27 Apr 2017

Weaponized Crowdsourcing: Threats and Opportunities (1:10-1:50 pm ET)

and

Secure Embedded Systems Research and Training in the Center for Reverse Engineering and Assured Microelectronics (CREAM) (2:00-2:40 pm ET)

Mark your calendars and come join your friends in the CAE community for a Tech Talk. We are a warm group that shares technical knowledge. CAE Tech Talks are free and conducted live in real-time over the Internet so no travel is required. You can attend from just about anywhere (office, home, etc.) Capitol Technology University (CTU) hosts the presentations using their online delivery platform (Adobe Connect) which employs slides, VOIP, and chat for live interaction. Just log in as “Guest” and enjoy the presentation(s).

Below is a description of the presentation(s) and logistics of attendance:

**Date:** Thursday 27 Apr 2017  
**Time:** 1:10-1:50 pm ET  
**Location:** [https://capitol.adobeconnect.com/cae_tech_talk/](https://capitol.adobeconnect.com/cae_tech_talk/)  
Just log in as “Guest” and enter your name. No password required.  
**Title/Topic:** Weaponized Crowdsourcing: Threats and Opportunities  
**Audience Skill Level:** All Levels
**Presenter(s):** Prof. James Caverlee, Texas A&M University, Department of Computer Science and Engineering

**Description:**

Crowdsourcing systems have successfully leveraged the attention of millions of “crowdsourced” workers to tackle traditionally vexing problems. From specialized systems like Ushahidi (for crisis mapping), Foldit (for protein folding) and Duolingo (for translation) to general-purpose crowdsourcing marketplaces like Amazon Mechanical Turk and Crowdflower - these systems have shown the effectiveness of intelligently organizing large numbers of people. However, these positive opportunities have a sinister counterpart: what we dub “Weaponized Crowdsourcing”.

Already we have seen the first glimmers of this ominous new trend – including large-scale “crowdturfing”, wherein masses of cheaply paid shills can be organized to spread malicious URLs in social media, form artificial grassroots campaigns (“astroturf”), spread rumor and misinformation, and manipulate search engines. Unfortunately, little is known about Weaponized Crowdsourcing as it manifests in existing systems, nor what are the ramifications on the design and operation of emerging socio-technical systems. Hence, this talk shall focus on key research questions related to Weaponized Crowdsourcing as well as outline the potential of building new preventative frameworks for maintaining the information quality and integrity of online communities in the face of this rising challenge.

**Date:** Thursday 27 Apr 2017

**Time:** 2:00-2:40 pm ET

**Location:** [https://capitol.adobeconnect.com/cae_tech_talk/](https://capitol.adobeconnect.com/cae_tech_talk/)

Just log in as “Guest” and enter your name. No password required.

**Title/Topic:** Secure Embedded Systems Research and Training in the Center for Reverse Engineering and Assured Microelectronics (CREAM)

**Audience Skill Level:** All Levels

**Presenter:** Dr. Kevin Kornegay from Morgan State University

**Description:**

The Internet of things (IoT) is the inter-networking of physical devices with microcontrollers/processors, software, sensors, actuators, and network connectivity that enable these devices to collect and exchange data. In a more general sense, IoT devices may also be classified as embedded systems. Critical infrastructure such as transportation, smart grid, manufacturing and health care are highly dependent on embedded systems for distributed control, tracking, and electronic data collection. While it is paramount
to protect these devices from hacking, intrusion or physical tampering, current solutions are often based on a patchwork of legacy devices, and this model is unsustainable in the long-term. Thus, we have established the **Center for Reverse Engineering and Assured Microelectronics (CREAM)** to provide the intelligence community with knowledge, solutions, and highly skilled hardware security engineers to help prevent penetration and manipulation of our nation’s critical infrastructures. To achieve this goal, we conduct hardware security research using reverse engineering techniques to evaluate the assurance of IoT devices. We also develop countermeasures and trusted platform module designs to secure these devices against sensitive data extraction, disruption, diversion, and obfuscation. In this talk, we will highlight some of the secure embedded systems research and student training activities.

### CAE Tech Talks are also recorded

Recordings of live presentations are posted to the website below:


Pdf versions of the presentations are posted to the website below:

[https://capitol.instructure.com/courses/510/files](https://capitol.instructure.com/courses/510/files)

### Contact

CAE Tech Talk events are advertised thru email and posted to the news and calendar section of the CAE community website: [www.caecommunity.org](http://www.caecommunity.org)

For questions on CAE Tech Talk, please send email to [CAETechTalk@nsa.gov](mailto:CAETechTalk@nsa.gov)