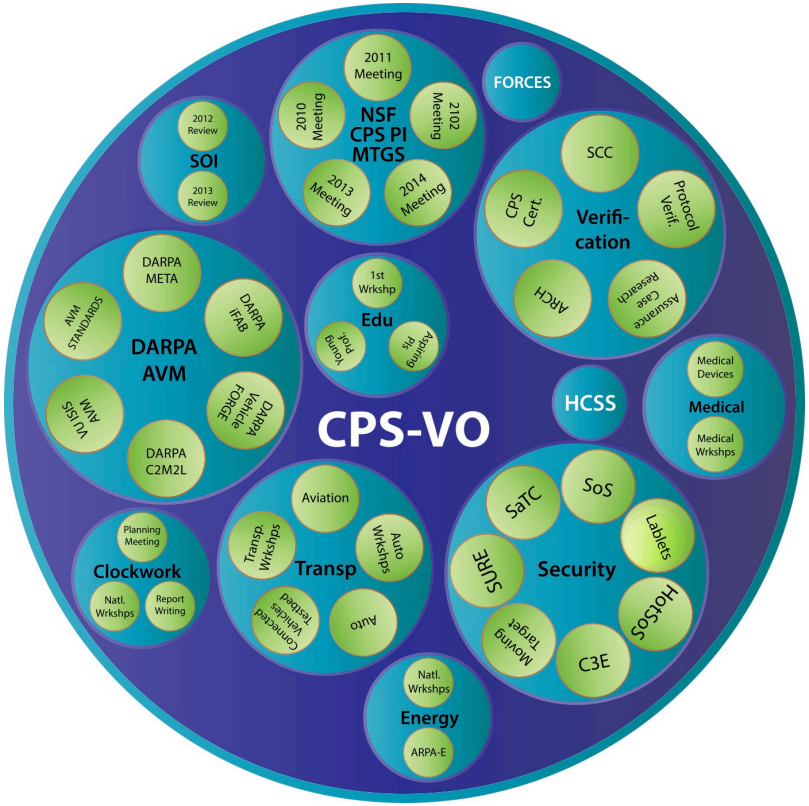
SURE

OUTLINE

- **The Cyber-Physical Systems Virtual Organization (CPS-VO)**
- **The Science of Security Virtual Organization (SoS-VO)**
- **The SURE presence on the VO**
  - Public group
    - Research Team
    - Projects
    - Artifacts
    - Meetings
  - Internal groups
    - Project Management
    - Reporting
  - What's next?
    - Tools and Software

CPS-VO

- What is the CPS-VO?
  - Community
  - Collaboration
  - Technology Transfer & Translational Research
  - Long-Distance / International Collaboration



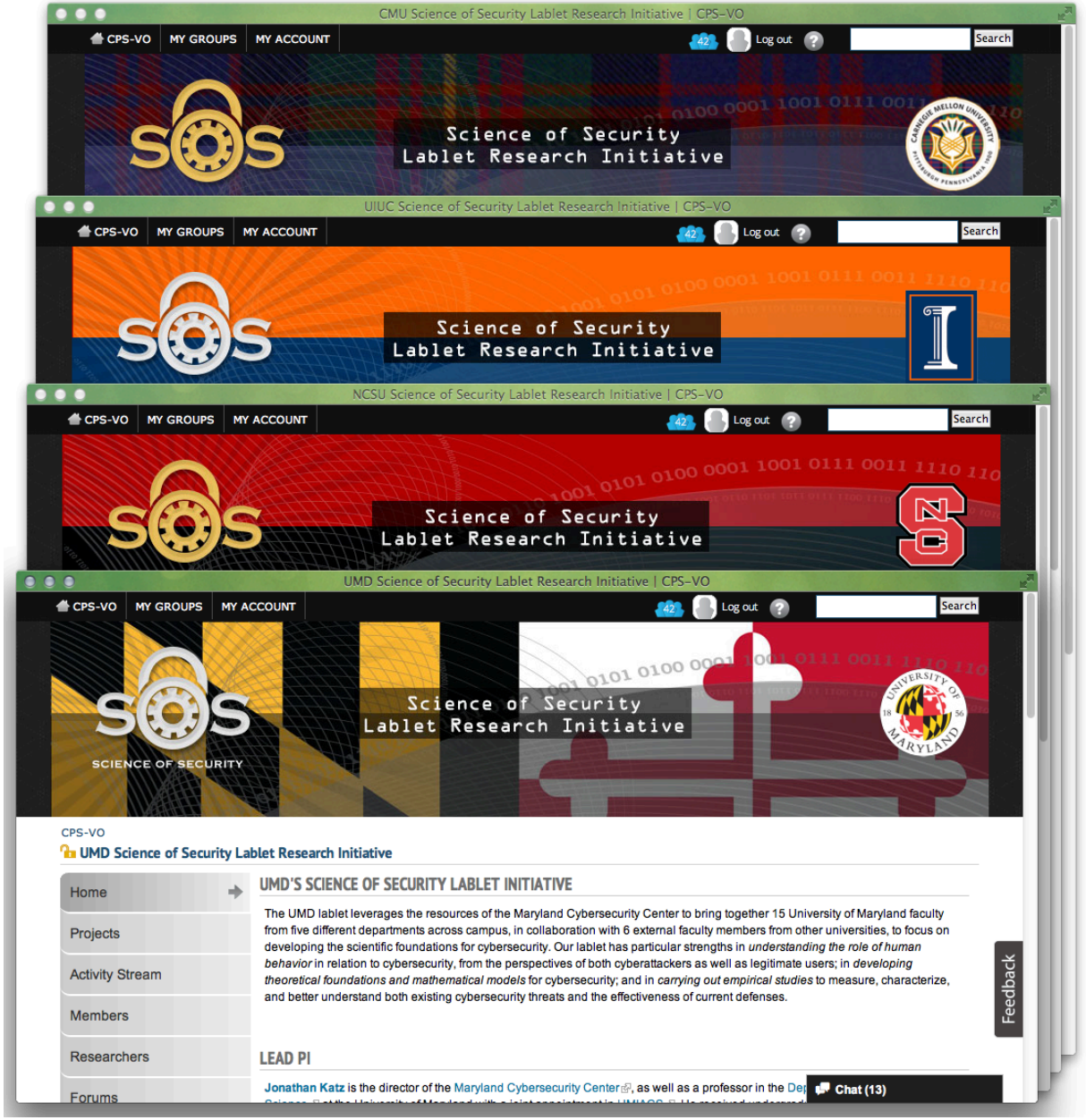
SOS-VO

- What is the SoS-VO?
  - Family of related groups on the CPS-VO
    - Science of Security Virtual Organization
    - NSA SoS Lablets
    - Research Competition
    - Workshop and Conference sites
    - SURE Project

SOS-VO.ORG


SCIENCE OF SECURITY
An Online Community to Advance Cyber-Security Science
Join Us!
CPS-VO
Science of Security VO
Home
About
Calendar
Search
Members
Contact Us
Forums
Files
SUBGROUPS
Science of Security VO
Best Scientific Cybersecurity Paper Competition
CMU Science of Security Lablet Research Initiative
Moving Target Research
NCSU Science of Security Lablet Research Initiative
Science of SecUre and REsilient Cyber-Physical Systems (SURE)
SoS Lablet Reports
Symposium and Bootcamp
In the Spotlight
Upcoming Events
Upcoming Events Worth Checking Out
Upcoming Events Worth Checking Out
The lastest information on all upcoming science of security related events.
more
Newsletter
Best Scientific Cybersecurity Paper
HotSoS '15
Hard Problems
Recently Posted Publications
Feature Cross-Substitution in Adversarial Classification
Abstract: The success of machine learning, particularly in supervised settings, has led to numerous attempts to apply it in adversarial settings such as spam and malware detection. The core challenge in this class of applications is that adversaries are not static data generators, but make a deliberate... more
Recent News
New Report on Measuring Computer and Security Expertise
Researchers at Indiana University released a technical report that... more
Insight to Modern Cyber Threat Intelligence
This article provides expert insights to modern cyber threat... more
Lablet Quarterly Meeting
exchanged research and technical discussions on SoS and the five Hard Problems in cybersecurity
For a brief summary of the two day quarterly Science of Security... more
more
Upcoming Events
12/01/14 - 03/31/15
3rd Annual Best Scientific Cybersecurity Paper Competition
03/23/15 - 03/25/15
TCC 2015
03/26/15 - 03/27/15
MSPWorld Spring Conference 2015
more

SOS LABLETS

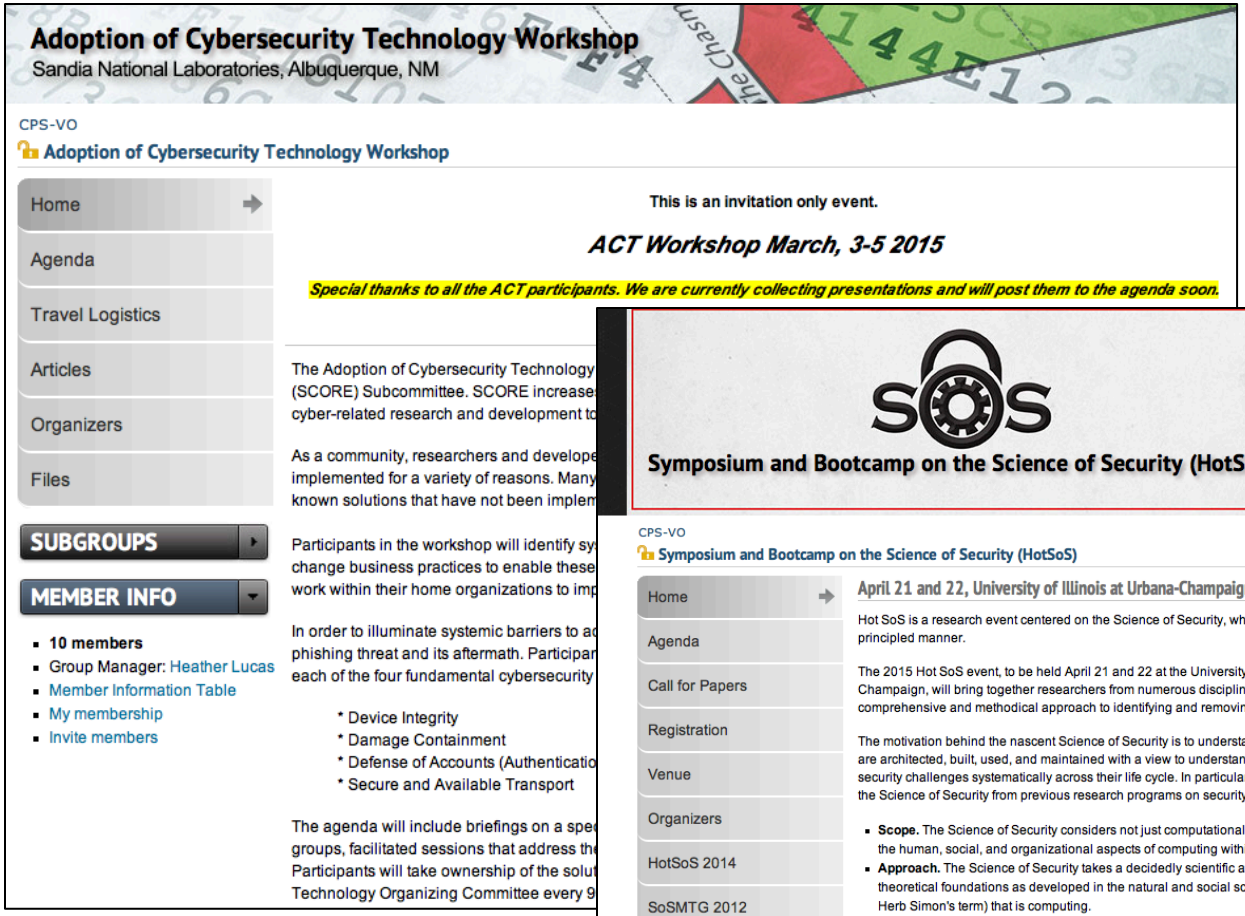


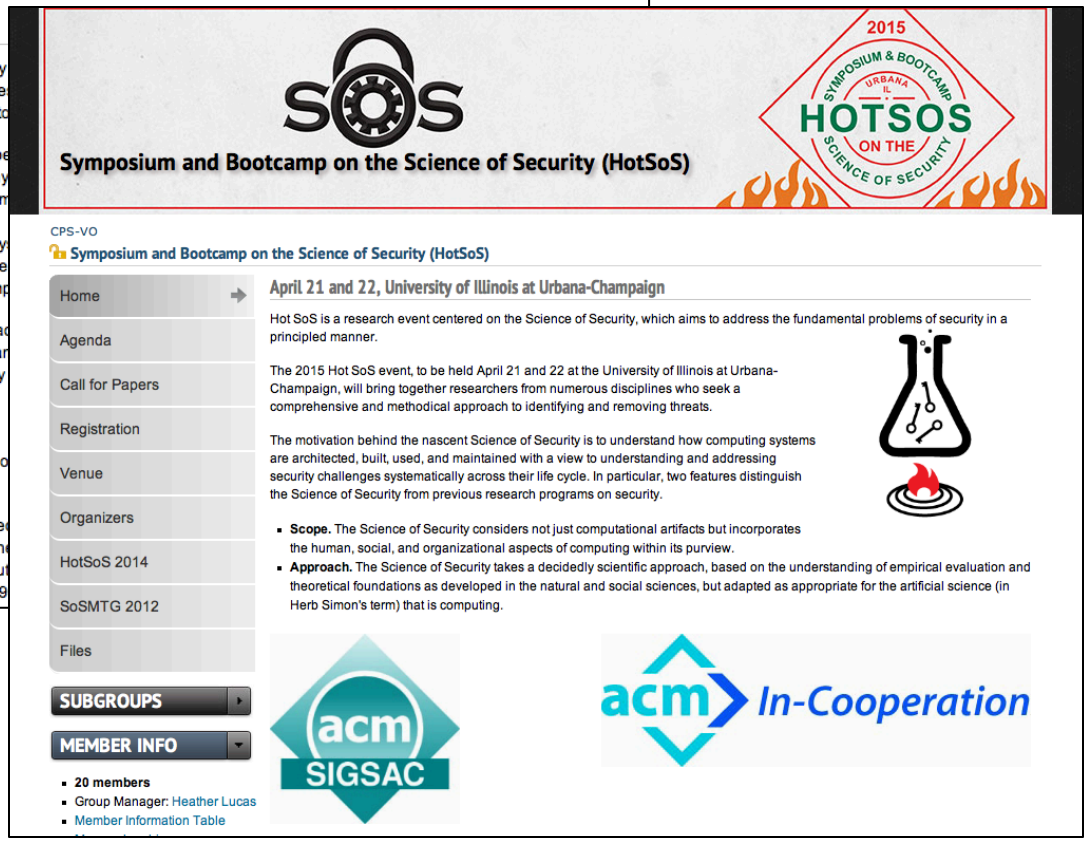
RSITY

RESEARCH COMPETITION

SURE

WORKSHOP/ CONFERENCE SITES





OUTLINE

- **The Cyber-Physical Systems Virtual Organization (CPS-VO)**
- **The Science of Security Virtual Organization (SoS-VO)**
- **The SURE presence on the VO**
  - Public group
    - Research Team
    - Projects
    - Artifacts
    - Meetings
  - Internal groups
    - Project Management
    - Reporting
  - What's next?
    - Tools and Software

SURE GROUP

CPS-VO

Science of SecUre and REsilient Cyber-Physical Systems (SURE)

- Home
- Research Team
- Projects
- Meetings
- Members
- Files

SUBGROUPS

MEMBER INFO

The project on the **S**ystem Science of Sec**U**rity and **RE**silience for cyber-physical systems (SURE) will develop foundations and tools for designing, building, and assuring cyber-physical systems (CPS) that can maintain essential system properties in the presence of adversaries. The technology base of SURE will provide CPS designers and operators with models, methods, and tools that can be integrated with an end-to-end model-based design flow and tool chain.

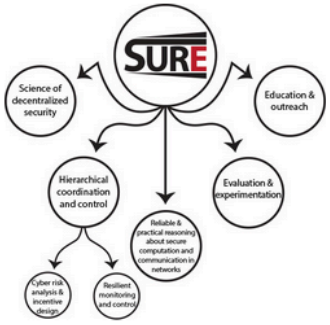
To date, security and resilience have been considered as largely disjoint (frequently even totally missing) aspects of CPS design. This separation was natural due to the traditionally segmented nature of design flows along isolated aspects of physical and cyber (software and computing) design. However, modern CPS does not permit such separation anymore due to advances and integration in wireless sensor-actuator networks, the internet of "everything", data-driven analytics, and machine-to-machine interfaces. These developments have given CPS the ability to inter-operate and adapt to open dynamic environments, and enabled new trends: (1) Faster operational time-scales; (2) Greater spatial interconnectedness; (3) Larger number of mixed initiative interactions; and (4) Increased heterogeneity of components. These trends are forcing increasingly physical and cyber sides of systems to be tightly coupled. The failure of loosely coupled physical and cyber schemes is evident in chronically unresolved design conflicts between performance and resilience against faults and intrusions, and conflicts between needs for performance optimization while maintaining robustness against adversarial impacts.

Networked CPS can be designed using a hierarchical coordination and control architecture that ensures resilient distributed dynamics. Resilient dynamics generalize functional performance by augmenting design concerns to attain robustness against faults and cyber attacks. The effects of failures and intrusions are usually modeled as uncertainties and casted as adversarial games. One of the key innovations is the introduction of a novel layer in the hierarchical coordination control architecture that is designed for interaction with the human operators using risk analysis and incentive-based approaches. The role of the risk analysis and incentive design is to support distributed decision making for balancing performance and security risks. The theoretical foundations for this innovation lie on dynamic games. The expected benefit of this framework is its potential of helping the convergence of individual decisions toward optimizing mission success.

As integral part of the proposed research program, we will launch a sustained effort to create a new generation of engineers that are comfortable with understanding, exploiting and managing security and resilience in the context of integrated computational, physical phenomena interacting with human designers and operators.

Research Thrusts

1. *Hierarchical Coordination and Control* which is organized further into:
   i. *Cyber risk analysis and incentive design* that aim at developing regulations and strategies at the management level.
   ii. *Resilient monitoring and control* of the networked control system infrastructure
2. *Science of decentralized security* which aims to develop a framework that will enable reasoning about the security of all the integrated constituent CPS components.
3. *Reliable and practical reasoning about secure computation and communication in networks* which aims to contribute a formal framework for reasoning about security in CPS.
4. *Evaluation and experimentation* using modeling and simulation integration of cyber and physical platforms that directly interface with human decision.
5. *Education and Outreach* component that aims at education the next generation of researchers in the field of security and resilience of CPS.



VANDERBILT UNIVERSITY

RESEARCH TEAM

SURE

Science of SecUre and REsilient Cyber-Physical Systems (SURE)

CPS-VO » SCIENCE OF SECURITY VO » SCIENCE OF SECURE AND RESILIENT CYBER-PHYSICAL SYSTEMS (SURE) » RESEARCH TEAM

Research Team

- Home
- Research Team
- Projects
- Meetings
- Members
- Files

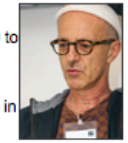
SUBGROUPS

MEMBER INFO

Principal Investigators

Xenofon Koutsoukos (Lead PI) is a Professor in the Department of Electrical Engineering and Computer Science at Vanderbilt University. He is also a Senior Research Scientist in the Institute for Software Integrated Systems (ISIS). Before joining Vanderbilt, Dr. Koutsoukos was a Member of Research Staff in the Xerox Palo Alto Research Center (PARC) (2000-2002), working in the Embedded Collaborative Computing Area. He received his PhD in Electrical Engineering from the University of Notre Dame in 2000. His research work is in the area of cyber-physical systems with emphasis on formal methods, distributed algorithms, diagnosis and fault tolerance, and adaptive resource management. He has published numerous journal and conference papers and he is co-inventor of four US patents. He was the recipient of the NSF Career Award in 2004, the Excellence in Teaching Award in 2009 from the Vanderbilt University School of Engineering, and the 2011 NASA Aeronautics Research Mission Directorate (ARMD) Associate Administrator (AA) Award in Technology and Innovation.

Saurabh Amin (MIT PI) is an Assistant Professor in the MIT Department of Civil and Environmental Engineering. His research focuses on the design and implementation of resilient network control algorithms for infrastructure systems. He works on robust diagnostics and control problems that involve using networked systems to facilitate the monitoring and control of large-scale critical infrastructures, including energy, transportation, and water distribution systems. He also studies the effect of security attacks and random faults on the survivability of these systems, and designs incentive mechanisms to reduce network risks.



Dusko Pavlovic (U. of Hawaii PI) was born in Sarajevo, studied mathematics at Utrecht, and was a postdoc at McGill, before starting an academic career in computer science at Imperial College and at Sussex. He left academia from 1999 to 2009 to work in software research at the Kestrel Institute in Palo Alto. He was a Visiting Professor at Oxford University from 2008-2012, Professor of Information Security at Royal Holloway, University of London (part time at University of Twente in the Netherlands) 2010-2013. He took his current chair in Computer Science at University of Hawaii at Manoa in 2013.

Through the years, Dusko's publications covered a wide area of research interests, from mathematics (graphs, categories) through theoretical computer science (semantics, symbolic computation) and software engineering (behavioral specifications, adaptation), to security (protocols, trust, physical security) and network computation (information extraction). Dusko's past publications and the slides of some of his recent talks are available from his web page.

S. Shankar Sastry (UC Berkeley PI) received his B.Tech. from the Indian Institute of Technology, Bombay, 1977, a M.S. in EECS, M.A. in Mathematics and Ph.D. in EECS from UC Berkeley, 1979, 1980, and 1981 respectively. S. Shankar Sastry is currently dean of the College of Engineering. He was formerly the Director of CITRIS (Center for Information Technology Research in the Interest of Society) and the Banatao Institute @ CITRIS Berkeley. He served as chair of the EECS department from January, 2001 through June 2004. In 2000, he served as Director of the Information Technology Office at DARPA. From 1996-1999, he was the Director of the Electronics Research Laboratory at Berkeley, an organized research unit on the Berkeley campus conducting research in computer sciences and all aspects of electrical engineering. He is the NEC Distinguished Professor of Electrical Engineering and Computer Sciences and holds faculty appointments in the Departments of Bioengineering, EECS and Mechanical Engineering. Prior to joining the EECS faculty in 1983 he was a professor at MIT.

VANDERBILT UNIVERSITY

PROJECTS


cps-vo.org/group/sos/sure/projects
CPS-VO
MY GROUPS
username
Log in
Search
Not a member?
Click here to register!
Forgot username or password?
SURE
Science of SecUre and REsilient Cyber-Physical Systems (SURE)
CPS-VO » SCIENCE OF SECURITY VO » SCIENCE OF SECURE AND RESILIENT CYBER-PHYSICAL SYSTEMS (SURE) » PROJECTS
Projects
Home
Research Team
Projects
Meetings
Members
Files
SUBGROUPS
MEMBER INFO
Project Title
Decentralization in Security: Consequences and Incentive Des...
In security, our concern is typically with securing a particular network, or eliminating security holes in a particular piece of software. These are important, but they miss the fact that being secure is fundamentally about security of all constituent...
Evaluation and Experimentation
This research thrust focuses on the design and development of a highly accessible and scalable testbed environment for supporting the evaluation and experimentation efforts across the entire SURE research portfolio. This work is based on our existing...
Resilience and security in component-based software architec...
Abstract:
Cyber-Physical Systems are converging towards a component-oriented and platform-based implementation. The community-driven Robotic Operating Systems and the proprietary Residential Operating System (of Prodea) are just two examples that indicate...
Resilient Monitoring and Control
CPS employ Networked Control Systems (NCS) to facilitate real-time monitoring and control. Security of the NCS infrastructure is a large problem due to (1) the wide deployment of commercial-off-the-shelf (COTS) computing devices, (2) the connectivity of...
Threat Modeling/Risk Analysis
With the increased use of cyber physical systems in current defense, medical, and energy applications, it is critical for the infrastructure to remain secure. As such, it is important to identify potential security flaws early in the design process in...

PROJECTS

SURE

CPS-VO » GROUPS » SCIENCE OF SECURE AND RESILIENT CYBER-PHYSICAL SYSTEMS (SURE)

Evaluation and Experimentation

- Home
- Research Team
- Projects
- Meetings
- Members
- Files
- SUBGROUPS
- MEMBER INFO

VIEW

Submitted by volgy on Tue, 10/07/2014 - 12:25pm

This research thrust focuses on the design and development of a highly accessible and scalable testbed environment for supporting the evaluation and experimentation efforts across the entire SURE research portfolio. This work is based on our existing technologies and previous results with the Command and Control Windtunnel (C2WT), a large-scale simulation integration platform and WebGME, a metaprogrammable web-based modeling environment with special emphasis on on-line collaboration, model versioning and design-reuse. We are utilizing these core technologies and other third-party tools (e.g. Emulab) to provide a web-based interface for designing, executing and evaluating testbenches on a cloud-based simulation infrastructure. The metaprogramable environment enables us to develop and provide modeling languages, which specifically target each research thrust. Furthermore, by leveraging built-in prototypical inheritance we are building re-usable library components in the target domains.

First, the developed visual/modeling languages will be used to capture the physical, computational and communication infrastructure. Also, the simulation models will describe the deployment, configuration and/or the concrete strategies of security measures and algorithms. Third, the environment will provide entry points for injecting various attack or failure events from an existing library of components or by providing a model-based description of the algorithm.

For stimulating the experimentation and validation efforts in the SURE research thrusts and to motivate students and outside contributors to participate we are developing "Red Team" vs "Blue Team" simulation scenarios, where a using a given CPS infrastructure model each team is tasked to develop and/or configure security and fail-over measures while the other team develops an attack model. After the active design phase--when both teams are working in parallel and in isolation--the simulation is executed with no external user interaction, potentially several times. The winner is decided based on the scoring weights and rules which are captured by the infrastructure model. If successful, we may organize championships and maintain a leader board for each infrastructure model.

PI

volgy

Peter Volgyesi is a Research Scientist at the Institute for Software Integrated Systems at Vanderbilt University. In the past decade Mr. Volgyesi has been working on several novel and high impact projects sponsored by DARPA, NSF, ONR, ARL and industrial companies (Lockheed Martin, BAE Systems, the Boeing Company, Raytheon, Microsoft). He is one of the architects of the Generic Modeling Environment, a widely used metaprogrammable visual modeling tool, and WebGME - its modern web-based variant. Mr. Volgyesi had a leading role in developing the real-time signal processing algorithms in PinPtr, a low cost, low power countersniper system. He also participated in the development of the Radio Interferometric Positioning System (RIPS), a patented technology for accurate low-power node localization. As PI on two NSF funded projects Mr. Volgyesi and his team developed a low-power software-defined radio platform (MarmotE) and a component-based development toolchain targeting multicore SoC architectures for wireless cyber-physical systems. His team won the Preliminary Tournament of the DARPA Spectrum Challenge in September, 2013.

Related Artifacts

SURE: Topics -> Evaluation and experimentation

- Online Collaborative Environment for Designing Complex Computational Systems
- Rapid Synthesis of Multi-Model Simulations for Computational Experiments in C2
- System Science of SecUrity and Resilience for Cyber-Physical Systems (SURE)

VANDERBILT UNIVERSITY

BIBLIO ARTIFACTS

CPS-VO » SCIENCE OF SECURITY VO » SCIENCE OF SECURE AND RESILIENT CYBER-PHYSICAL SYSTEMS (SURE) » BIBLIO LIST

Online Collaborative Environment for Designing Complex Computational Systems

- Home
- Research Team
- Projects
- Meetings
- Members
- Files

SUBGROUPS

MEMBER INFO

VIEW

Submitted by volgy on Tue, 10/07/2014 - 1:58pm

Title	Online Collaborative Environment for Designing Complex Computational Systems
Publication Type	Conference Paper
Year of Publication	2014
Authors	Maroti, Miklos, Kereskenyi, Robert, Tamas Kecskes, Volgyesi, Peter, Ledeczi, Akos
Conference Name	The International Conference on Computational Science (ICCS 2014)
Date Published	06/2014
Publisher	Elsevier Procedia
Conference Location	Cairns, Australia
Keywords	cyberinfrastructure, Evaluation and experimentation, Foundations, model-based software; online collaboration; automatic code generation; web-based design environment, Modeling, Resilient Systems, science of security, simulation, Testing, Validation and Verification, WebGME
Abstract	Developers of information systems have always utilized various visual formalisms during the design process, albeit in an informal manner. Architecture diagrams, finite state machines, and signal flow graphs are just a few examples. Model Integrated Computing (MIC) is an approach that considers these design artifacts as first class models and uses them to generate the system or subsystems automatically. Moreover, the same models can be used to analyze the system and generate test cases and documentation. MIC advocates the formal definition of these formalisms, called domain-specific modeling languages (DSML), via metamodeling and the automatic configuration of modeling tools from the metamodels. However, current MIC infrastructures are based on desktop applications that support a limited number of platforms, discourage concurrent design collaboration and are not scalable. This paper presents WebGME, a cloud- and web-based cyberinfrastructure to support the collaborative modeling, analysis, and synthesis of complex, large-scale scientific and engineering information systems. It facilitates interfacing with existing external tools, such as simulators and analysis tools, it provides custom domain-specific visualization support and enables the creation of automatic code generators.
DOI	10.1016/j.procs.2014.05.227
Citation Key	4630

Groups: Science of SecUre and REsilient Cyber-Physical Systems (SURE)

model-based software; online collaboration; automatic code generation; web-based design environment WebGME cyberinfrastructure Evaluation and experimentation Foundations Validation and Verification Modeling Resilient Systems Science of Security Simulation Testing

VANDERBILT UNIVERSITY

FILE ARTIFACTS

CPS-VO » SCIENCE OF SECURITY VO » SCIENCE OF SECURE AND RESILIENT CYBER-PHYSICAL SYSTEMS (SURE) » FILES

Files

- Home
- Research Team
- Projects
- Meetings
- Members
- Modboard
- Forums
- Files
- COLLABORATE
- SUBGROUPS
- MEMBER INFO

EDIT GROUP | TRACK | CLONE | TAXONOMY | BROADCAST | PANELS | DEVEL | GROUP STATS

SURE: Topics	45.5 MB	9
Hierarchical Coordination and Control	35.88 MB	6
Science of decentralized security	3.21 MB	1
Reliable and practical reasoning about secure c...	3.21 MB	1
Evaluation and experimentation	3.21 MB	1
System Science of SecUrity and Resilience for C...	3.21 MB	[download file]
Education and outreach	0 bytes	0
SURE: Meetings	52.66 MB	10
Kickoff Meeting, Oct'14	52.66 MB	10
Covert flows and authentication in cyber, physi...	4.73 MB	[download file]
CPS Gets Noticed: IIC, IOT, IIOT...	773.24 KB	[download file]
Incentive Mechanisms for CPS Security	22.93 MB	[download file]
Model-Based Simulation for Evaluation of CPS Se...	3.23 MB	[download file]
Resilience and Security in Component-Based Soft...	3.02 MB	[download file]
Resilient Monitoring of Flow Networks	2.47 MB	[download file]
Resource Aware Large-Scale Malware Classification	2.31 MB	[download file]
Secure Control and Optimization for Cyber-Physi...	3.76 MB	[download file]
System Science of SecUrity and Resilience for C...	3.21 MB	[download file]
The Science of Decentralized Security for Cyber...	6.25 MB	[download file]

Select a folder to create a new subfolder.

Create Folder:

Create

File upload

Upload files to selected folder:

Upload files

MEETINGS

Meetings

Home
Research Team
Projects
Meetings
Members
Files
SUBGROUPS
MEMBER INFO

SURE Review Meeting - March 17-18, 2015

The SURE Project review meeting will be held Tuesday, March 17 through Wednesday, March 18, 2015. The meeting will be held at Vanderbilt University in Nashville, Tennessee. The address is **1025 16th Avenue South, Nashville, TN 37212**.

Please register for the meeting at http://cps-vo.org/sure/reviewmtg2015/registration.

Program Agenda

TUESDAY, MARCH 17, 2015	
1200 - 1300	*Registration	Lunch pickup* **Project Overview** Xenofon Koutsoukos (Vanderbilt)
1300 - 1345	**Evaluation Testbed** Peter Volgyesi and Himanshu Neema (Vanderbilt University)
1345 - 1430	**Science of Adversarial Risk in CPS** Yevgeniy Vorobeychik (Vanderbilt)
1430 - 1445	*Break*
1445 - 1530	**Incentive Mechanisms for CPS Security** Saurabh Amin (MIT)
1530 - 1615	**Malware Classification - Title TBD** Anthony Joseph (UC Berkeley)
1615 - 1700	**Modeling Privacy in Human CPS** Roy Dong (UC Berkeley)
WEDNESDAY, MARCH 18, 2015	
0830 - 0900	Check-In | Continental Breakfast
0900 - 0945	**Secure Computation in Actor Networks** Dusko Pavlovic (U of Hawaii)
0945 - 1015	**Attack-Resilient Observation Selection** Aron Laszka (Vanderbilt University)
1015 - 1045	**Resilient Sensor Network Design for Flow Networks** Waseem Abbas (Vanderbilt University)
1045 - 1100	Break
1100 - 1145	**Resilient CPS - Title TBD** Claire Tomlin (UC Berkeley)
1145 - 1215	**Resilient and Secure Component-Based Software for CPS Architectures** Gabor Karsai (Vanderbilt University)
1215 - 1315	Lunch Pickup **Science of Security Virtual Organization** Katie Dey (Vanderbilt University)
1315 - 1345	**Demo: Resilient and Secure Component-Based Software for CPS Architectures** William Emfinger and Pranav Kumar (Vanderbilt University)
1345 - 1430	**Information Flow Policy in CPS** Janos Sztipanovits (Vanderbilt University)
1430 - 1500	Wrap-up and feedback
1500	Meeting adjourned

RSITY

PRESENTATIONS

INTERNAL WORKING GROUP

CPS-VO

Science of SecUre and REsilient Cyber-Physical Systems (SURE), internal

EDIT GROUP | TRACK | CLONE | TAXONOMY | BROADCAST | PANELS | DEVEL | GROUP STATS

- Home
- Calendar
- Members
- Activity Stream
- Modboard
- Reporting
- Forums
- Files

COLLABORATE

SUBGROUPS

MEMBER INFO

Welcome

This is a private group accessible only to team members from Berkeley, U of Hawaii, MIT, and Vanderbilt.

Quick Links

- Public SURE group: http://cps-vo.org/group/sos/sure *(Currently private)*
- Science of Security VO group: http://cps-vo.org/group/sos
- Science of Security Lablet groups: CMU, NCSU, UMD, UIUC

Project List: http://cps-vo.org/node/17238

Previous quarterly SoS Lablet meeting archives:

- 2014: CMU
- 2013: NCSU, UIUC, CMU
- 2012: NCSU, UIUC, CMU

Previous SoS community meeting archives:

- 2014 Symposium and Bootcamp on the Science of Security
- 2012 Science of Security Community Meeting

Teleconference Particulars

USA Toll-Free: 888-446-7584
USA Caller Paid/International Toll: 212-372-3742
Participant code: 8363915

Upcoming Events

04/21/15 - 04/22/15
2015 Symposium and Bootcamp on the Science of Security (HotSoS)

07/14/15 - 07/15/15
SoS Quarterly Lablet Meeting at CMU

10/13/15 - 10/14/15
SoS Quarterly Lablet Meeting at UMD

more ▶

Past Events

01/06/15 - 01/07/15
Quarterly SoS Lablet Meeting

10/28/14 - 10/29/14
Quarterly SoS Lablet Meeting

10/30/14 - 10/31/14
CONFLICT: Bill McKeever

10/30/14
Conflict: Gabor

more ▶

VANDERBILT UNIVERSITY

INTERNAL WORKING GROUP

CPS-VO » SCIENCE OF SECURITY VO » SCIENCE OF SECURE AND RESILIENT CYBER-PHYSICAL SYSTEMS (SURE) » SCIENCE OF SECURE AND RESILIENT CYBER-PHYSICAL SYSTEMS (SURE), INTERNAL » REPORTING

Reporting

Home
Calendar
Members
Activity Stream
Modboard
Reporting
Forums
Files

COLLABORATE
SUBGROUPS
MEMBER INFO

EDIT GROUP | TRACK | CLONE | TAXONOMY | BROADCAST | PANELS | DEVEL | GROUP STATS

NEW PROJECT REPORT

Title	Quarter	Institution	Workflow
	Aug-Oct 2014 Nov'14-Jan'15	MIT U of Hawaii UC Berkeley Vanderbilt	In Progress Ready for Review Accepted

Research Thrust(s)

Cyber risk analysis and incentive design
Hierarchical Coordination and Control
Resilient monitoring and control
Science of decentralized security
Reliable and practical reasoning about secure computation and communication in netwo
Evaluation and experimentation
Education and outreach

Apply | Reset

Project Title	Quarter	Hard Problem(s)	Status	Created	Updated
Risk Analysis and Incentive Design & Resilient Monitoring and Control	Aug-Oct 2014	Cyber risk analysis and incentive design, Hierarchical Coordination and Control, Resilient monitoring and control	Accepted	Mar 3 2015 - 5:52pm	Mar 3 2015 - 5:52pm
Risk Analysis and Incentive Design & Resilient Monitoring and Control	Nov'14-Jan'15	Cyber risk analysis and incentive design, Hierarchical Coordination and Control, Resilient monitoring and control	Accepted	Mar 3 2015 - 5:26pm	Mar 3 2015 - 5:26pm
Resilient Sensor Network Design For Infrastructure Flow Networks	Nov'14-Jan'15	Resilient monitoring and control	Accepted	Feb 20 2015 - 10:22am	Mar 3 2015 - 5:55pm
Evaluation Testbed	Nov'14-Jan'15	Evaluation and experimentation	Accepted	Feb 19 2015 - 10:05pm	Mar 3 2015 - 5:55pm
Resilience and security in component-based software architectures for CPS	Nov'14-Jan'15	Resilient monitoring and control	Accepted	Feb 19 2015 - 9:39pm	Mar 3 2015 - 5:55pm
Science of Trust and Running Actor Networks	Nov'14-Jan'15	Reliable and practical reasoning about secure computation and communication in networks	Accepted	Feb 19 2015 - 9:02pm	Mar 3 2015 - 5:55pm
Price of Anarchy in Decentralized Security	Nov'14-Jan'15	Science of decentralized security	Accepted	Feb 9 2015 - 3:51pm	Mar 3 2015 - 5:55pm
Secure Control, Optimization, and Machine Learning for CPS	Aug-Oct 2014	Hierarchical Coordination and Control, Science of decentralized security	Accepted	Oct 30 2014 - 6:23pm	Feb 19 2015 - 8:45pm
Resilient Sensor Network Design For Flow	Aug-Oct	Resilient monitoring and control	Accepted	Oct 30 2014	Feb 19 2015 -

SPONSOR REPORTING GROUP

CPS-VO

Science of SecUre and REsilient Cyber-Physical Systems (SURE), reporting

- Home
- Members
- Forums
- Files

COLLABORATE

SUBGROUPS

- Science of Security VO
  - CMU Science of Security Lablet Research Initiative
  - NCSU Science of Security Lablet Research Initiative
  - Science of SecUre and REsilient Cyber-Physical Systems (SURE)
    - Science of SecUre and REsilient Cyber-Physical Systems (SURE), internal
    - Science of SecUre and REsilient Cyber-Physical Systems (SURE), reporting

MEMBER INFO

This is the private reporting website accessible to members of this group only.

Quarterly Technical Reports

Year 1

- **Quarter 1:** August 1, 2014 - October 31, 2014
- **Quarter 2:** November 1, 2014 to January 31, 2015

Publications, Presentations, and Posters

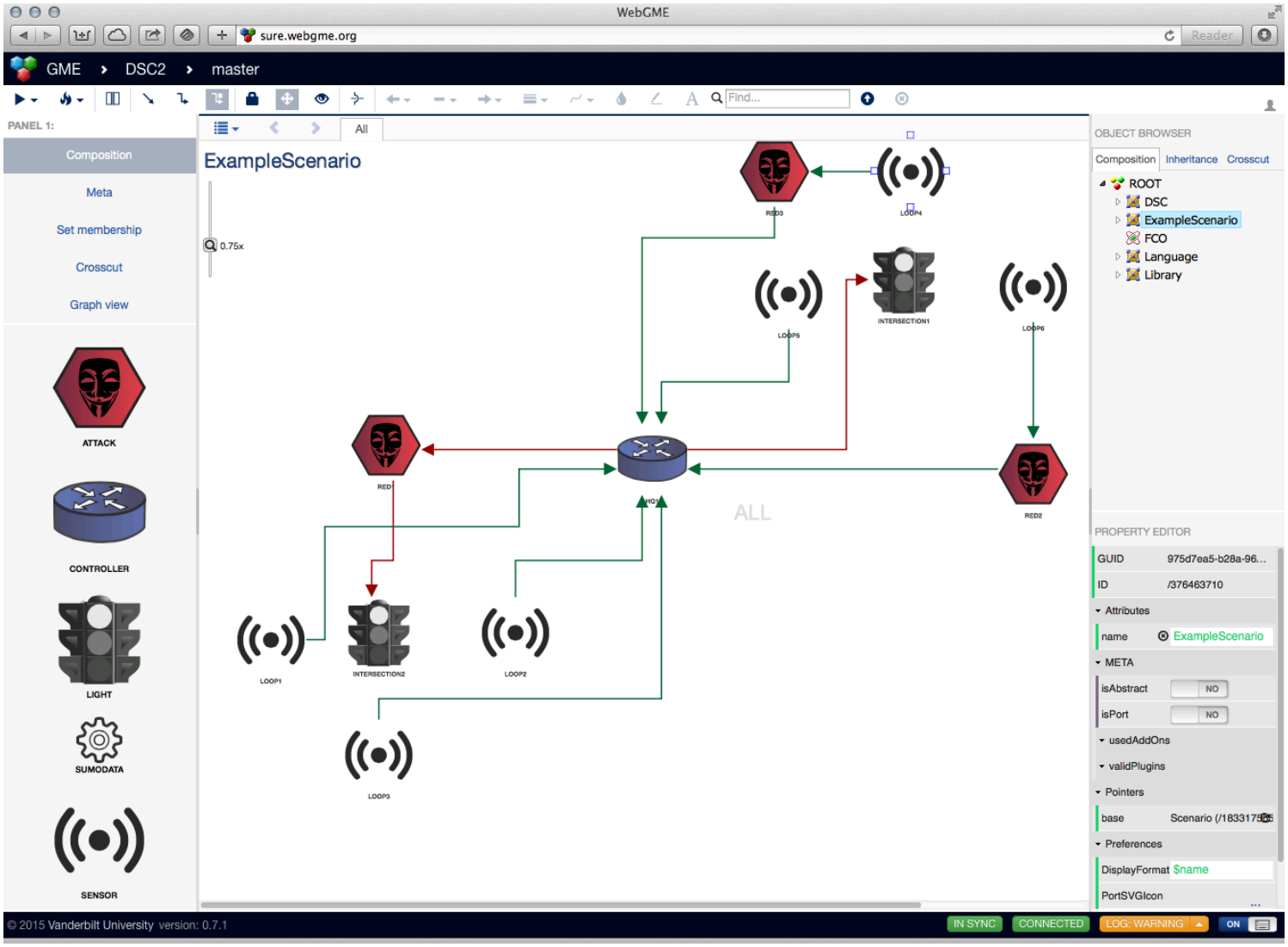
Year 1

- Quarter 1
- Quarter 2

TY

WHAT'S NEXT?

- **Publish tools and software**



THANK YOU

SURE site

http://cps-vo.org/group/sos/sure

Katie Dey

katie.dey@isis.vanderbilt.edu

AGENDA

SURE

0830 – 0900: Check-In | Continental Breakfast

0900 – 0945: **Secure Computation in Actor Networks**
Dusko Pavlovic (U of Hawaii)

0945 – 1015: **Attack-Resilient Observation Selection**
Aron Laszka (Vanderbilt University)

1015 – 1045: **Resilient Sensor Network Design for Flow Networks**
Waseem Abbas (Vanderbilt University)

1045 – 1100: Break

1100 – 1145: **Using Machine Learning to Improve the Resilience of Control**
Claire Tomlin (UC Berkeley)

1145 – 1215: **Resilient and Secure Component-Based Software for CPS Architectures**
Gabor Karsai (Vanderbilt University)

1215 – 1315: Lunch Pickup

Science of Security Virtual Organization
Katie Dey (Vanderbilt University)

1315 – 1345: **Demo: Resilient and Secure Component-Based Software for CPS Architectures**
William Emfinger and Pranav Kumar (Vanderbilt University)

1345 – 1430: **Information Flow Policy in CPS**
Janos Sztipanovits (Vandebilt University)

1430 – 1500: Wrap-up and feedback

1500 Adjourned