CyDentity Sandpit

Homeland Security
Science and Technology

JUNE 29-JULY 1, 2015

Hosted by:

CCICADA Center of Excellence, Rutgers University, the State University of NJ - Busch Campus
7th Floor (Room 701), CoRE Building | 96 Frelinghuysen Road, Piscataway, NJ 08854-8018

Sponsored by:

U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Cyber Security Division (CSD)

Welcome Reception (June 29):

5:30-7:30pm **Welcome Reception**
The Old Bay Restaurant - New Jersey's premier New Orleans-style restaurant!
61-63 Church Street, New Brunswick, NJ 08901
Website: http://www.oldbayrest.com/

Day 1 (June 30): 8:00AM – 5:00PM

Topic	Discussion Details	Who	Location	Start
Registration & Coffee	Registration	ALL	Rm 701	8:00 AM
Welcome and Opening Remarks	- Welcome from CCICADA/Rutgers - Welcome from DHS S&T CSD - Background on DHS S&T CSD's interest and vision - Meeting objectives, attendees and format	Fred Roberts, Rutgers University Doug Maughan, DHS S&T Joe Kielman, DHS S&T Emily Saulsgiver, Meeting Facilitator	Rm 701	8:30 AM
Session A: Provocateur Panel	- What are the gaps in identity research? - What does this community need to focus on?	Anil John (Moderator), DHS S&T CSD Andrew Nash, Confyrm Ian Glazer, Salesforce Steve Wilson, Lockstep	Rm 701	9:00 AM
Session B: Review Theme Challenge Statements	-Are we missing anything in the Themes? -Overview of Breakout Group objectives -Introduce Concept Templates	Emily Saulsgiver	Rm 701	10:00 AM
Networking Break		All	Rm 701	10:20 AM
Session C: Break-out into Concept Groups	- Discuss research challenges within Theme 1: Identity Proofing in the Era of Social Media and Data Breaches - Determine research domains required to address	Kaliya, Leola Group (Moderator) Ryan Whytlaw (Knowledge Agent)	Rm 701	10:40 AM
	- Discuss research challenges within Theme 2: Provenance for the "Internet of Things" - Determine research domains required to address	Dave Thurman, PNNL (Moderator) Charles File (Knowledge Agent)		

	- Discuss research challenges within Theme 3: Metrics for Trust - Determine research domains required to address	Dennis Egan, Rutgers (Moderator) Jonathan Bullinger (Knowledge Agent)		
Lunch	Luncheon Presentation	Nina Fefferman, Rutgers University	Rm 401	12:00 PM
Session D: Group Lightning Summaries	-Short brief-out by Moderators on Breakout discussion high-points	Kaylia Dave Thurman Dennis Egan	Rm 701	1:00 PM
Session E: Gallery Walk & Research Theme Development	-Self-organizing small groups -Draft templates on potential research efforts to address aspects of challenge statements	ALL	Rm 701	1:30 PM
Networking Break		ALL	Rm 701	2:30 PM
Session F: Provocateur Panel 2 – Insights from the Day	- Further Comments to the group based on breakout groups and concept discussions	Anil John, DHS S&T CSD (Moderator) Andrew Nash, Confyrm Ian Glazer, Salesforce Steve Wilson, Lockstep	Rm 701	2:45 PM
Session G: Concept Refinement & Posting	- Refine templates and add to the front wall	ALL	Rm 701	3:45 PM
Session H: Concept Canvassing / Adjourn	-Canvassing options: (A) support this concept, (B) Support and can provide additional expertise	ALL	Rm 701	4:30 PM
CyDentity Project Team Meeting	Closed Meeting	CyDentity Organizers	Rm 701	5:00 PM

6:30pm **CyDentity Sandpit Dinner**
Panico's
103 Church Street, New Brunswick, NJ 08901
Website: http://www.panicosrestaurant.com/

DAY 2 (JULY1): 8:00AM – 1:00PM

Topic	Discussion Details	Who	Location	Start
Registration, coffee, and networking	Registration	ALL	Rm 701	8:00 AM
Welcome and Opening Remarks	- Recap of Day 1 - Discussion of high-level findings of Concept Themes - Identify where others may contribute to these ideas	Anil John Joe Kielman Emily Saulsgiver	Rm 701	8:30 AM
Session I: Concept Team Talks and Group Discussion	- Author teams give overview of concept (5 minutes each) - Group discussion	Concept Teams	Rm 701	9:00 AM
Working Lunch	Concept Template Refinement - Author teams update and build-out concepts based on group discussion	ALL	Rm 401	12:00 PM
CyDentity Sandpit Concludes	- Turn in final templates	Joe Kielman, Anil John, Emily Saulsgiver	Rm 401	1:00 PM

CyDentity Themes and Scenarios

CyDentity will combine expanded provenance, trust metrics, and identity proofing in a high-precision process that would secure cyber and critical infrastructures.

Theme 1: Identity Proofing in the Era of Social Media and Data Breaches

What challenges exist in each of the identity proofing steps with respect to balancing privacy with the need for data collection, ability to validate information when source authorities are not available, and lack of confidence in verification that depends on knowledge based questions which can be answered by mining social media or bought in underground forums that sell data from breaches. Mobility in the era of ubiquitous smart, portable devices, requiring identity proofing anywhere and anytime, further complicates these steps. Furthermore, if the goal is truly real-time functionality, the usability of proofing methods becomes a major concern.

Scenario: Anywhere/everywhere, anytime/always-on social media; a constant stream of data breaches; and national ID or identity cards. These are just a few of the aspects of our cyber environment being discussed in national-level conversations.

Key questions:

- To what level does the first topic contribute to the second?
- Is privacy possible or even desirable under such conditions? Or, is it even relevant?
- And would the third topic be a realistic way to mitigate the potential damage caused by the second?
- What should we know about the source or history of data to trust them?
- How do you know you can trust where your data came from or who sent it to you?
- What and how are decisions made regarding privacy within a network and information sharing systems?

Theme 2: Provenance for the "Internet of Things"

Provenance here refers to a recorded history of a digital object, which captures that object's point of creation and all subsequent transfers and transformations. Provenance must include the actions taken on or with an object and the actors who took them. Today, some type and level of provenance is available for some digital objects. The research challenge is expanding the notion of provenance such that it is universally available to ensure an acceptable level of trust in the identity of the objects.

Scenario: Today's critical infrastructures are often controlled by obsolete SCADA systems that were designed and built as closed ecosystems. None were meant to be interconnected nor connected to the chaotic world that is now represented by the Internet of Things.

Key questions:

- What are the threats?
- What challenges do infrastructures owners or providers face in protecting their systems and interconnections?
- How do we build smart cyber defenses useful for dumb Infrastructures?

- How would we then measure the security of an individual component, of a sector's infrastructure, and of the interconnected cyber-physical world?
- What do we protect and to what level and at what cost?
- How can we model individual and societal responses to cyber failures?
- How do people interact and react under various stress conditions?
- What are the interdependencies of infrastructure protection and societal practices?
- At what point does the system break down?
- What can we measure and use as indictors?

THEME 3: METRICS FOR TRUST

A third objective for the CyDentity program is to offer a method for quantifying and expressing the relative trust of our cyber infrastructures, digital objects, and cyber identities. Metrics and measurements could be helpful in specifying the level of security or trust attainable and in making decisions about how to select and allocate cyber defenses effectively. Metrics that involve the degree of expanded provenance and identity proofing attainable might need to be augmented with metrics for expressing the value of the data or information contained on networks.

Scenario: Fraud is an ever-present reminder that we as individuals and our computer systems consistently mistake the identity of those individuals or systems with whom and with which we interact. Money or identities are lost; infrastructures are compromised and rendered inoperative; illicit or counterfeit goods are exchanged. We engage in risk-taking behaviors without ever knowing the extent of the risks involved, and without consideration of the potential secondary effects on our communities and social infrastructures.

Key questions:

- Can we use risk as a proxy for trust in such situations?
- What does preventing fraud teach us about security-proofing our cyber systems?
- What types of tools are needed to communicate fraudulent access and activity?
- What does risk mean in a cyber-world?