PACT Newsletter

Issue (1) nnsa-pact.org Spring 2020

Welcome to our First Issue of PACT Newsletter

Salim Hariri, University of Arizona

It is my pleasure to introduce to you our project entitled "Partnership for Proactive Cybersecurity Research and Training (PACT)" was awarded close to $3 Million from DoE National Nuclear Security Administration for three years starting 10/1/2019. The partnership includes three universities (University of Arizona, Howard University and Navajo Technical University) and one DOE Laboratory (Argonne National Laboratory).

The primary goal of the PACT is to address the current and future cybersecurity research challenges and educate and train the next generation of highly skilled cybersecurity workforce that will be heavily recruited from underrepresented and minorities.

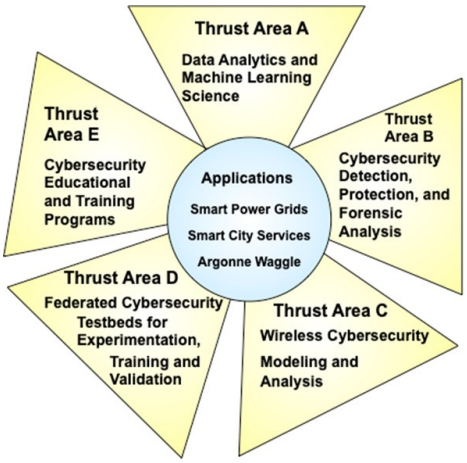
The partnership goals are the following:

•Establish a comprehensive cybersecurity science agenda that provides the theoretical foundation to:
(a) Use data analytics and machine learning science to accurately quantify and characterize "normal" operations of cyber systems and services,
(b) Model and quantify the risks and impacts of vulnerabilities and attacks on cyber systems,
(c) Develop data-driven cyber security and forensic modeling, analysis and prediction; and
(d) Design and analyze innovative detection and protection techniques.

•Validate and demonstrate the usefulness of the cybersecurity solutions on large scale case studies (critical infrastructures, smart cities, Argonne Waggle project)

•Integrate the Consortium's research projects with established cybersecurity educational and training programs to provide effective cybersecurity learning opportunities for both undergraduate and graduate students.

The partnership will heavily recruit underrepresented minority students to be involved in our research projects, cybersecurity summer training and mentoring camps, and internship programs.



In this issue, we like to highlight the ongoing research and training activities that were developed and currently used to train minority students since the start of the project on November 1st, 2019.

Inside this issue

Online Workshop

Overview of PACT:

Research and Training Projects

April 24th, 2020
11 am-5:00 pm (EST)
Zoom Meeting
https://arizona.zoom.us/j/843090356

Time (EST)	Program Agenda	Time (PST)
11:00-11:30AM	Department of Energy – PACT Program *David Canty, Program Manager, National Nuclear Security Administration, DoE*	8:00- 8:30AM
11:30-12:00PM	Overview of UA PACT Research and Education Projects *Salim Hariri, Tamal Bose and Gregory Ditzler, University of Arizona*	8:30- 9:00AM
12:00-12:15PM	Federated Cybersecurity Tesbeds for Experimentation, Validation *Danda Rawat, Howard University*	9:00- 9:15AM
12:15-12:45PM	NTU Education and Training Projects *Frank Stomp, Navajo Technical University*	9:15- 9:45AM
12:45- 1:30PM	Lunch Break	9:45- 10:30AM
1:30- 2:00PM	Zero-Trust Waggle-based Edge Platform *Rajesh Sankaran, Argonne National Laboratory*	10:30- 11:00AM
2:00- 2:30PM	Collaboration Plan with Cybersecurity Sandia National Labs *Wellington Lee, Sandia National Labs*	11:00- 11:30AM
2:30-3:30PM	Howard University Student Research Projects *Danda Rawat, Howard University*	11:30- 12:30PM
3:30-4:30PM	UA Student Research Projects *Secure Modulation Classification, Alex Berian* *Adversarial Machine Learning and Its Applications, David Schwartz* *Anomaly Behavior Analysis of Industrial Control Systems, Clarisa Grigalva*	12:30- 1:30PM
4:30-5:00PM	Open Discussion, Action Plans and Moving Forward on PACT *David Canty, Salim Hariri, Danda Rawat*	1:30– 2:00PM

REU Summer Program

Location and Time: TBD

Zero-Trust-based Waggle-enabled Smart-Edge

Rajesh Sankaran, Argonne National Laboratory
Salim Hariri, University of Arizona

Rajesh Sankaran

The open-source Waggle AI@Edge Platform is primarily designed and developed by Argonne National Laboratory. Waggle is an agile, reconfigurable, and remotely programmable cloud-enabled edge-computing platform to support innovative sensing/actuation and cyberinfrastructure features. Waggle is being extended to support a growing number of scientific applications, by taking advantage of novel low-power and high-performance computing devices, advanced software virtualization techniques, and AI/ML techniques to draw inferences from high-bandwidth sensors like LiDARs, cameras, and microphones.

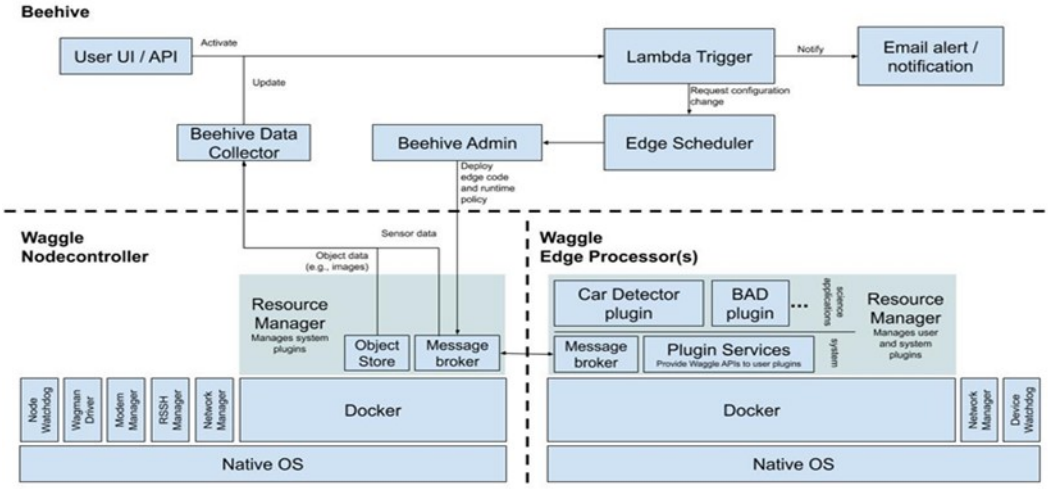


Figure 1. Waggle architecture

Waggle nodes pair sensors and actuators with computing, and function with full operational autonomy, with the ability for out-of-band remote management by a central cloud resource called Beehive (Figure. 1). In the Waggle architecture, nodes execute compute jobs deployed in Linux Containers (edge plugins) to support the edge inference and actuation/feedback goals to meet the various science objectives. The inferences are then aggregated in Beehive, which may be further computed upon for acquiring global knowledge and triggering operational changes at the nodes. Toward this end, the Waggle edge-compute nodes are deployed on insecure Internet-connected networks, and edge-plugins are often produced by scientific end-users of the platform, thereby introducing several trusts, privacy, and security challenges at the edge, beehive and in-between.

ACS architecture is based on Zero Trust Architecture (ZTA) that is described in the NIST SP800-207 draft that was published in September 2019. ZTA is an end-to-end approach to network/data security that encompasses identity, credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure. Zero trust is an architectural approach that is focused on data protection. The initial focus should be on restricting resource access to those with a “need to know.” Traditionally, agencies (and enterprise networks in general) have focused on perimeter defense, and authorized users are given broad access to resources. As a result, unauthorized lateral movement within a network has been one of the biggest challenges for federal agencies.

Continue on page 5

To illustrate, in Figure 2, a user or machine needs access to an enterprise resource. Access is granted through a Policy Decision Point (PDP) and corresponding Policy Enforcement Point (PEP).

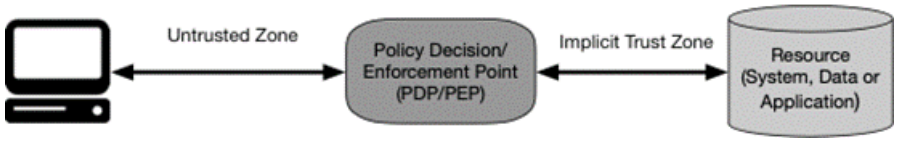


Figure 2. Zero trust architecture.

The system must ensure the user is "trustworthy" and the request is valid. The PDP/PEP passes proper judgment to allow the subject to access the resource. This implies that Zero Trust applies for two basic areas: authentication and authorization. These principles can be directly applied to the Waggle framework toward authenticating jobs from users on edge resources and authorizing the use of edge sensors, data streams, and actuators by user-developed applications.

As shown in Figure 3, ACS consists of two main modules:

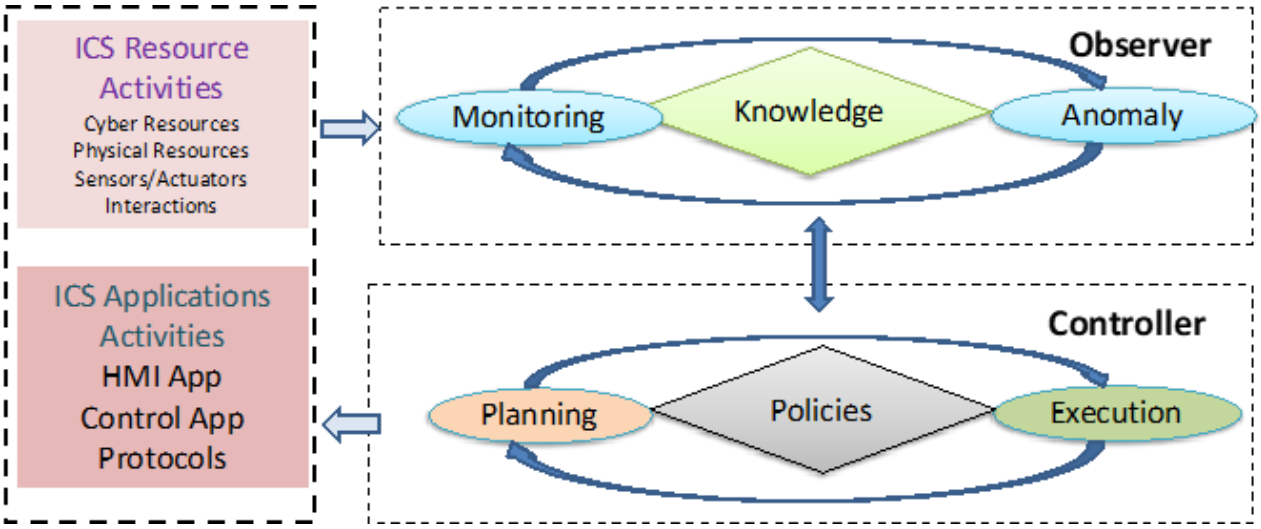


Figure 3. Autonomic cybersecurity architecture.

1) Observer module that continuously monitors the cyber components as well as the physical components of the ICS infrastructure such as network activities and host log, along with physical-data such as power consumption, acoustic, acceleration, and temperature, power consumption. The Observer module is to continuously enforce the zero trust principle by performing two main functions:

a. Continuous Resource Authentication (CRA) – The Observer module will use AI and ML techniques to guarantee the authenticity of each cyber and physical component,

b. Continuous Policy Enforcement (CPE) – The Observer module will use whitelisting and Anomaly Behavior Analysis (ABA) techniques to make sure the observed operations are allowed and do not violate current security policies. Once a violation is detected, it will send an alert to the Controller module;

2) Controller module that once it receives an alert from the observer module, it will check its security policies and best practices to take proactive actions to stop the attacks and/or mitigate their impacts on the normal operations of ICS resources and applications.

We plan to explore and extend the ACS Zero-trust to Waggle platform to support trusted sensing, computing, and inference at the edge and explore the applicability of the techniques in evaluating the security and trustworthiness of the user-developed edge-applications.

Collaboration Plan with Cybersecurity Sandia National Labs

Sandia TraceFire training workshop

The University of Arizona cybersecurity research team lead by Dr. Hariri met with Mr. Wellington Lee from Sandia National Labs on December 19, 2019, at the Autonomic Computing Lab at the University of Arizona.

In the meeting, Wellington reviewed Sandia cybersecurity training programs and their involvement in IoT and industrial control systems. The UA PACT team reviewed our ongoing cybersecurity research projects and showed demonstrations of our cybersecurity detection and protection tools.

The PACT team will potentially collaborate with Sandia Cybersecurity R&D team in the following areas:

- Participate in the TracerFire program that aims at 1) creating a community of cyber defenders sharing expertise, skills, and competencies; 2) Attract, inspire, and grow the next generation of expert cyber defenders for the US; and 3) Support educational institutions to create educational capabilities and infrastructure to foster the development of future cyber defenders.
- Invite Sandia cybersecurity research team to provide training during the planned REU summer workshop to be determined once the Covid-19 pandemic restriction is relaxed and allow us to organize it.
- The PACT researchers will utilize the Sandia forensic and training programs. Participate in PACT future training workshops and programs.

In addition, the Sandia research team is interested in collaborating with PACT researchers in the following research areas:

- Threat Area B: Cybersecurity Detections, Protection, and Forensic Analysis
- Threat Area E: Cybersecurity Educational and Training Programs

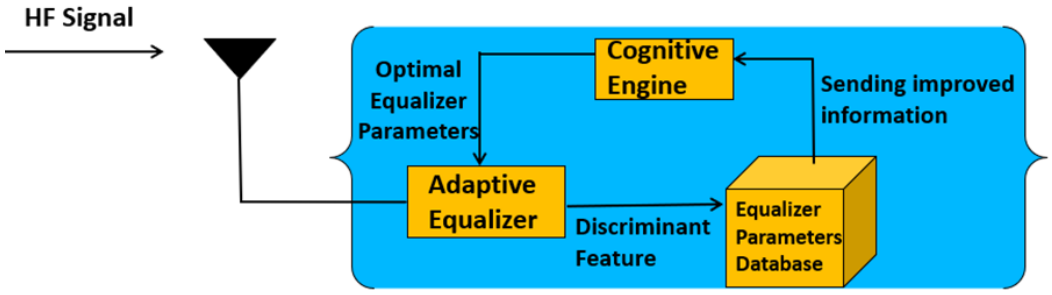
Cognitive/Adaptive Equalization for HF Channels

Noel Hagos

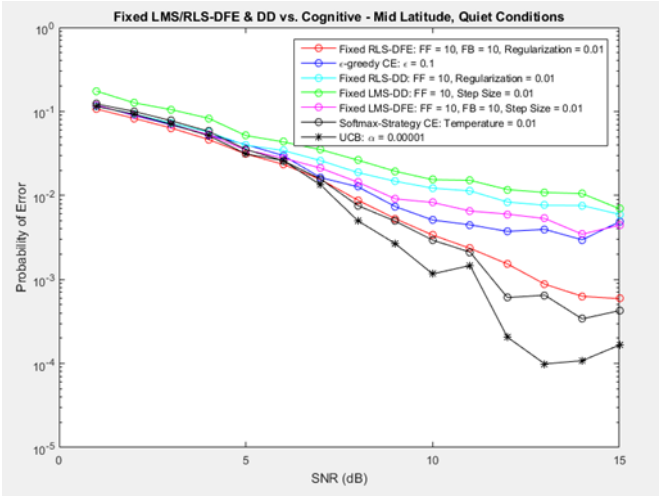
Noel Hagos, University of Arizona

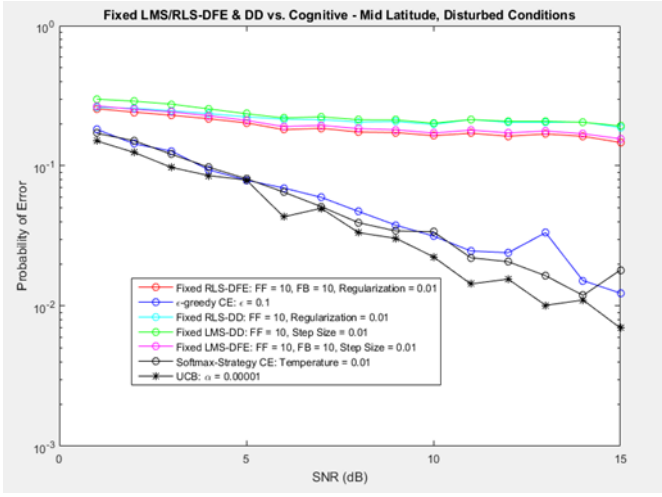
Noel Teku received his Bachelor's and Master's degrees in Electrical Engineering in 2012 and 2017, respectively, from the University of Arizona. He is pursuing a Ph.D. in Electrical Engineering at the University of Arizona under the supervision of Dr. Tamal Bose. His research involves employing reinforcement learning algorithms to increase the reliability of High Frequency (HF) communications. Specifically, he has used reinforcement learning to be able to search for optimal parameters of equalization (i.e., tap length, step size, filter type, etc.) for different simulated HF channels.

Problem Statement: The High Frequency (HF) band, which covers the portion of the spectrum ranging from 3-30 MHz, has long been of interest to researchers in wireless communications and signal processing. The band has been used for a variety of applications due to the capability for long-range communications without a significant amount of equipment (i.e., cell towers, satellites, etc.). This is accomplished by using the ionosphere as the primary medium of transmission. However, a pivotal drawback is that the ionosphere varies drastically based on numerous factors beyond our control (i.e., time of day, location, etc.). These fluctuations can cause significant distortions to the transmitted signal. To remove these channel impairments, a technique used frequently in the literature is adaptive equalization. However, the optimal structure of an adaptive equalizer (i.e., tap length, step size, adaptive algorithm, filter type) is regularly not known ahead of time.



Method: We are investigating the concept of cognitive equalization, which entails using a form of machine learning called reinforcement learning to determine the optimal structure of an adaptive equalizer for a specific HF channel. The motivation behind this idea is to provide the receiver with the flexibility to adjust its equalization settings to determine which parameters (i.e. tap length, step size, adaptive algorithm, filter type) are most optimal for a specific set of HF channel conditions.





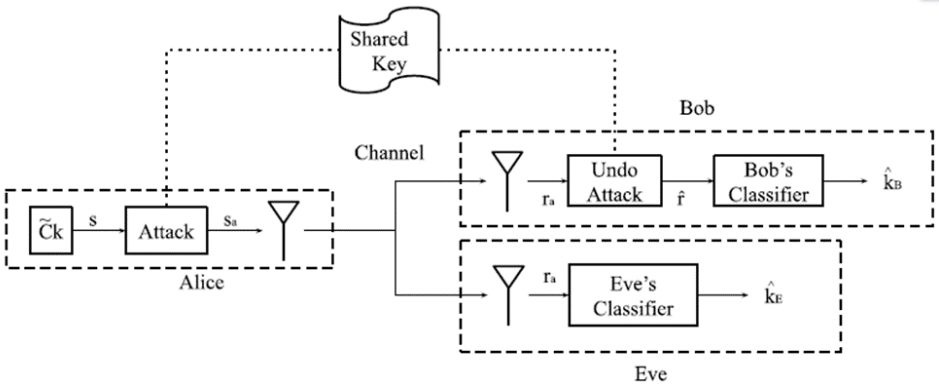
Secure Modulation Classification

Alex Berian

Alex Berian, University of Arizona

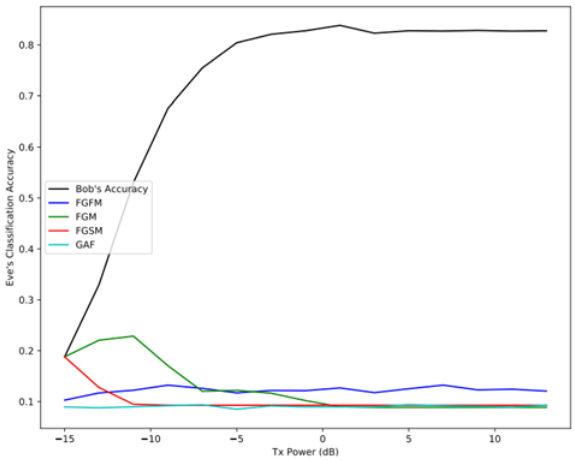
Alex Berian is pursuing a Ph.D. in Electrical and Computer Engineering with a focus on physical layer security in wireless communication using machine learning. Alex has worked as an intern at the fiber optics research lab at Panduit and as a signal processing engineer at Raytheon. His hobbies include longboarding, pizza making, and brewing.

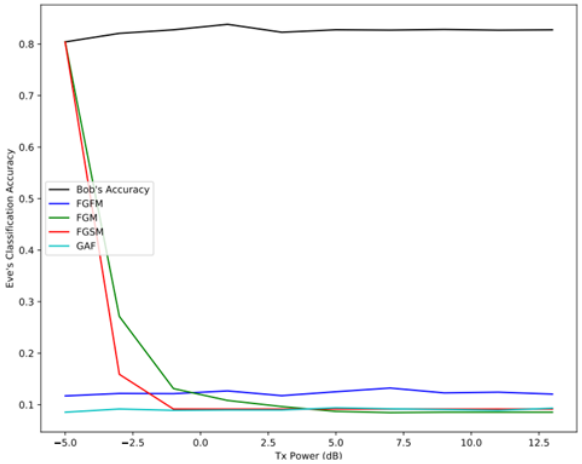
My work focuses on the security of data communication means. In wireless communication systems, parties typically agree on a *Modulation Format,* which dictates how parties send data to each other. Even if you did not make a system designed to understand all modulation formats, you could still classify them. Classifying modulation formats is useful for identifying enemies in military applications, securing precious wireless spectrum from unwanted users, and radar applications as well.



The novelty we are working on is modifying our data transmissions, so enemies cannot identify how we are communicating. We analyze an eavesdropper scenario, where the transmitter (Alice) wants to send a message to a receiver (Bob) without allowing an eavesdropper (Eve) know what the modulation format is. We show that traditional *Adversarial Learning* methods are not enough when transmit power is limited. To solve this problem, we proposed novel *Adversarial Filtering* algorithms, which are much more effective for Alice and Bob to keep their modulation format a secret from Eve than traditional adversarial learning methods.

Secrecy of the modulation format is measured by the eavesdroppers classification accuracy. In experiments it is shown that the novel adversarial filtering algorithms achieve better secrecy than traditional adversarial learning algorithms. The figure below demonstrates the effectiveness of the novel algorithms (FGFM and GAF) when Alice's transmission power is limited, and the drawback of existing algorithms (FGM and FGSM).





FCTaaS: Federated Cybersecurity Testbed as a Service

Birkan Kolcu, University of Arizona

The main goal of the FCTaaS is to enable the integration of isolated heterogenous cybersecurity testbeds that are operated by different organizations under a single federation while maintaining the privacy and security of experimenters. Furthermore, FCTaaS will significantly reduce the experimenters' efforts to discover individual testbeds, create a federated cybersecurity testbed and then perform the desired cybersecurity experiments as the integrated cybersecurity testbeds can be easily browsed and the experimentation can be performed through FCTaaS web interface. The FCTaaS architecture is shown in Fig. 1 that is hosted in the Scaleway Cloud [17] and provide the following services: 1) Interoperability Service – to allow different testbeds to interoperate correctly even when each testbed might use different semantics and terminology; 2) Privacy and Security Service – to ensure that the formed federated testbed maintains the required privacy and security policies associated with each testbed that might be governed by different organizations; 3) Experiment Management Service – to allow users to create and manage their cybersecurity experiments through the connected cybersecurity testbeds under FCTaaS; and 4) FCTaaS Web Service – to provide ubiquitous user interface to FCTaaS so that the users can have access from anywhere, any time, and using any device (mobile or stationary) with the Internet connectivity.

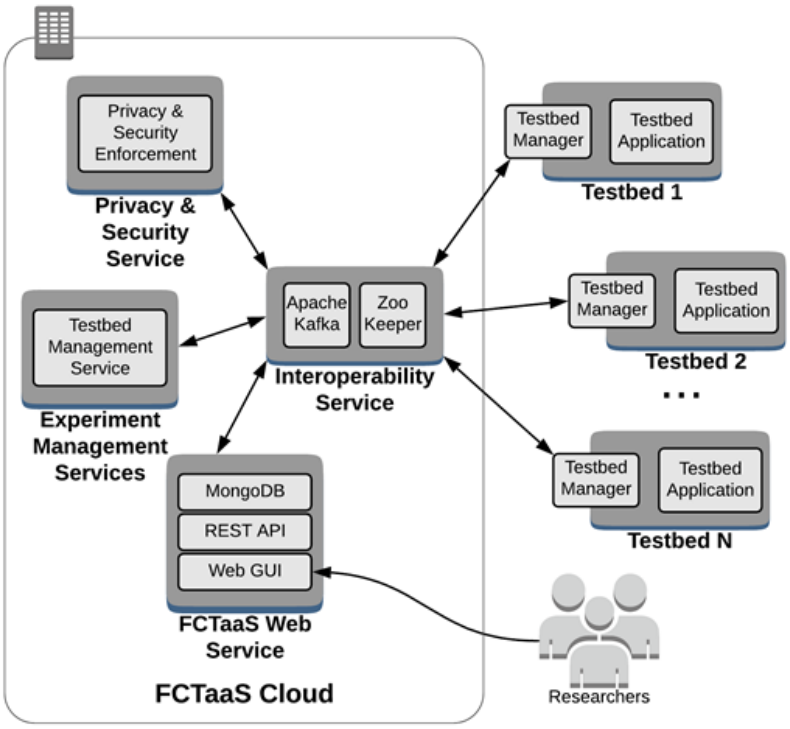


Figure 1. FCTaaS Cloud

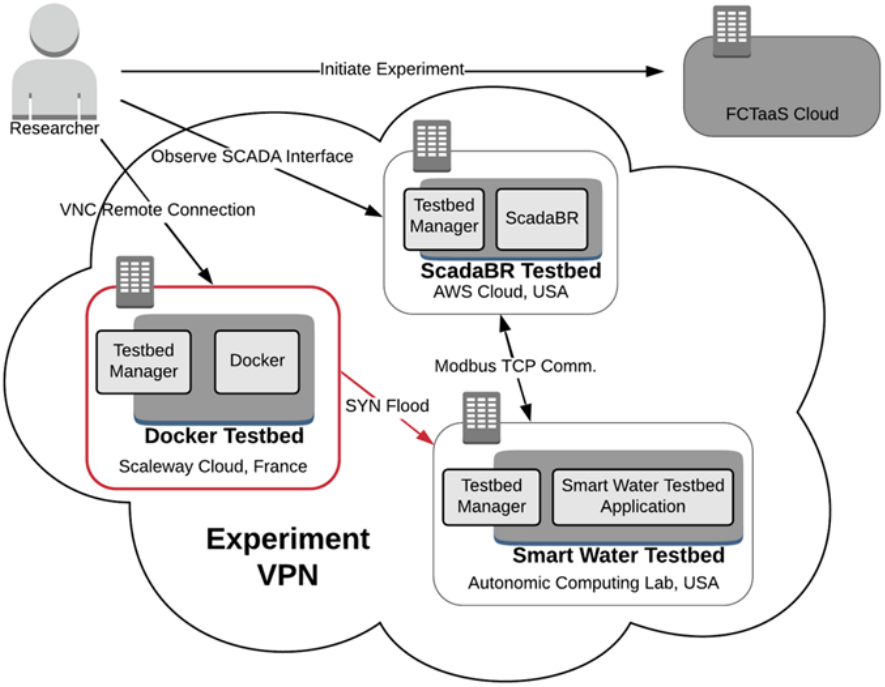


Figure 2. Experiment VPN

This figure demonstrates one use case scenario where the FCTaaS creates a federated cybersecurity testbed by combining a Docker based attack testbed, a ScadaBR testbed, and a smart water testbed. After allocating these testbeds, FCTaaS creates an experiment VPN and connects all these experiments. The users can study the effects of cybersecurity attacks and how they can propagate through different testbeds this way.

Data Analytics and Machine Learning Team

Greg Ditzler

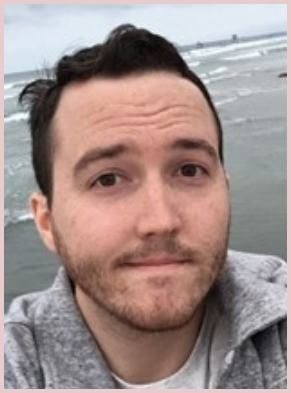
Greg Ditzler, University of Arizona

Dr. Ditzler's group is developing advanced ML technologies that defend against an adversary in cyber environments. The robustness and vulnerability of Deep Neural Networks (DNN) is a critical area of interest since these models are in widespread use across real-world applications.

His team recently proposed an algorithm to detect adversarial audio by using a DNN's quantization error. Specifically, we showed that adversarial audio typically exhibits a larger activation quantization error than benign audio, which leads to a higher detection rate.

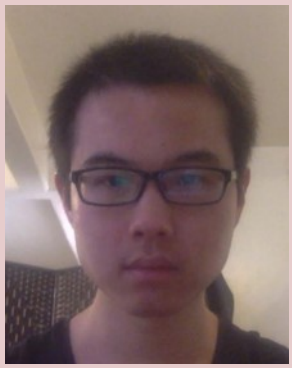
David Schwartz

David Schwartz earned a B.S. and M.S. in Electrical and Computer Engineering and a B.S. in Mathematics from the University of Arizona. He is pursuing a Ph.D. in Computer Engineering at the University of Arizona under the supervision of Dr. Gregory Ditzler. His research explores novel ways to leverage progress in information theory to better understand learning and computation in neural networks. In recent work with CAC, David has characterized the detectability of certain cyber-attacks on HTML and XML data as limited by the state-of-the-art machine learning techniques.



Brandon Black

Brandon Black earned his B.S. in Electrical and Computer Engineering with a minor in Mathematics from the University of Arizona in 2019. He is currently in the Accelerated Masters program to earn his M.S. in Electrical and Computer Engineering. His focus is on machine learning theory with special consideration for ensembles in adversarial settings. Brandon additionally is working on applications of synthetic adversarial data generation for improved model performance in restricted sample environments.



Heng Liu

Heng Liu received his B.Eng. Degree from the University of Electrical and Scientific Technology of China, Chengdu, Sichuan, in 2015. He is currently a Ph.D. candidate from the Department of Electrical and Computer Engineering, University of Arizona. He also works as a research assistant at the Machine Learning and Data Analytics Lab. His research interests are open problems in machine learning with special interests in large-scale feature subset selection, information theory, deep neural network quantization, LSTM, scalable and adversarial machine learning, greedy algorithms. He is a student member of the IEEE society.

Adversarial Machine Learning and Its Applications to Cybersecurity

Heng Liu and Gregory Ditzler , University of Arizona

The majority of machine learning (ML) algorithms rely on the assumption that data are sampled from a fixed probability distribution. This assumption is often violated in practice, which results in classification and regression strategies that are far from optimal or even reliable, even with neural networks. As an example, the image on the left shows how a neural network can easily be fooled into making an incorrect decision. The image on the left if an image of a panda that is correctly classified by a deep neural network and the image on the right is the image of the panda with judiciously chosen noise; however, the image on the right is classified as a gibbon.

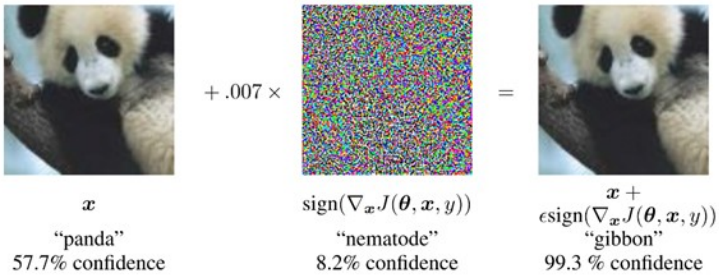


Fig 1. Example of an adversary poisoning (middle) an image of a panda (left) to make the neural network predict the image on the right as a panda

PI Ditzler's group is developing advanced ML technologies that defend against an adversary in cyber environments. The robustness and vulnerability of Deep Neural Networks (DNN) is a critical area of interest since these models are in widespread use across real-world applications. A DNN's vulnerability is exploited by an adversary to generate data to attack the model; however, the majority of adversarial data generators have focused on image domains with far fewer work on audio domains. More recently, audio analysis models were shown to be vulnerable to adversarial audio examples. Thus, one urgent open problem is to detect adversarial audio reliably.

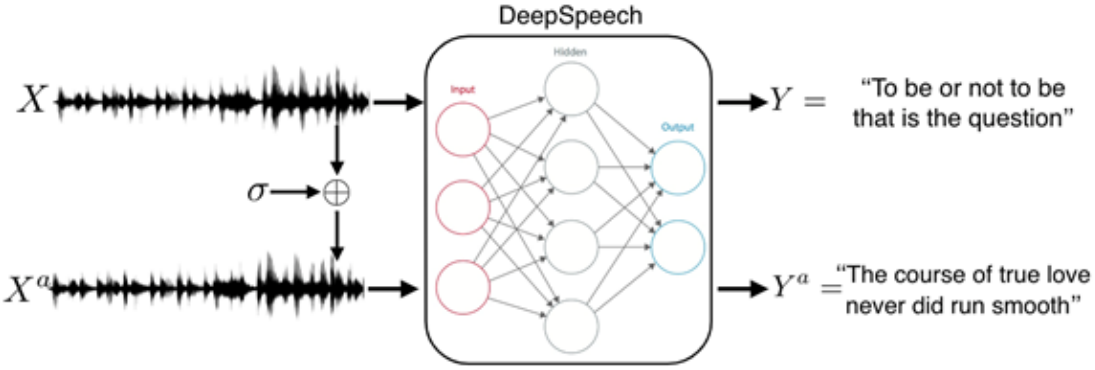


Fig 2. Overview of the Carlini attack algorithm. Benign audio produces the correct transcription via DeepSpeech. The adversary uses an attack to obtain a perturbed adversarial audio.

PI Ditzler's research team recently proposed an algorithm to detect adversarial audio by using a DNN's quantization error. Specifically, we showed that adversarial audio typically exhibits a larger activation quantization error than benign audio, which leads to higher detection rates (see figure). Experiments with three the-state-of-the-art audio attack algorithms against the DeepSpeech model show our detection algorithm achieved high accuracy on the Mozilla dataset. This research will be presented at the IEEE/INNS Joint Conference on Neural Networks.

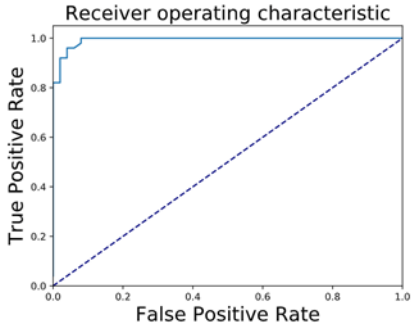


Fig 3. ROC showing the high detection rates of adversarial audio samples

Shalaka Satam

Anomaly Behavior Analysis of Bluetooth Protocols

Shalaka Satam, University of Arizona

Problem: The rapid deployment of IoT devices has made Bluetooth (IEEE 802.15.1) the wireless network of choice for close-range/ indoor communications. Bluetooth network finds its primary use in the delivery of audio streams to speakers, connecting peripheral devices like keyboards, and in connecting wearables like smartwatches, heart monitors to their controllers. Bluetooth devices use FHSS over 79 frequencies and operate in a Master/Slave configuration. A master can connect up to 7 slave devices to form a Piconet. A slave device can be part of multiple Piconets to form scatter-nets, as shown in figure 1. In hospitals and offices, devices communicate with one another, sharing sensitive and critical information over Bluetooth scatter-nets, making it necessary to secure these Bluetooth networks against attacks like Man in the Middle attack (MITM), eavesdropping attack, and Denial of Service (DoS) attacks. As a part of this research, we are developing a Multi-Level Bluetooth Intrusion Detection System (IDS) to secure the Bluetooth protocol. This IDS is not only able to detect attacks on Bluetooth protocols with precision up to 99.6% and recall up to 99.6% but is also able to perform whitelisting to prevent unauthorized devices from connecting to the network.

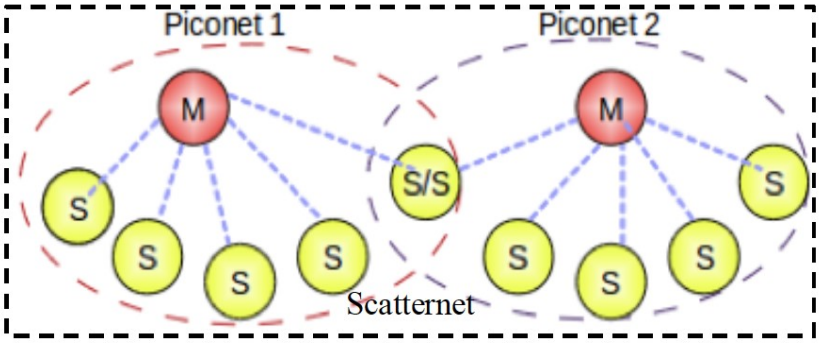


Figure 1. Bluetooth Scattternet

Approach: Figure 2 shows the architecture of the Multi-Level Bluetooth Intrusion Detection System (MLBIDS). In the figure, multiple Bluetooth piconets connected to one another over wired network form a large Bluetooth network used to share information. The networks are split into different levels based on the criticality of the connected devices and the importance of the data shared. The Bluetooth Behavior Analysis Unit (Figure 3) is deployed on the master of each Bluetooth piconet to secure the piconet against attacks like Man in the Middle and Denial of Service attacks. When a new device tries to connect to the Bluetooth network, the MLIDS performs device authentication and whitelisting by all piconet masters forwarding all the connection requests to a Master Whitelisting Server (MWS), which authenticates each connecting device with into the piconets based on device identity and piconet level.

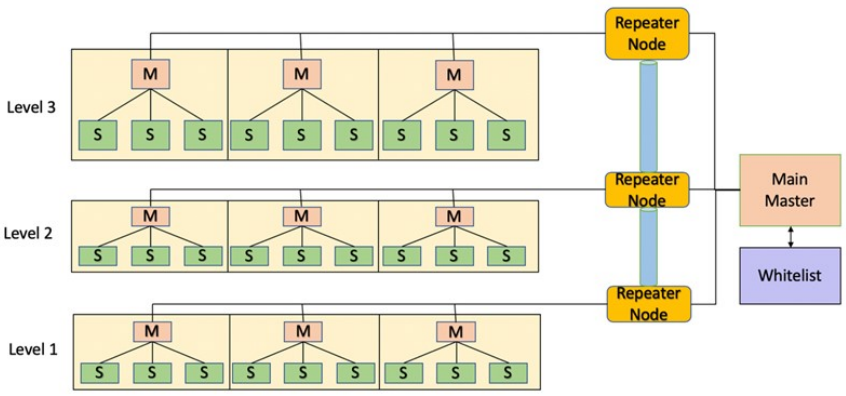


Figure 2: Architecture of Multilevel Bluetooth Network

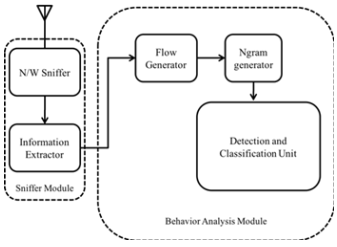


Figure 3
Bluetooth Behavior Analysis Architecture

The Bluetooth Behavior Analysis Unit

(BBAU) consists of a sniffer module and behavior analysis module. The Sniffer module collects the Bluetooth frames from the wireless medium, processes the collected frames and passes the processed frames to the Behavior Analysis Module. The Behavior Analysis Module analyses the behavior of the received Bluetooth frames. The data received is split into Observation-flows of size t seconds. The observation-flow is then converted to n-grams. The probability of that observed n-gram being either normal or abnormal is calculated using predetermined heuristics

Results: The presented Bluetooth Behavior Analysis Unit was deployed on a Bluetooth network to detect attacks. The Bluetooth Behavior Analysis architecture was testing with eavesdropping and Denial of Service (DoS) attacks like BlueSnarfing and Power Draining attacks. Figures 4a, 4b, and 4c show the performance of the IDS. From the results presented in Figure 4a-c, conclude that the presented architecture is able to detect attacks with very high accuracy and low false positives and negatives.

The performance of the whitelisting approach was measured similarly to detect and prevent unauthorized devices from connecting to the network. The whitelisting approach was successfully able to detect and prevent unauthorized devices from connecting to the network.

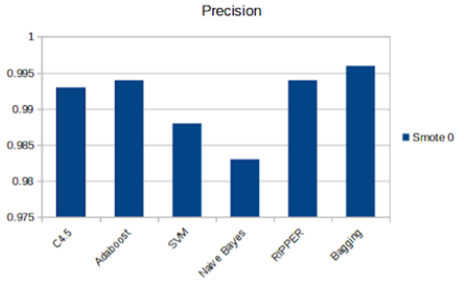


Figure 5.a: Precision for various classifiers

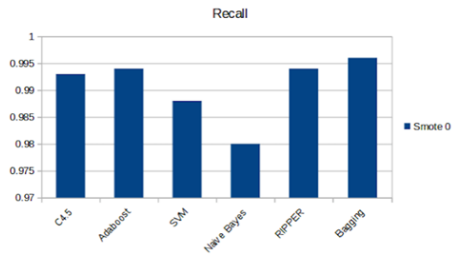


Figure 5.b: Recall for various classifiers

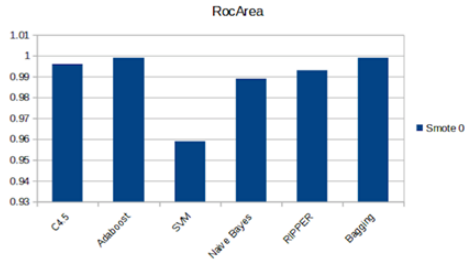


Figure 5.c: RoC area for various classifiers

A Survey of 5G Network Security Vulnerabilities: Moving on to 6G

Zahra Sadeq, University of Arizona

5G (fifth generation) systems have just been deployed around the world as of 2020. However, because there are persisting issues within these devices, the investigation has already begun in the development of 6G systems. 6G networks will enable higher data rates, which are expected to incur a lower latency to denser networks compared to 5G networks. To meet these demands in 6G, one of the crucial elements is to operate in millimeter-wave (mmWave) frequencies. Another point to mention is that AI will also play a critical role in supporting ultra-high capacity and throughput by optimizing the services used in 6G.

It will also aim to enhance the safety and security of 6G by mitigating the existing vulnerabilities of AI-enabled communications that are operating in high frequencies. There are many network security issues that 5G faces, which need to be addressed in the 6G networks. Some examples of the security attacks in 5G that need to be mitigated include traffic analysis, eavesdropping, and man-in-the-middle attacks. We will be investigating these issues in 6G and defining mitigation schemes based on realistic communication scenarios, propagation channel models, and modulation schemes. We will also derive AI-based solutions to these problems within the context of 6G to overcome the challenges found in 5G networks.

Clarisa Grijalva

Anomaly Behavior Analysis of Industrial Control Systems (ICS)

Clarisa Grijalva, University of Arizona

Problem: The exponential growth of the Internet of Things (IoT) has influenced all aspects of our lives and has led to the adoption of Industrial IoT (IIoT). Traditionally Industrial Control Systems (ICS), that were used to control factory floor manufacturing, power supply utilities, water supply utilities were isolated from other networks, were composed of specialized devices like Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs), and Supervisory Control And Data Acquisition (SCADA), running proprietary software over specialized protocols. Modern ICS are not completely isolated from other networks, use more generic communication protocols like TCP/IP, and have IIoT devices in them that provide enhanced connectivity and operational analysis. These changes in the structure of ICS have made it easier to design, develop and improve the performance of the ICS.

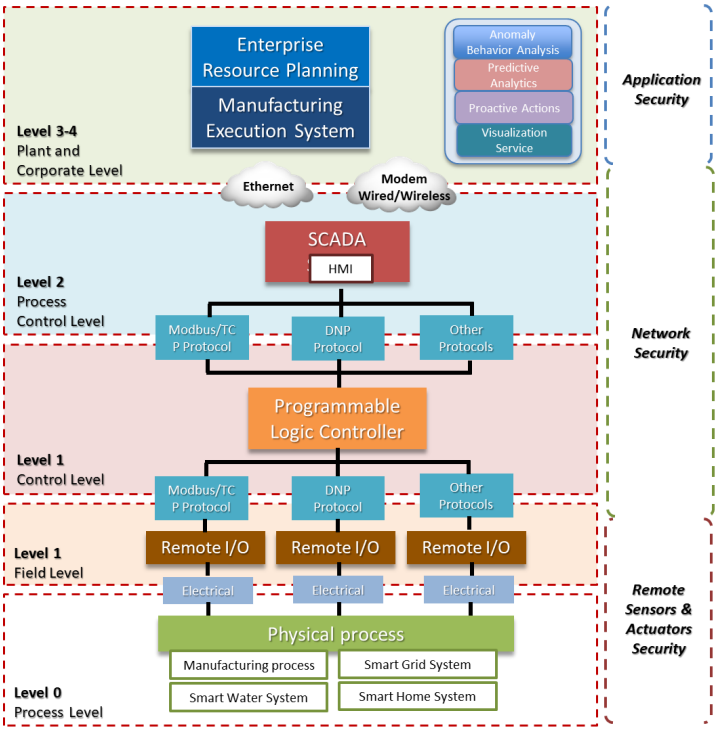


Figure 1. ICS Testbed.

Although the addition of IoT devices has improved the functionality of ICS, it has also increased the attack surfaces that an attacker can target to exploit the ICS, as demonstrated by the attacks on Ukraine power supply companies in 2015 and 2016, that left a huge population without electricity for a day. Moreover, attacks on ICS has a more lasting effect due to controlled software and expensive equipment utilization. It takes months for a full recovery for all the ICS functionality after an attack. Thus there is a need to design and develop approaches to secure ICS from cyber attacks.

As a part of this research, we will be developing a methodology to uniquely identify and fingerprint each sensor and actuator in an ICS. Machine learning models developed using deep neural networks will be used to identify the sensors and actuators, thus securing the ICS against sensor impersonation attacks and damages due to the installation of compromised sensors and actuators. We have in past developed intrusion detection systems (IDS) to secure Modbus, BACnet, and DNP3 protocols. This methodology, in combination with the mentioned IDS' will aid in securing ICS entirely.

Approach: Components of an ICS can be split into five levels based on their functionality.

Level 0 – Process Level: This level focuses on the threats associated with physical devices (sensors and actuators) and the potential vulnerabilities that can be exploited at this level.

Level 1 – Field Level: This level focuses on the vulnerabilities that can be exploited in PLC messages to be sent to the remote I/O field sensors and actuators using standard protocols like Modbus over TCP/IP, DNP3 or other protocols.

Level 1 – Control Field: This level focuses on the vulnerabilities of the PLC device as well as the vulnerabilities of the messages and communication protocols used to send the messages from the SCADA system (Level 2).

Continue on page 15

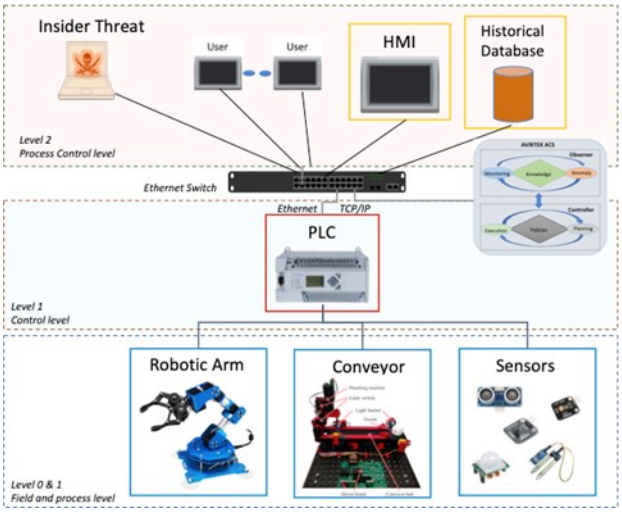


Fig 2. ICS Testbed Implementation

Level 2 – SCADA System: These levels focus on the vulnerability of the Human Machine Interface (HMI) application that obtains sensor data from the field components and issues commands to the actuators at the field level.

Level 3-4 – Plant and Corporate Level: This level focuses on the vulnerabilities that can be exploited by connecting the SCADA System to the rest of the corporate IP network.

In our work, we have further refined the ICS testbed environment and identified the most relevant protocols that can be used as shown in Figure 1. We will identify and analyze the threats on each level of the ICS environment shown in figure 1.

To develop the proposed methodology, we are building a testbed as shown in figure 2. The new testbed consists of Micrologic 1400 (1766:L32AWA) PLC, Panelview Plus 7 (2711P:TYC21D8S) HMI, NTC MF58 3950 B 10K Ohm 5* Thermistor Temperature sensors, 20A Range Current Sensor Module ACS712 Module current sensors, 6DOF robot xArm Full Metal Programmable Robotic Arm with Feedback of Servo Parameter, Wireless/Wired Mouse Control, Mobile Programming, and fischertechnik Punching machine.

Results:

Initially, our goal is to detect any event triggered by maliciously changing the sensor data or replacing the sensors or PLCs with compromised devices. Figure 3 shows the experiment we performed to collect the temperature sensor and then use Wavelet techniques to classify the data received from each sensor.

The collected data consisted of time-series information collected over several hours from thermistors. The raw data was discretized using a discrete wavelet transform. The transformed data were analyzed using a 1-D convolutional neural network. Figure 4. shows the loss function for the thermometer detector that was trained over more than 70 epochs (i.e., updates to the neural network). We noticed a convergence in the loss function, and we also did not observe a large change in the classification error (refer to the figure below) as the neural network was trained over time. We trained the classifier to detect malicious samples. The malicious data were generated as follows: the original data were multiplied by a constant, then we also added a constant to transform the data to make it appear that they were not normal data samples.

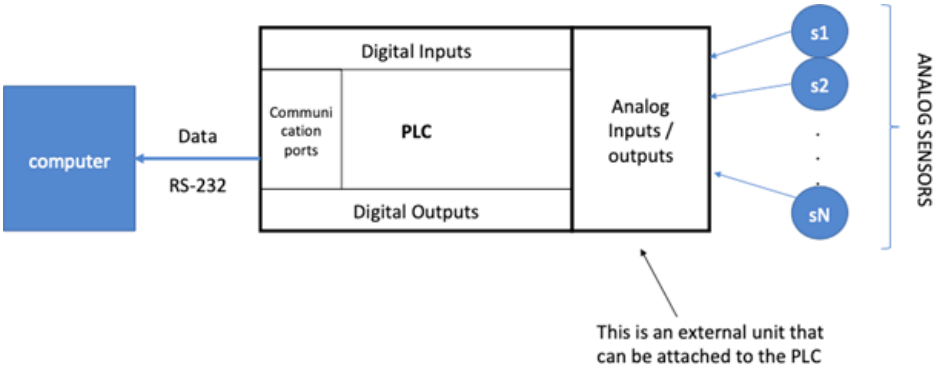


Fig 3. Temperature sensor data collection experiment.

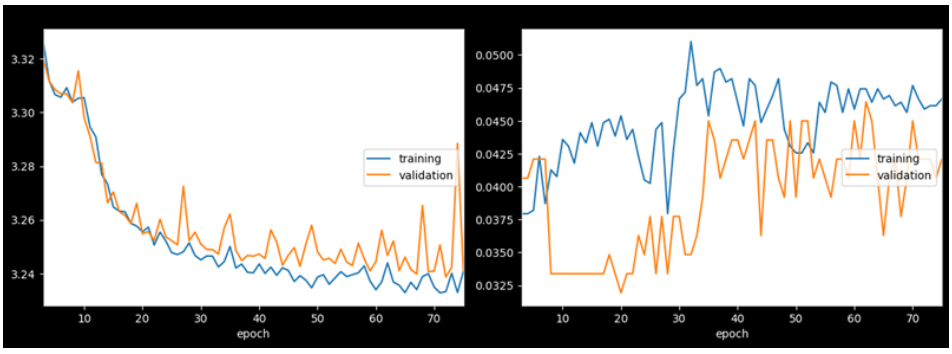


Fig 4. Loss function for classification algorithm

Cybersecurity Lab as a Service (CLaaS)

Pratik Satam

Cihan Tunc

Cihan Tunc, University of Arizona
Pratik Satam, University of Arizona

(http://www.askcypert.org/node/5)

Problem. The explosive growth of IT infrastructures, cloud systems, and IoT have resulted in complex cyber systems that are extremely difficult to secure and protect due to many factors such as their size, architecture complexity, distributed nature, heterogeneity, the large numbers of users, and diversity of services provided, just to name a few. These have resulted in the increase of the attack surface of cyber-infrastructure by several orders of magnitudes. These challenges, coupled with a shortage of skilled cybersecurity experts and the extreme difficulty in setting up experimental cybersecurity environments, have resulted in cyber systems that are vulnerable and easily exploitable by cyberattacks. Therefore, there is a critical need for cybersecurity testbeds to train students on how to detect existing vulnerabilities in cyber systems and protocols and how to protect them from malicious attacks.

Approach. In this project, we developed a Cybersecurity Laboratory as a Service (CLaaS) as shown in Figure 1 which aims at offering virtual cybersecurity and operations experiments as a cloud service that can be accessed from anywhere and from any device (desktop, laptop, tablet, smart mobile device, etc.) with Internet connectivity. The CLaaS enables

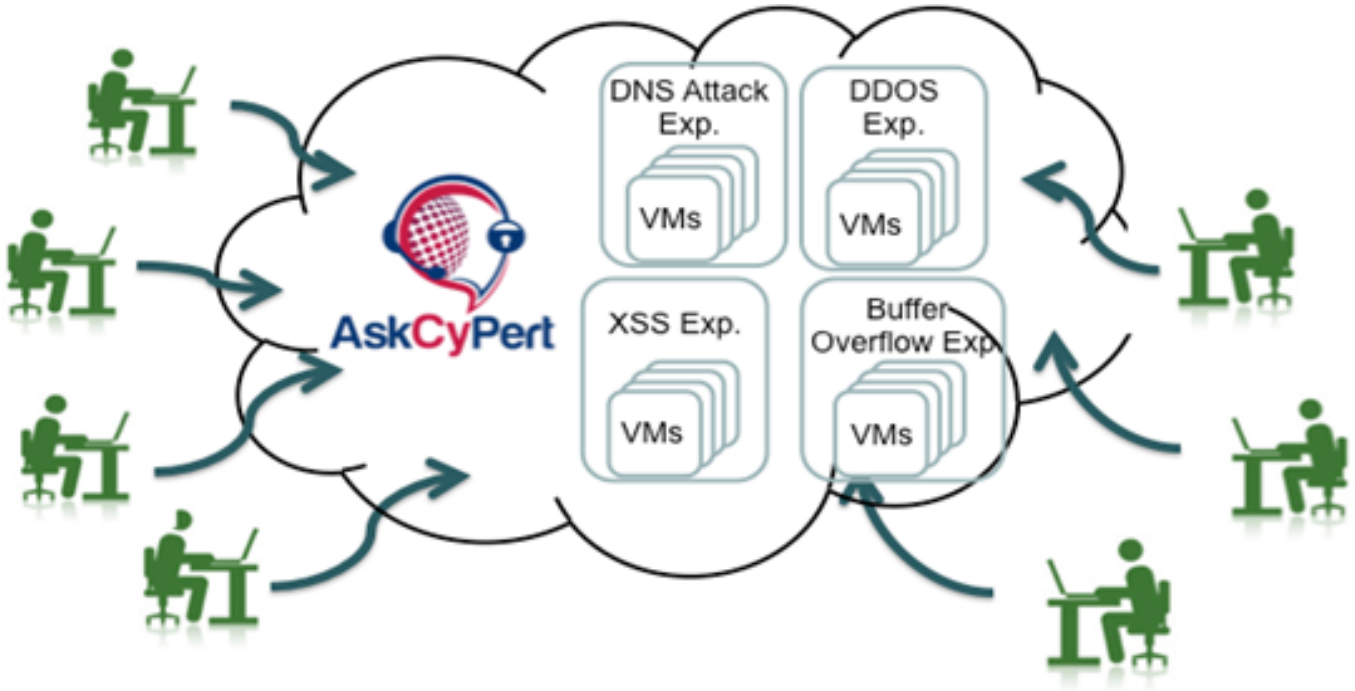


Fig 1. CLaaS offers ubiquitous access to virtual cyber security experiments from anywhere, any time, and using any device with Internet connectivity

Continue on page 17

students or trainees to conduct virtual cyber operations experiments in a closed virtual cloud environment to: a) understand the methodology of launching cyber attacks; b) train on how to use cyber security detection and protection tools; c) perform penetration testing for software systems; and d) evaluate new cybersecurity detection and protection algorithms.

We have developed a proof-of-concept CLaaS prototype that has been ported to Amazon AWS public cloud and is currently used by students at UA The University of Arizona as well as students at the University of Lyon 1, France, who use the solution for The CLaaS virtual cybersecurity experiments. These experiments are accessible from our AksCypert portal, www.askcypert.org. The below Figure demonstrate the CLaaS architecture that will be used to implement the proposed CLaaS functions and services.

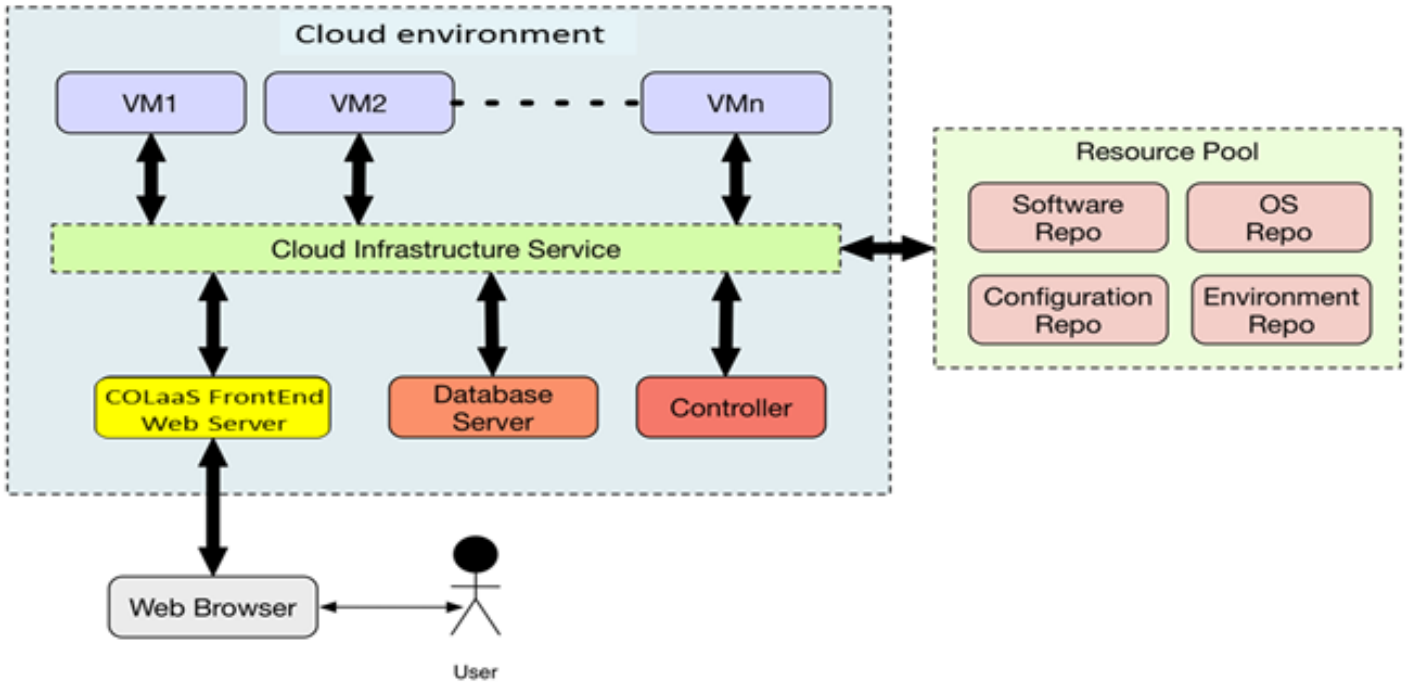


Fig 2. CLaaS architecture and its main components

Using the web browser, the user can log-in to the CLaaS website where the user selects the virtual cybersecurity or cyber operation experiment required by a given training program. Based on the user's request, the controller creates the necessary virtual experiment environment by setting up all the VMs and software tools for the selected experiment. The required VMs are created from a combination of (Configurations, OSs, and software). The CLaaS is provided with a local resource pool that has four repositories: 1) VM configuration repository; 2) OSs templates repository; 3) Software repository; and 4) Environment repository. VM configuration repository stores VM configuration templates to determine things like the number of cores, assigned main memory, and the number of network interfaces. The OSs repository will have the images of the OSs that are used by the experiments and their metadata; for example, the minimum core, minimum disk space, and minimum memory requirements. The software repository stores the software packages (e.g., Wireshark, Apache Webserver, bind9, Hping3, Hydra), configurations of the packages, and deployment conditions. The environment repository stores information about a whole complete test environment or an experiment, ; i.e., it stores required VM configuration, OSs image type on the required VMs, how the OSs need to be configured, what software to be run and how (e.g., user access), how the software needs to be configured, and finally what should be the network structure for connecting the environment.

Federated Cybersecurity Testbed

Danda Rawat, Howard University

Danda Rawat

Emerging smart city systems and applications are so complex and diverse (different quality of service, delay, computing capabilities, etc.) that traditional approaches for cybersecurity, performance prediction, measurement and management are not applicable in a straightforward manner. Thus, we proposed to use federated framework for data analytics and decision making is depicted in the figure below, where individual or group of domain specific devices by forming clusters can process the data for a real-time response offload their data to the edge for near real-time processing and get the response back or use the cloud computing for off-line processing and data warehousing. We are in the process of developing a federated testbeds that can integrate many different cyber physical testbeds to study the interdependencies among different smart city applications (e.g. the impact of power failures on transportations, financial networks, hospitals, etc.); and to use the federated testbed for experimentation, validation and training on the cybersecurity detection and protection tools to be developed in this project.

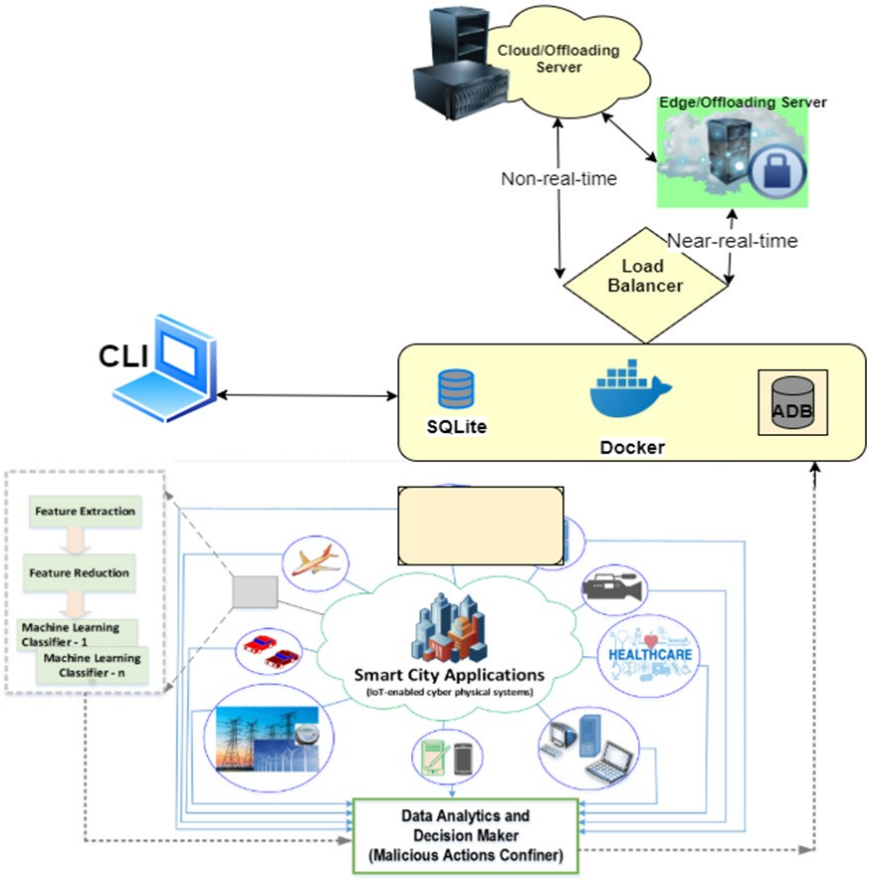


Fig 1. Federated Testbeds for Experimentation, Validation and Demonstration

Dr. Rawat is engaged in research and teaching in the areas of cybersecurity, machine learning, and wireless networking for emerging networked systems, including cyber-physical systems, Internet-of-Things, smart cities, software-defined systems, and vehicular networks. His professional career comprises more than 15 years in academia, government, and industry. He has secured over $4 million in research funding from the US National Science Foundation, US Department of Homeland Security, Department of Energy, National Nuclear Security Administration (NNSA), DoD Research Labs, Industry (Microsoft, Intel, etc.) and private Foundations.

Howard University Research Team

Danda Rawat, Howard University

Dr. Danda B. Rawat is an Associate Professor in the Department of Electrical Engineering & Computer Science (EECS), Founding Director of the Howard University Data Science and Cybersecurity Center (DSC2), Founding Director of Cyber-security and Wireless Networking Innovations (CWiNs) Research Lab, Graduate Program Director of Howard-CS Programs and Director of Graduate Cybersecurity Certificate Program at Howard University, Washington, DC, USA. His team includes graduate and undergrad students as follows.

Erik Muhati
PhD Candidate

Ronald Doku
PhD Candidate

Abdulhamid Adebayo
PhD Candidate

Kikiola Akanbi
Undergrad

Jasmon Cooley
Undergrad

Dalila Scott
Undergrad

Genesis Smothers
Undergrad

Derek Major
Undergrad

Justin Stewart
Undergrad

Oluwadare O. Bankole
Undergrad

17 NTU Students to Receive UA/PACT Network Security Certificate

Salim Hariri, University of Arizona

We are pleased to report that 17 students and staff members from NTU participated in the UA/PACT Network Security Certificate Program that started on Jan 21, 2020, and they will complete their program by May 29,2020.
The certificate objective and topics to be covered are as follows:

Certificate Objectives:

This certificate is intended to technical professionals who want to become experts in network operations and security. The UA-NSC will enable you when you successfully complete this certificate program to use the data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze network events for the purpose of detecting and mitigating attacks against the network.

The skills to be learned according to the National Initiative on Cybersecurity for Education (NICE) (NIST SP 800-181) are the following:

- Skill in conducting vulnerability scans and recognizing vulnerabilities (S0001)
- Skill in analyzing network traffic capacity and performance characteristics (S0004)
- Skill in detecting host and network-based intrusions via intrusion detection technologies (S0025)
- Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump) (S0046)
- Skill in using Virtual Private Network (VPN) devises and encryption (S0059)
- Skill in protecting a network against malware (S0079)
- Skill in using network analysis tools to identify vulnerabilities (e.g., fuzzing, nmap, etc.)
- Skill in configuring and utilizing network protection components (eg., Firewalls, VPNS, Network IDS) (S0084)

The topics that are covered in the program are the following:

Block 1: Network Design and Configuration
Block 2: Introduction to Network Security and Vulnerability Analysis
Block 3: Virtual Private Network
Block 4: Network Monitoring Tools
Block 5: Network Vulnerability Analysis
Block 6: Network Attacks
Block 7: Network Security Tools
Block 8: Secure Network Design and Configuration

Navajo Technical University Research Team

Frank Stomp, Navajo Technical University

NTU is a technical university whose student body is mostly composed of Native Americans. The PIs at NTU are dedicated in undergraduate education and undergraduate research. Dr. Stomp has a strong technical background in distributed computing algorithms and cryptography. Frank received his bachelor's and master's from the University of Utrecht in Mathematics, and his PhD from Eindhoven University of Technology, Netherlands. His research and professional experiences include Wayne State University, Oakland University, Salish Kootenai College and Navajo Technical University.

In early January 2020, three (undergraduate) students were hired as student interns to work on the PACT research activities. The student area of expertise fits into one of the STEM areas:

- Mathew Ellison, computer science, will work on the programming project (using Python) implementing the German enigma machine.
- Tyranni Shepherd (environmental science) and Meriel Simpson (information technology) will work on machine learning.

There were once-a week-meetings, but communication in the last month has been challenging. This is due to the closure of campus to students, because of the COVID-19 outbreak.

Many of the registered students do not have a laptop or Wi-Fi at home. As part of the PACT budget, we have ordered the necessary computers and we hope to be delivered to the students soon.

The three students have been given research material to study machine learning and pointers to related work. They need a significant amount of help, especially when the material is technical. The PACT research team is developing training materials on machine learning and AI techniques. Once these training programs become available, these students will be registered in order to provide them with the required knowledge so they can succeed in the development of ML-based research projects.

Following students enrolled in the first Network Security Certificate Course.

Aliyah Sodamade,
Ashton Brown,
Benveno Yazzie,
Conrad Begay,
Deirdra Deswood
Felicie Trebian,
Joel Yazzie,
Jonathan Smith,
Marcie Vandever,
Marla Price,
Mathew Ellison
Monsuru Ramoni,
Nylana Murphy,
Shalii White ,
Victoria Charley,
Wanda Jimmie,
Wynona Wilson

Publications and Presentations

Accepted

H. Liu and G. Ditzler, (2020) “Detecting Adversarial Audio via Activation Quantization Error” in the proceedings of the IEEE/INNS International Joint Conference on Neural Networks.

Submitted

Shao, Sicong, Cihan Tunc, Amany Al-Shawi, and Salim Hariri, (2020) "Ensemble of Ensemble Learning-based Author Attribution for Internet Relay Chat Forensics," ACM Transactions on Management Information Systems (TMIS).

Published

1) K.S. Peng, G. Ditzler and J. Rozenblit, (2019) "Self-Supervised Correlational Monocular Depth Estimation using ResVGG Network," International Conference on Intelligent Systems and Image Processing

2) G. Ditzler, S. Miller, and J. Rozenblit, (2019) "Learning What We Don’t Care About: Regularization with Sacrificial Functions," Information Sciences, vol. 496, pp. 198-211.

3) H. Liu and G. Ditzler, (2019) "A Semi-Parallel Framework for Greedy Information-Theoretic Feature Selection,” Information Sciences, vol. 492, pp. 13-28.

4) Shao, Sicong, Cihan Tunc, Amany Al-Shawi, and Salim Hariri, (2019) "One-Class Classification with Deep Autoencoder Neural Networks for Author Verification in Internet Relay Chat." In 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), pp. 1-8. IEEE.

5) Shao, Sicong, Cihan Tunc, Amany Al-Shawi, and Salim Hariri, (2019) "Automated Twitter Author Clustering with Unsupervised Learning for Social Media Forensics." In 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), pp. 1-8. IEEE.

Presented

1) K.S. Peng presented at the International Conference on Intelligent Systems and Image Processing. The date of the conference was 9/5-9/9/2019

2) K.S. Peng presented at the International Conference on Intelligent Systems and Image Processing and received the best presentation award. The date of the conference was 9/5-9/9/2019.

Awards

Title: Tactical Cyber Immune System
PI: Gregory Ditzler
Amount: $200,000

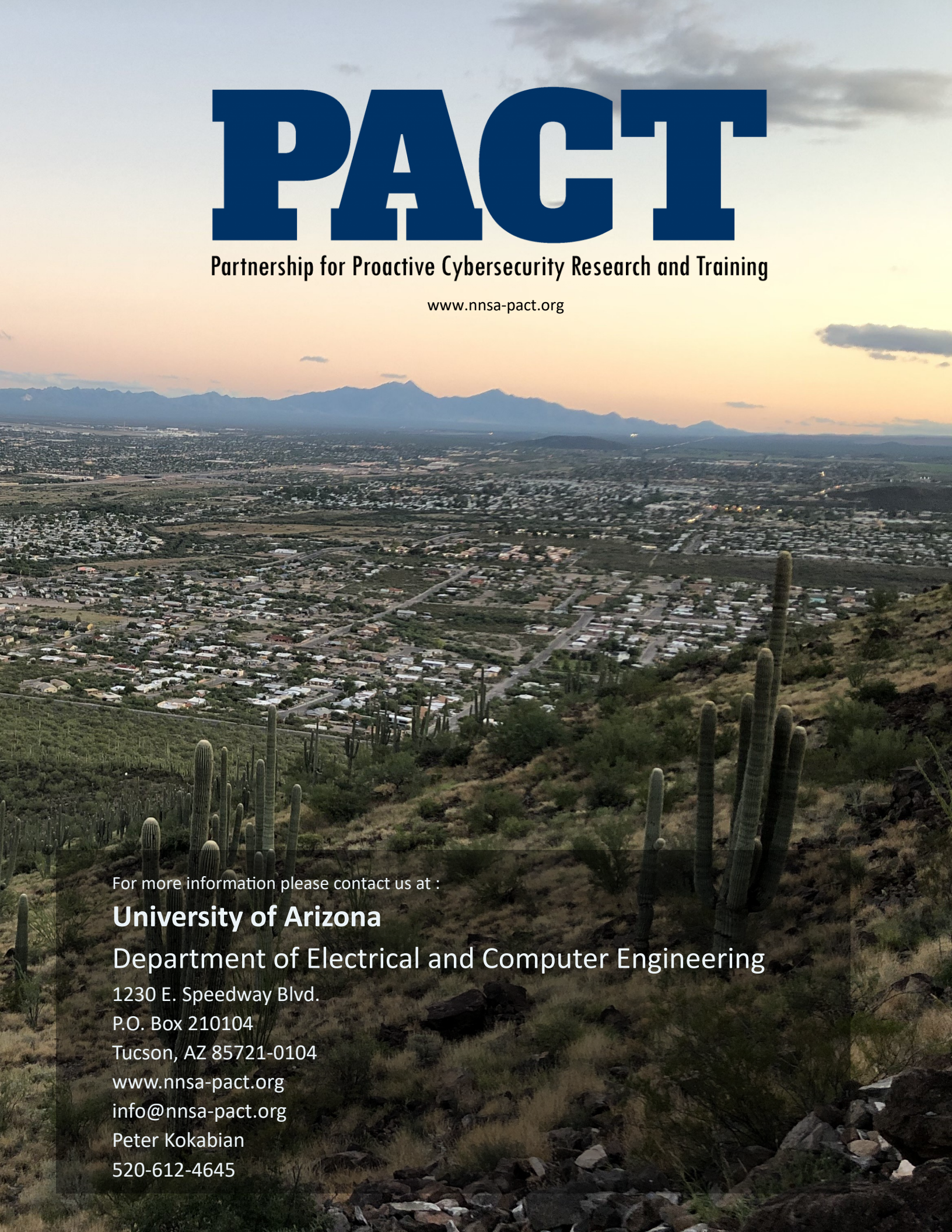
Abstract: This project leverages the tools and results to build a fully functional tactical cyber immune systems (TCIS) prototype. The TCIS prototype's tangible benefits to end-users of TCIS will be: (i) Maintaining acceptable performance of cyber systems and applications in spite of malicious attacks; (ii) Surveillance and autonomic enforcement of normal user behavioral semantics in order to seamlessly detect any non-self behavior by users; (iii) Metrics for evaluating the security; and (v) Seamless recovery of a cyber system's components from catastrophic failures and security breaches.

Title: AMAP-based Autonomic Security Operations Center (ASoC)
PI: Ali Akoglu
Co-PI: Gregory Ditzler
Amount: $200,000

Abstract: In this STTP project, we extend the current AMAP prototype to develop an innovative security architecture that assumes any cyber component is malicious until it can be verified that it is free from any malicious components. The autonomic computing provides the mechanisms to take proactive actions to stop cyber-attacks, their propagation as well as mitigates their impacts. The main modules are Continuous Threat Modeling, Cyber Situation Awareness, and Anomaly Behavior Analysis.

Title: CAREER: Learning in Adversarial and Nonstationary Environments
PI: Gregory Ditzler
Amount: $500,000

Abstract: This CAREER studies when and why feature selection fails with an adversary. Not only will this research focus on understanding why feature selection fails, but also the transferability of black and white box attacks on feature selection. This project also proposes to develop novel methods to attack information-theoretic algorithms and approaches for resilient information-theoretic feature selection.



PACT

Partnership for Proactive Cybersecurity Research and Training

www.nnsa-pact.org

For more information please contact us at :

University of Arizona

Department of Electrical and Computer Engineering

1230 E. Speedway Blvd.
P.O. Box 210104
Tucson, AZ 85721-0104
www.nnsa-pact.org
info@nnsa-pact.org
Peter Kokabian
520-612-4645