ECS Center for Cybersecurity Presents: Firewallside Chat Series Talk

Talk: Incident Response: Hackers in the system!

Date/Time: Thursday, May 5, 2016, 10:00 am – 1:00 pm

Location: Holiday Inn & Suites Fullerton
2932 East Nutwood Avenue, Fullerton, CA 92831

RSVP: http://bit.ly/1Wf7XyC

Firewallside Chats

ECS Center for Cyber Security hosts a series of talks called Firewallside Chats, featuring security experts discussing pressing issues in cyber security. The events aim to educate students, faculty, and the general public about cutting edge cyber security research and practice.

This Firewallside Chat is the is the last event of this semester. The events will resume in the fall

Incidence Response

Incident response is an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident).

The goal is to handle the situation in a way that limits damage and reduces recovery time and costs. An incident response plan includes a policy that defines, in specific terms, what constitutes an incident and provides a step-by-step process that should be followed when an incident occurs (source: http://searchsecurity.techtarget.com/definition/incident-response)

In this Firewallside Chat we are joined by an experienced team of security experts from Bechtel Corporation who will share the wisdom, knowledge, and stories about incident response. Bechtel is a civil engineering company responsible for many well known construction projects such as the Hoover Dam and invests heavily in protecting itself from the constant onslaught of cyberattacks.

Laura Chiu

IRMA: Incident Response & Malware Analysis

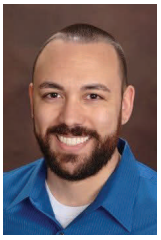
Laura will discuss the architecture and use of the open source tool for malware triage and how easy it is to create custom plugins for anti-virus scanners, commands, and even sandboxes. She will also cover how IRMA can be integrated with existing tools and used in automation efforts.

Chris Pavan

Beholder: Network Traffic Capture and Decoding using Commodity Hardware

Chris will step through how open source software coupled with commodity hardware can be used to create a robust packet capture and decoding appliance for network security and research. Attendees will learn how to easily create their own appliance and start capturing packets by the end of the day.

Ryan Chapman



Finding the Needle in a Binary Haystack with Log Aggregation

Ryan will discuss how to harness the power of a log aggregation system such as Splunk to find malicious actors and stop them in their tracks. He will discuss how the process of hunting can lead to the creation of saved searches that can identify anomalies and/or malicious activity.