Special Cyber Operations Research & Engineering

Computational Cybersecurity in Compromised Environments

C3E

Welcome to the C3E Mid-Year Event!

May 11, 2016

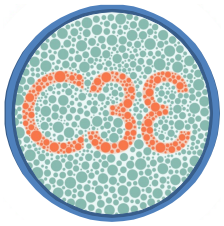
Computational Cybersecurity In Compromised Environments (C3E)

Workshop on Cyber Consequences

Wednesday, 11 May 2016

What is C3E?

- C3E workshops initiated to develop novel solutions to the rapidly changing cyber security landscape
  - As an unclassified WORKshop
  - With an emphasis on diversity of disciplines
  - With a focus from the conceptual to the practical; increasing emphasis on the practitioner
- Sponsored by the Special Cyber Operations Research and Engineering (SCORE) Committee



What is C3E?

- C3E gatherings and their emphasis
  - 2009 (Santa Fe, NM) to understand how adversaries have insinuated themselves into our systems and networks, and the extent to which computational and other analytic approaches could be leveraged to mitigate their influence
  - 2010 (Santa Barbara, CA) to understand state-of-the art models and data practices could inform strategy and tactics for the practitioner
  - 2011 (Keystone, CO) to discuss predictive analytics and the role of intersecting anomalies and emergent behavior in supporting them
  - 2012 (West Point, NY) to discuss cognitive and other influences on decision making in cyberspace and how to best visualize data
  - 2013 (West Point, NY) to discuss navigation in cyberspace and consequences of action in cyberspace
  - 2014 (Atlanta, GA) to discuss data integrity and security by default.
  - 2015 (Pittsburgh, PA) to discuss adaptive defense and identifying the adversary

What is C3E?

- C3E is also a *community of interest* focused on novel approaches and solutions needed, drawn from multiple areas
  - Starting in C3E 2011, we drew heavily from the astronomy, behavioral sciences, biomedical informatics, financial assessment, and other areas.
  - C3E 2012 Challenge problem involving epidemiological intelligence reaffirmed the value of analytic diversity for emerging problems; C3E 2013/4 Challenge Problems focused more directly on cyber security
  - COI has potential to look at slightly broader class of problems and solutions while still keeping an eye on cyber security
- The major objective for the day is to focus the broad track themes into specific issues and threads to focus on in this year's C3E, tentatively scheduled for October 2016.
  - Including potentially useful data sets
  - Including potential track leadership and approaches

SCORE Research Priorities for FY16

a) Security in a Transparent World
Continuously Evolve Resilient Capabilities
Operations in Compromised Environments

b) Cyber Intelligence in Context
Understanding and anticipating adversary Tactics, Techniques and Procedures; Predictive warning
Continuous mapping and measurement of the Internet and beyond
Situational Awareness that enables decision making

c) Cyber Deterrence - Shifting the Balance in Cyber Threats
Security by Default; Eliminate the known 80% Vulnerabilities
Moving Target Technologies and Adaptive Resilient Defense
Cyber and Non-Cyber Deterrence Mechanisms and Incentives
Cyber Denial and Deception

d) Understanding The Cyber Environment
Modeling and Simulation
Metrics, Measurement, Analysis, and Risk Management

e) Ensuring Integrity of Data, Information, and Systems
Improved Analytic Tradecraft; Quantifying and Understanding Uncertainty
Roots of Trust for Systems and Information
Supply Chain, Data Quality, Anti-tamper, and Data/Information Flow Analysis Techniques
Insider Threat Prevention, Detection, and Damage Mitigation

Themes and Approach

- Overarching C3E workshop theme for 2016 is Cyber Consequences
- Today's session will focus on Understanding Cyber Dependencies and Analytic Context for Understanding Resilience, the proposed track themes for C3E 2016.
- All participants will be involved in discussing both track themes
- Use of facilitation and worksheets to capture everything from brilliance to stray thoughts
- End of day review should emphasize both substantive and process/people thoughts about the October C3E event

C3E Workshop on Cyber Consequences
Agenda

0800-0900	Arrival at the Keck Center, 500 Fifth St. NW, Washington, DC	
0900-0910	**Welcome**	
	Opening Remarks	Kathy Bogner
0910-0935	Lightning Round (Mini-Introductions)	
0935-0945	C3E Recap Briefing	Kevin O'Connell & Dan Wolf
0945 – 1015	**Understanding Cyber Dependence – Network Mapping**	Walter Willinger, Niksun, Inc.
1015 – 1030	Morning Break	
1030– 1100	**Understanding Cyber Dependence - Use Case**	Jason Lim, Transportation Security Administration
1100 – 1215	Content Development Session: Understanding Cyber Dependence	

C3E Workshop on Cyber Consequences Agenda

1215 – 1315	Working LUNCH 2106 Challenge Problem Discussion	Dan Wolf, Chip Willard
1315 – 1400	**CyberSecurity Data in Context**	Marco Carvalho, Florida Institute of Technology
1400 – 1415	Afternoon Break	
1415 – 1545	Content Development Session: CyberSecurity Data in Context	
1545 – 1615	Development Session Out Briefs	
1615 – 1630	Closing Remarks & Next Steps	Brad Martin
1630	Workshop Adjourns	

Understanding Cyber Dependence – Initial Questions

Our inability to understand cyber dependence is a long-standing problem. Failure to understand the linkages, values and priorities of defensive actions limits proper planning and courses of action. Key analytic challenges here are approaches to validate known dependencies and uncover unknown ones.

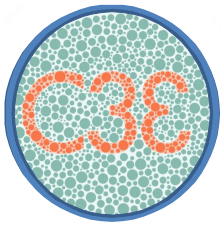
- What analytic methods or tools inform us of our interdependencies, and at what confidence levels?
- What is state-of-the-art in understanding links and nodes within networks and systems?
- What level of detail can we define and describe with a view toward decision-making?
- What new approaches can inform our thinking about this? What capabilities are needed to delineate the degree of dependence that is acceptable for decision-making?

Improving Analytic Frameworks for Resilience – Initial Questions

The Federal Cyber R&D Strategy (2016) defines resilience as "the ability to prepare for and adjust to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."

In order to achieve resilience and agility in cyberspace, we have to better understand the context of actions by others.

- How can analytic frameworks — such as the pursuit of enhanced context — be applied in order to maximize courses of action?
- How can we formalize context in order to improve insights about risk of action to decision-makers?
- What tools are available and/or needed that can help us to tailor investments so that risk can be more easily managed?\
- How would we define analytic context in the cyber realm?
- What kinds of data are potentially helpful as contextual data?
- What are the best practices of capturing, measuring, evaluating these kinds of data?



C3E Challenge/Discovery Problem

- Identity Discovery Challenge (2012)
- APT Infection Discovery Using DNS Data (2013)
- Metadata-based Malicious Cyber Discovery (2014)
- Approaches to Avoid Misattribution of Malicious Cyber Activity (2015)
- **Modeling Consequences of Ransomeware on Critical Infrastructure** (2016)

Administrative Issues

- Today's session is UNCLASSIFIED
- Please do not broadcast anything from this session into the social media sphere or elsewhere
- Remember that the person next to you may have a very different background than you; diversity strengthens the approach if barriers can be broken

Looking Ahead to the Fall C3E Workshop

We look forward to your continued participation with the extended C3E Community at our Fall C3E Workshop!

- Hosted by the Georgia Technology Research Institute (GTRI), http://gtri.gatech.edu/
- 17-19 October 2016
- Details available soon on the C3E.Info website, by invitation only