**EN.650.621 Critical Infrastructure Protection Group Projects**

On May 11, 2017 the President signed an executive order entitled "Strengthening the Cybersecurity of **Federal Networks and Critical Infrastructure**." Section 1 addresses the Cybersecurity of Federal Network, where the focus is on **risk management** due mostly to "known but unmitigated vulnerabilities," **anomaly detection**, **recovery**, and **information sharing**. Section 2 mentions President Obama's February 12, 2013 Executive Order by name; thus, focusing on enhancing cyber security via cyber incident sharing and **cyber security education**, the development of **risk-based standards, and resilience** especially against **botnets**. In Section 3 there is a focus on an open but secure Internet and **deterrence** and protection against cyber threats [1]. Finally, on May 12, 2017 a cybersecurity related press release mentions **Internet of Things (IoT) security** [2].

[1] The White House Website: Executive Order, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", Accessed September 2017, https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

[2] The White House Website: "President Trump Protects America's Cyber Infrastructure", Accessed September 2017, https://www.whitehouse.gov/the-press-office/2017/05/12/president-trump-protects-americas-cyber-infrastructure

---

## Anomaly Detection

**Group Project #1:** Optimizing Machine Learning-based Analytics for Industrial Control Systems (ICS) Intrusion Detection

Recently updated TCP/IP-based cyber physical devices for SCADA and DCS technologies have emerged as some of the most important yet vulnerable devices in the Energy, Chemical, Critical Manufacturing, Water, Food Processing and Dams Sectors. One of their largest threats is Advanced Persistent Threat (APT); however, equally as dangerous threats are malicious insiders. Therefore, novel and protocol agnostic intrusion detection schemes have surfaced. Given the Inference-based Intrusion Detection System (iBIDS) described in [3], your tasks are to: (1) modify the machine analytics (i.e., SVM and Random Forest) to accept customizable parameters, (2) use our local ABB RTU560 testbed to optimize (**lower false alarm rate**) the machine learning analytics for ICMP network traffic, and (3) do the same for TCP/IP network traffic.

[3] Rahul Nair, Chinmohan Nayak, Kashif Memon, Lanier Watkins, Kevin Fairbanks, and William H. Robinson, "The Resource Usage Viewpoint of Industrial Control System Security: An Inference-based Intrusion Detection System", In Cybersecurity for Industry 4.0 Analysis for Design and Manufacturing, A Springer book edited by Lane Thames (Tripwire, Inc., USA) and Dirk Schaefer (University of Bath, UK), April 2017.

## Anomaly Detection

**Group Project #2:** *Using Power Levels to Infer Unauthorized Use in Wireless Sensor Nodes: A Hardware Implementation*

Wireless sensor networks (WSN) have been around for years now and have proven to be very useful data collection tools in situations unfavorable or infeasible for humans. Recently, WSNs have resurfaced in the form of medical body area networks (MBAN) or body sensor networks (BSN), which provide invaluable services to the Health Care Sector. Chandramouli et al. [4] implemented a decentralized intrusion detection scheme using a "Taddle-Tail" approach where nodes report their suspicious neighbors as possibly compromised to the gateway. Your task is to: (1) Simulate this intrusion detection scheme using Contiki and (2) upload your simulation to real wireless sensor node hardware and demonstrate the detection capability using these physical nodes.

[4] Jayanarayan Chandramouli, Juan Ramos, Lakshmi Srinivasan, Prahlad Suresh, Garth V. Crosby, and Lanier Watkins, "Using Network Traffic to Infer Compromised Neighbors in Wireless Sensor Nodes," In the IEEE Consumer Communications & Networking Conference Workshop, January 2017.

## Situational Awareness

**Group Project #3:** *Network-Based Detection of Mobile Malware Exhibiting Obfuscated or Silent Network Behavior*

Games downloaded from third party repositories are notorious for hosting trojanized applications. Once downloaded and active on the mobile device, trojans pose a huge threat to corporate and government networks. Because malware has the ability to obfuscate its network traffic and subvert host-based defenses (e.g., anti-virus, mobile device managers), traditional network and host intrusion detection systems become less effective in providing situational awareness into wireless networks. As an alternative, an application aware network-based malware monitoring method [5] has been developed and has shown promise.

Your task is to evaluate the efficacy of using this approach to accurately provide situational awareness into wireless networks by modifying a framework developed by a project team from a past year, to test 100s of legitimate and trojanized applications on a physical device. The framework uses the Android Application Exerciser Monkey along with a smartphone, and a network monitor (i.e., PC) to create ICMP ping profiles for one hundred pieces of malware and one hundred pieces of legitimate software. You will need to modify this framework to extract layer 1, layer 2 (i.e., 802.11), and layer 3 parameters, and create datasets with meaningful features, that can be used by machine learning to demonstrate the ability to discern malware operation from legitimate operation.

[5] Lanier Watkins, Amritha Lal Kalathummarath, William H. Robinson, Shuang Xie, and Tianning Yang," Network-Based Detection of Mobile Malware Exhibiting Obfuscated or Silent Network Behavior", Whitepaper, February 2015.

## Deterrence

**Group Project #4**: A *Smart Tool for Counter sUAS Defense*

Small Unmanned aerial Systems (sUAS) have recently become a popular hobbyist sensation. Now, pioneering business minds are quickly finding new and exciting commercial applications for these sUAS. The main issue with this is that researchers [6] have determined that current sUAS vendors are not security minded and thus are releasing products that are highly vulnerable to remote security attacks. Therefore, the end products that will result from commercializing sUAS may suffer from these same security issues. In [6] we describe a vulnerability that we later exploited to develop a counter sUAS defense system. At the heart of this system is the reliance on the MAC address to discern friendly access points from unfriendly access points (This tool only works for Wi-Fi-based sUAS, which all contain access points either in the sUAS itself or its controller). A smart attacker could spoof the MAC of his sUAS and defeat this tool. Your task is to determine if you can identify drones based on behavior of protocol, with the premise that different vendors may implement protocol functions differently. Examples might be the implementation of the modulation or rate switching algorithm in the 802.11 protocol or maybe something independent of the communications protocol (e.g., power management algorithm). If this approach is feasible, modify our existing tool to include your new smart decision model and demonstrate its capability. **Hint, machine learning may be helpful here.**

[6] Lanier Watkins, Juan Ramos, Gaetano Snow, Jessica Vallejo, William H. Robinson, and Avi Rubin, "Who Is Flying My Drone? An Introduction to the Small Unmanned Aerial Systems (sUAS) Security Problem" Submitted to IEEE Security & Privacy Magazine, 2017.

## IoT Security

**Group Project #5:** *Hacking and Exploiting Smart Meters*

The Internet of Things (IoT) security is very important as evidenced by great concern from our Executive Branch of Government (See above). One area of concern is smart meters. If smart meter vendors are anything like sUAS vendors, they have not done any serious security assessments of their products [6]. Your task is to: (1) perform penetration testing on a couple of smart meters from top vendors and (2) implement exploits to demonstrate the risk associated with any vulnerabilities found.

## IoT Security and Botnets

**Group Project #6: How to Ensure That Alexa Is Not A Ticking Time Bomb**

The Mirai botnet aggregated IoT devices to launch huge attack campaigns. Meanwhile the legitimate functions of the IoT devices were not disrupted and therefore the IoT owner was not impacted and unaware that their device was part a national attack. Your task is to design an IDS for consumer IoT devices. How do we detect Mirai botnet type of misbehavior? How can we detect a compromised IoT device and furthermore determine when that device is being controlled remotely to carry out other malicious activity? The first challenge would be to learn what's "normal" for an IoT system. This would involve leveraging wireless packet behavior (e.g., chattiness of protocol, sender/receiver patterns, etc.), and application data to understand the pattern of activities for an IoT system with and without sensing events occurring.

[9] Lanier Watkins, Sean Beck, Jared Zook, Anna Buczak, Jeffery Chavis, William H.

Robinson, Jose A. Morales, and Sameul Mishra, "Using Semi-supervised Machine Learning to Address the Big Data Problem in DNS Networks," In IEEE Computing and Communication Workshop and Conference, January 2017.

## Resilience

**Group Project #7:** *Bio-inspired Cyber Security: Building Better Firewalls*

In the Spring of 2017, I completed a MS degree in Biotechnology. One of the most interesting courses I took was Cell Biology. As a trained computer scientist and physicist, I had not taken a college level biology course before, but I learned a lot, so much that I was inspired to contemplate using biological systems to inspire better cyber security. For instance, consider an animal cell membrane. It keeps the liquid contents of the cell inside and the liquid environment of the exterior out of the cell unless there is a need for the interior or exterior contents to enter or leave (i.e., lipid bilayer). It also allows signals to pass in and out of the cell unaltered, see Figure 1. Your task is to: (1) study the animal cell membrane, (2) leverage 5 or more attributes to build a better network firewall, and (3) demonstrate with a working prototype the benefits of your new bio-inspired firewall by directly comparing it to 2 top vendor firewalls.

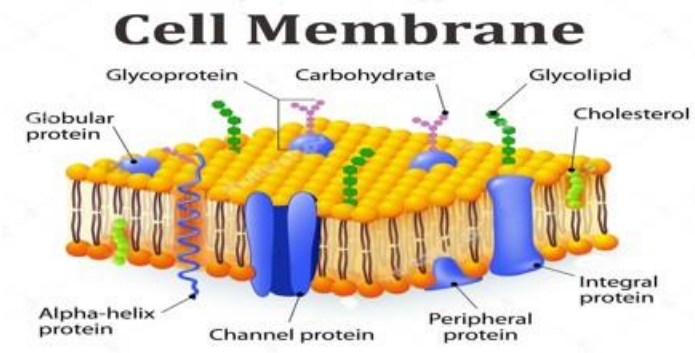


Figure 1. Animal cell membrane