Research Spotlight Forum

8.6.19 Cybersecurity

NMT Cybersecurity Centers

PRESENTED BY:

Lorie M. Liebrock, Director, Cybersecurity Centers

Cybersecurity Education Center & COE Cybersecurity Economic Dev.

Lorie.Liebrock@nmt.edu

Sandia National Laboratories | Georgia Institute of Technology | Illinois | Purdue University | The University of Texas at Austin | The University of New Mexico | NM State University | New Mexico Tech Science • Engineering • Research University

SAND2019-9382 PE

Institute for Complex Additive Systems Analysis (ICASA)

ICASA is a legislatively-chartered research institute housed at New Mexico Tech:

- **Focus**: applying complex-systems theory to problems of national-security and critical infrastructure interest
- **Background**:
  - Focus on data science, modeling/simulation, and analyst-in-the-loop enabling technology development
  - Emphasis on giving undergraduate and graduate students with diverse STEM backgrounds real-world experience
  - Federal, State, Municipal, International, and Private-Sector customers
- **Historical Cybersecurity:**
  - Incubated NM-based cybersecurity company RiskSense as an evolution to providing first-response to state-agency cyber incidents
  - Joint patent on detecting global internet disruption due to malicious / natural events
- **Current Work**:
  - Process Analysis for Cyber Operations (PACO): Hierarchical Task Decomposition based analysis of distributed sensor data for cyber intrusion detection
  - Development of a Cyber-Physical test environment in conjunction with the Playas Research and Testing Center
  - Direct collaboration with NMT Cybersecurity Center of Excellence as well as incident response support to NMT campus IT department

ABOUT Aly El-Osery

Dr. Aly El-Osery is a Professor of the Electrical Engineering and Acting Dean of Graduate Studies. His research interests are in the areas of inertial navigation and RF based aiding sensors, electronic warfare, navwar, multi-agents robotics, wireless communications, control systems, sensor networks and soft computing. He has over 65 journal, book chapters, and conference publications in these areas. He is a senior member of IEEE and several of its societies including Systems Man and Cybernetics Society, and Communication Society.

Keywords:

Inertial navigation, Estimation algorithms, GNSS (Global Navigation Satellite System).

CURRENT WORK IN CYBERSECURITY

Cyber-Electronic System Security is a the cornerstone of protecting most of our critical infrastructure. Protection of information being communicated between geographically distributed systems, e.g., systems relying on position, navigation, and time is the focus of this research.

"The U.S. Department of Homeland Security identifies 16 critical infrastructure, and has stated that 11 of those rely upon satellite timing signals as an essential part of their operation. And all 16 sectors use satellite navigation and timing to some degree. This is true across the globe. Any system that depends upon a single source for anything is fragile and subject to rapid and unanticipated disruption or failure." -- The Resilient Navigation and Timing Foundation

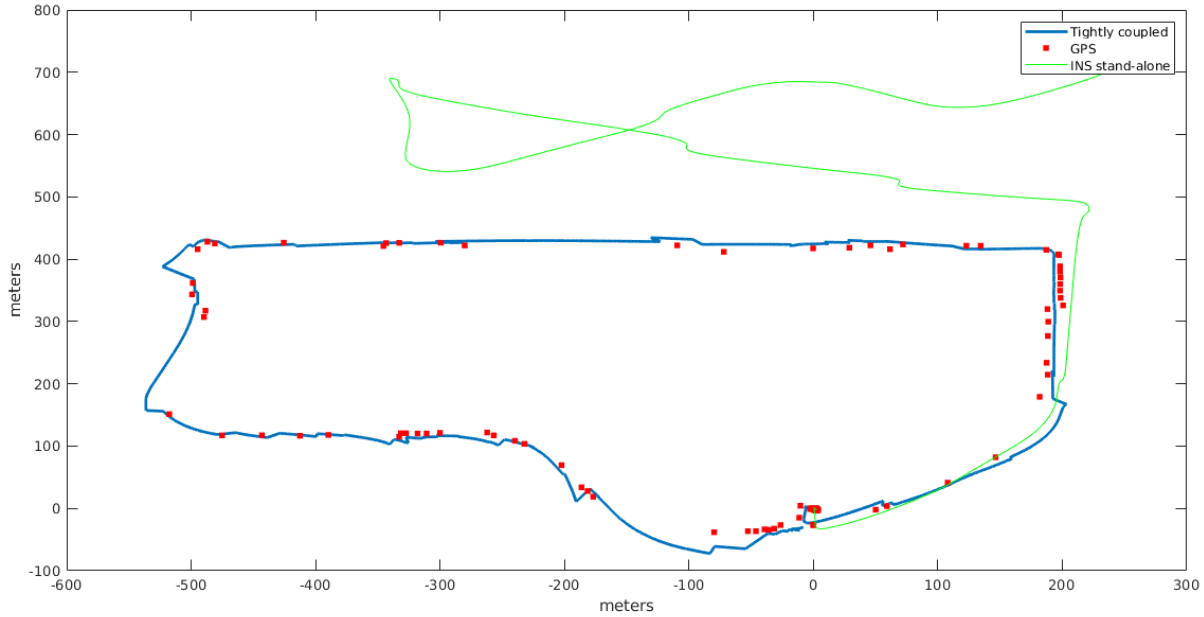
Leveraging signals of opportunity such as GNSS, existing RF infrastructure, imaging we are able to aide inertial navigation systems and provide position, navigation and timing at times where there are no GPS signals, its being maliciously jammed, or being indoors.

Using tightly coupled configuration to fuse information from WiFi, GNSS pseudorange and Doppler with Inertial Navigation systems.

FUNDING SOURCES

Applied Technology Associates – New Mexico Tech and Georgia Tech are subcontractors developing GNSS augmentation system.

Figure shows NMT contribution of implementing tightly coupled configuration and providing more reliable positioning information compared to IMU alone or GPS alone.



ABOUT Dr. Dongwan Shin

PhD. in Information Technology (UNC Charlotte, 2004)

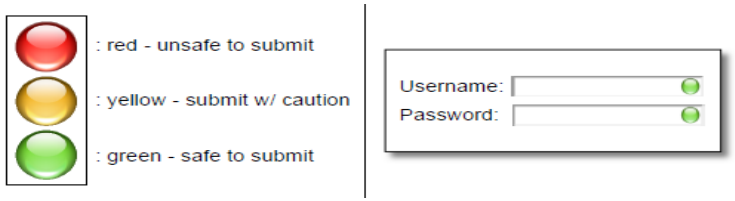
- Associate professor of CSE
- Director of Secure Computing Lab (http://scl.cs.nmt.edu)

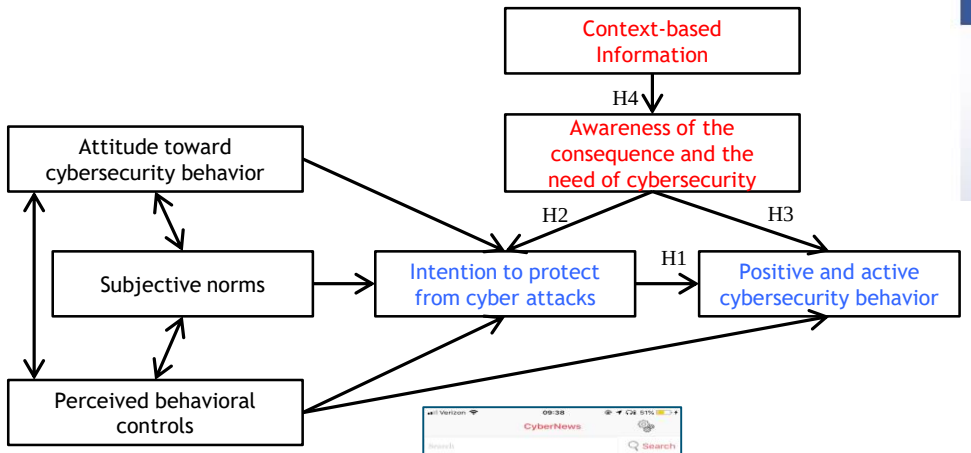
Research focuses on computer security & privacy

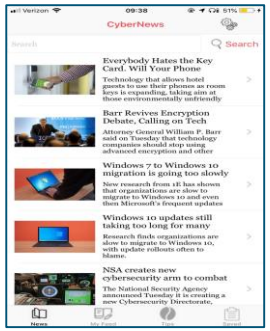
Usable Security

Visual Cue-based Solution to Enable an Informed Decision

- SSLight solution on Google Chrome







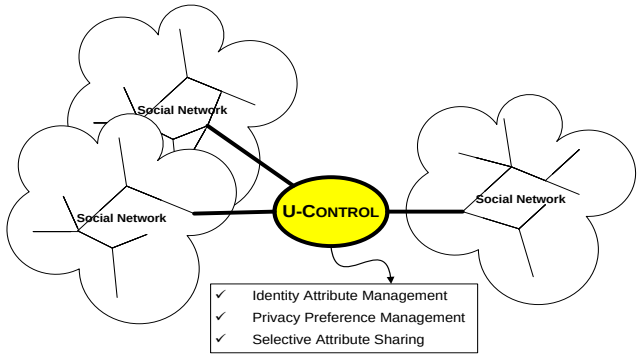
Behavior control-based Approach to Influencing User's Cybersecurity Actions (NSF)

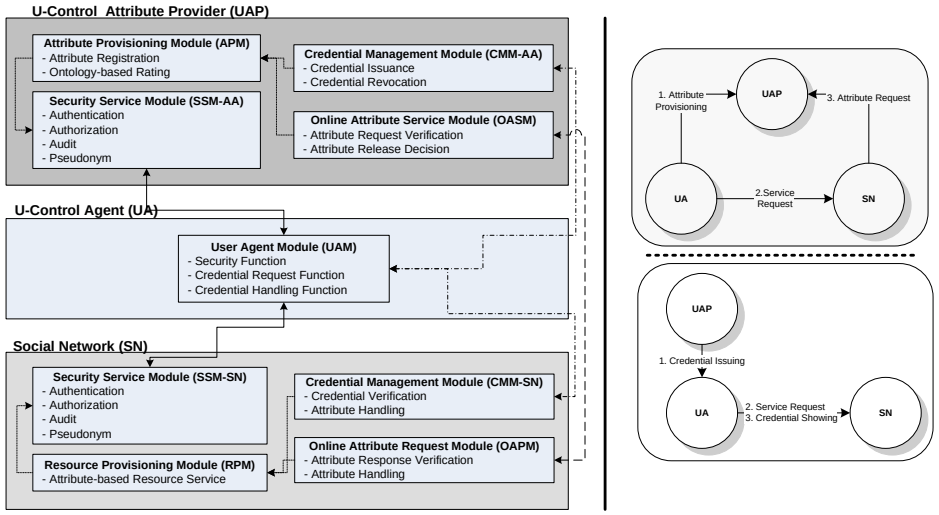
- Research framework to test hypotheses that context-based information has positive impacts on behavior
- Cylore application that provide a real-time security news based on context information such as WiFi type, search history, app usage, etc

User-centric Privacy

User-centric Digital ID & Privacy Control in SNS (NSF, ~2013)

- Selective Sharing of Attributes
- Composition of Attributes
- Open Source-based Design/Imp.





A) Functional Component-based System Architecture

B) Two Operational Architectures

User-centric Privacy for Smart Grids (NSF EPSCoR, 2018~)

- Differential Privacy
- Risk-based Privacy Framework
- Selective Sharing of Power Data

ABOUT Dr. Jun Zheng

- Ph.D. in Computer Engineering, UNLV, 2005
- Assistant Professor, Computer Science, Queens College, City University of New York, 2005-2008
- Assistant Professor, Computer Science, New Mexico Tech, 2008-2013
- Associate Professor, Computer Science, New Mexico Tech, 2013-Current
- **Research areas**: Mobile Security, Network Security, Smart Grid Security, Mobile HCI, Machine Learning and its Applications
- **Human-centered Computing and Security Lab**: 1 Ph.D., 2 M.S., 3 Undergraudates

Keywords:

Cybersecurity, Smart Grids, Smartphones, Machine Learning, Biometrics

CURRENT WORK IN CYBERSECURITY

- Smart grid security
  - light-weight authentication protocols for smart grids
  - Multi-modal biometrics authentication for electrical vehicles (EVs)
  - Secure group communication in ICN-based networking and communication infrastructure for smart grids
  - Distributed data-driven cyber-physical intrusion detection system for smart grids

- Mobile security
  - Novel screen unlock schemes for mobile devices
  - Enhacing Android pattern unlock with biometrics
  - Mobile malware detection using advanced machine learning techniques

FUNDING SOURCES

- RII Track-1: The New Mexico SMART Grid Center: Sustainable, Modular, Adaptive, Resilience, and Transactive, NSF OIA-1757207, PI at New Mexico Tech.
  - 20 million, 5-year NSF EPSCoR grant involves the University of New Mexico, New Mexico State University, New Mexico Tech, Santa Fe Community College, Sandia Laboratories, Los Alamos National Laboratory, and other organizations in New Mexico such as the Microgrid Systems Laboratory and Explora Museum.
  - New Mexico Tech is the leading institution to address the security and privacy challenges of the proposed SMART grid infrastructure.

- REU Site: Research Experiences for Undergraduates - Emerging Issues in Cybersecurity, NSF CNS-1757945, PI
  - 10-week summer Research Experiences for Undergraduates (REU) program.
  - Undergraduate students are supervised by faculty mentors to work on various cybersecurity research projects.

ABOUT Sihua Shao

Biography

- Visiting Faculty Electrical Engineering and Cybersecurity Centers
- PhD New Jersey Institute of Technology
- Dissertation: "Design, Analysis and Optimization of Visible Light Communications based Indoor Access Sytstems for Mobile and Internet of Things Applications"

Research Area

- Communications using Visible Light
- Intelligent Vehicle Communication Sensing and Positioning
- Localization for IoT devices
- Retroreflective Transportation Infrastructure

ABOUT Jizhou Tong

Biography

- Visiting Faculty in Computer Science and Engineering and Cybersecurity Centers
- PhD in Computer Science, The University of Toledo
- Dissertation: "Design and Implementation Security Testbed (HANSim) and Intrusion Detection Systems (IDS) for the Home Area Network in the Smart Grid"

Research Area

- Security of Information Flow Systems in Smart Homes
- Simulation Testbed for Home Area Networks
- Attack Simulation Approaches for Smart Homes
- Intrusion Detection Systems for Smart Home Networks
- Attack Prevention Systems for Smart Home Networks

ABOUT Lorie M. Liebrock

Biography

- Director of Cybersecurity Centers,
- Scholarship for Service PI,
- Professor of Computer Science, Former Dean of Graduate Studies
- PhD, Computer Science, Rice University

Research Area

- Transdisciplinary Cybersecurity Data Analytics and Emulytics for Enterprise-wide Cybersecurity

Research Group

- 4 PhD Students, 7 Masters Students, 9 Bachelors Students

Keywords:

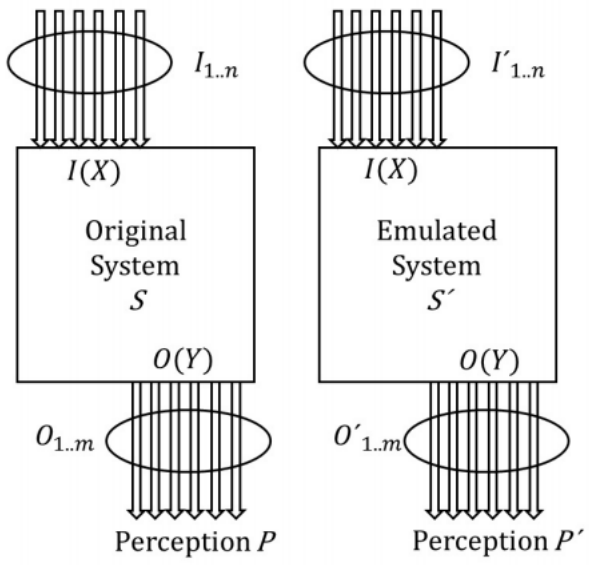
- Enterprise-wide Cybersecurity, Emulytics, Data Analysis, Visualization, and Parallel Processing

CURRENT WORK IN CYBERSECURITY

My group works across a variety of research areas in cybersecurity, primarily focused on enterprise-wide cybersecurity challenges including threat intelligence gathering and processing, emulytics, system process models.

Collection of a broad array of data and exploration of analytics methods to model the relationships between logs and online data sources. Analytics methods being explored include temporal analysis, network analysis, statistical analysis, and visualization.

Emulytics – we explore emulation of systems (entire network and operating system stack) as a means to understand and develop cyber deception.



Characterization of what a system (including enterprise computer network deployment, servers, end user devices, networking equipment, etc.) is doing to build process models that support understanding the state space of the enterprise. Essentially this makes the network a sensor for defenders to analyze what is happening in normal business processes versus adversarial processes.

FUNDING SOURCES

National Science Foundation – Scholarship for Service Program

Sandia National Laboratory – Emulytics

State of New Mexico

- Cybersecurity Education Center
  - Developing Transdisciplinary Cybersecurity Graduate Programs
  - Outreach to students across New Mexico to promote opportunities and improve cyber hygiene
- Center of Excellence in Cybersecurity Economic Development
  - Developing Cybersecurity Entrepreneurship Endeavors in New Mexico
  - Outreach to Companies and Municipalities in New Mexico to improve cyber hygiene and understand needs

Cybersecurity Education Center

The Cybersecurity Education Center (CEC) is an academic center at New Mexico Tech that is focused on cybersecurity education at both the undergraduate and graduate levels. The principal goals of the CEC are to educate undergraduate and graduate students in cybersecurity issues, and to provide them with the knowledge and skills needed to work and lead as cybersecurity professionals.

Goals:

- Improve Cybersecurity Hygiene in New Mexico Schools and Homes
- Increase Cybersecurity Education and Employment Opportunities in New Mexico
- Increase Awareness of Cybersecurity Opportunities in New Mexico

Needs

- Collaboration in Outreach, Education, and Research
- Collaboration and Coordination of Academic Programs Statewide
- Internship and Employment Opportunities
- Opportunity to update and resubmit MSIPP proposal for Cybersecurity Data Science

https://www.nmt.edu/academicaffairs/cybersecurity_centers/CybersecurityEducationCenter.php

Cybersecurity Center of Excellence in Economic Development

The Cybersecurity Center of Excellence (CCE) is a state-wide economic development center. The Center will serve as a catalyst for cybersecurity research, and workforce development in New Mexico by coordinating and facilitating collaborations among NM colleges and universities, government agencies and the private sector.

Goals:

- Improve Cybersecurity Hygiene in New Mexico Businesses and Municipalities
- Increase Cybersecurity Entrepreneurship and Innovation in New Mexico
- Increase the Number of Businesses and Employment in the Cybersecurity Industry in New Mexico\

Cybersecurity Entrepreneurship Workshop

- September 27, 2019 (11:30am – 5pm), Fidel Center, New Mexico Tech campus
- This workshop will bring together cybersecurity ideas, problems, and challenges with entrepreneurial opportunities to grow the cyber economy of New Mexico
- Energy Sector Cybersecurity Concerns Analysis

Needs

- Collaboration on Entrepreneurship, Innovation, Economic Development, and Employment

https://www.nmt.edu/academicaffairs/cybersecurity_centers/CybersecurityCenterOfExcellence.php