UA CAC Technews

Cloud and Autonomic Computing Center

National Science Foundation

The University of Arizona

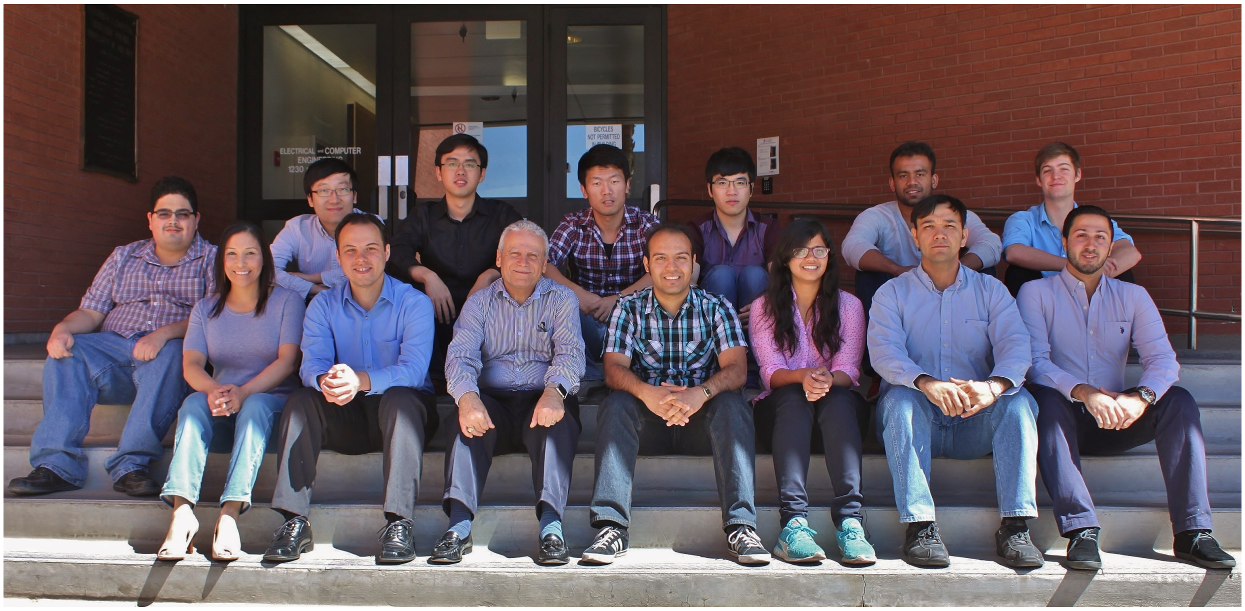
Issue 5

Visit our website: http://nsfcac.arizona.edu

Fall 2016

Update from the Director

It is my please to let you know that our Phase II proposal to extend our NSF/ICRC Center for Cloud and Autonomic Computing (CAC) for another 5 years has been awarded 500K by the National Science Foundation (NSF). The CAC mission is to conduct near-term research projects to advance the knowledge of how to design cloud and autonomic computing systems that are capable of self-healing, self-protecting, and self-optimizing themselves with little involvement of users or system administrators. These systems are sometimes referred to as Self-* systems, where * is a placeholder for a specific objective or attribute to be managed at runtime such as performance, security, fault, availability, energy, etc. Unlike past research that attempted to manage these attributes in isolation, the CAC research approach is a paradigm shift that addresses all these properties in a holistic approach. In Phase II of our NSF Industry/University Cooperative Research Center for Cloud and Autonomic Computing , our goal is to continue to advance the design and deployment of Self-* systems and applications that will overcome the current security and management challenges of IT and Cloud infrastructures. Autonomic computing provides the methodology to continuously monitor, analyze, and manage the systems, applications, and cyber resources so they can meet their requirements whenever abnormal event is observed or detected.



Inside this issue

Update from the Director (cont. from page 1.)

In Phase II, the Center will focus on new emerging important research areas such as cybersecurity, autonomic cybersecurity protection of cloud systems, and Internet of Things (IoT), and how autonomic computing and cloud services can advance the IoT deployment and services. In this aspect, we will closely collaborate with industry and government agencies that are interested in these new areas of research. The following are concrete examples of industry-relevant ongoing research projects that are being pursued by CAC researchers:

- **Autonomic Cyber Security (ACS)** — In this project, we are developing algorithms to self-protect computers, data, applications and cyber resources with little involvement of users or system administrators. This project will utilize CAC autonomic monitoring tools, Anomaly Behavior Analysis (ABA) methodology, and Self-management tools to deliver the required ACS capabilities.
- **Autonomic Management of Performance and Energy** —This project utilize CAC ABA methodology and data analytics and prediction to optimize performance and energy in large scale data centers and cloud systems.
- **Automated and Integrated Management for Insider Threat Detection**— This project integrates the results from three disciplines (computer science, mathematical and statistical techniques , and social behavior sciences) to reveal, explain and predict patterns of malicious threats. User cyber and bio metrics will be used to analyze and detect malicious user operations or activities.
- **Big Data Cybersecurity Analytics**— This project aims at utilizing big data analytics tools to provide unprecedented cybersecurity capabilities to proactively monitor, analyze and mitigate sophisticated and advanced persistent threats and exploitations.
- **IoT Security Development Framework for Smart Cyber Infrastructures**— This project aims at integrating security issues at all the stages of software development of IoT applications and services rather than being ad-hoc and after thought.
- **Anomaly-based Detection of Attacks against Wireless Networks—** This project aims at applying our ABA methodology to secure and protect all types of wireless network technologies including WiFi, Bluetooth, ZigBee, etc.
- **Resilient Cloud Services (RCS)—** This project leverages Moving Target Defense (MTD), Software Behavior Encryption (SBE) technique, and Autonomic computing to build cloud services that can tolerate any type of attacks (insiders or outsiders), known or unknown, faults or accidents (malicious or natural).
- **Resilient Cyber Physical Systems—** This projects extends the RCS capabilities to smart cities, grids, buildings and cars.
- **Resilient Software Defined Radio Architecture—**This projects extends RCS capabilities to deliver resilient radio and satellite communications that can tolerate and operate normally in spite of Denial of Service (DoS) or jamming attacks.
- **Hacker Data Analytics**— In this project we are developing autonomic bots that can collect information about hackers using IRC forums to identify and predict malicious activities that are being circulated and planned within the hacker communities.
- **Cyber Security Assistant (CSA)** - This project aims at applying ACS technology to secure and protect all types of users (novice or advance) by using ABA and cognitive computing techniques.
- **Autonomic Workflow Management—** This project applies ABA and autonomic computing to achieve self-optimization of large scale scientific and engineering applications.

Benefits of Center Membership

- Collaboration with CAC faculty, graduate students, post-doctoral researchers and with researchers at other Center sites (Texas Tech University and Mississippi State University) as well as with our affiliated universities (University of Detroit, Mercy).
- Select your own project that will be supported by the membership fee. The project will also leverage the funding provided by NSF and the university reduced overhead on the membership fee in order to allow us to support one or more graduate students to work on the company project for one full year and partially support a faculty to supervise the company project.
- Formal periodic reviews along with continuous informal interactions and timely access to reports and papers.
- Access to unique world-class equipment, facilities and other CAC infrastructures at UA and other CAC sites.
- Recruitment opportunities among excellent graduate students.
- Leverage of investments, projects and activities by all CAC members at all sites
- Professional networking with other CAC members who can new customers or partners for competitive funding opportunities.

As we move forward, we would like to invite you to join the Center so together we can develop innovative cloud and autonomic technologies and services that will revolutionize how to design and deploy next generation information and communications services.

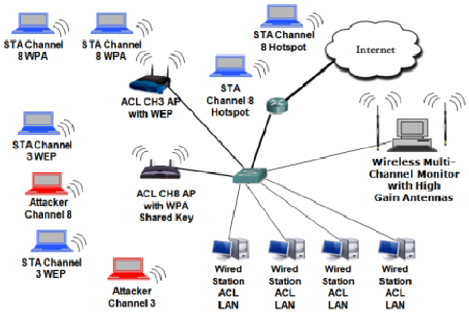
Salim Hariri, UA CAC Director

CAC Cybersecurity Test-beds

Industrial Process Control Test-bed

Private Cloud

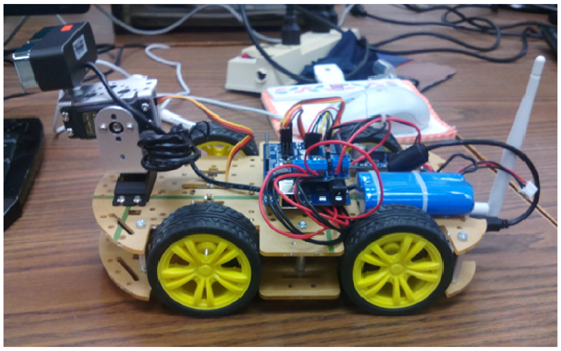
Smart Building

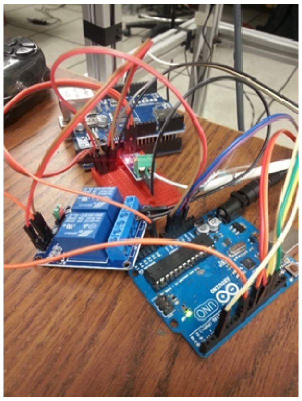


GPU Cluster

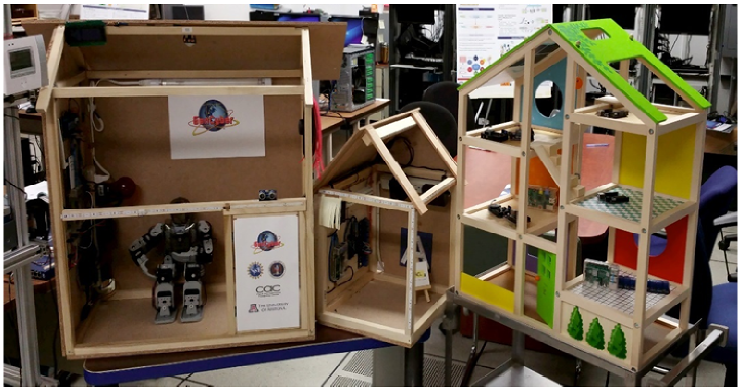
Smart Devices Testbed

- Raspberry PI, Microduino and Arduino
- ZigBee, WiFi, blue tooth, Ethernet
- Modbus, DNP3, Backnet





NI Grid



Autonomic Cyber Security (ACS): A paradigm shift in cyber security

(http://nsfcac.arizona.edu/research/autonomic-cyber-security.html)

By Salim Hariri

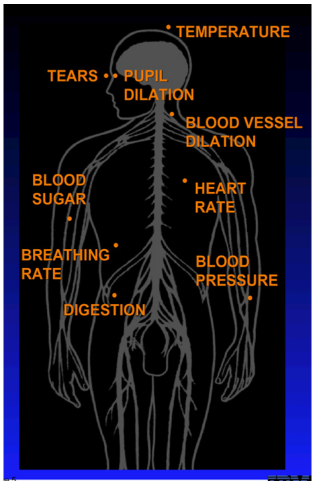


Figure 1. Human nervous system.

Current security analysis, detection and protection systems are mainly static and manually intensive. At the same time, the complexity of networked computing systems, their dynamic behavior, and the availability of many heterogeneous devices that are static and mobile make these tools incapable to accurately characterize current states, detect malicious attacks, and stop them or their fast propagation and/or minimize their impacts. In contrast to static, manual and labor intensive, heuristic analysis, and control and management approaches, we are developing a paradigm shift based on autonomic computing principle inspired by human nervous systems shown in Figure 1. In autonomic management, the cyber infrastructure and services would be self-management with little involvement by users or system administrators to meet their performance requirements (self-optimize), reconfigure to tolerate hardware and/or software faults (self-heal), and stop and/or mitigate the impacts of threats and cyberattacks (self-protect). The salient features of this paradigm are its capabilities to deliver the following:

- **Integrated monitoring, analysis, and management solutions** to allow cyber-infrastructure reasoning that is required to achieve self-diagnostic and self-managed systems. This will lead to cyber superiority operations for critical missions that can be resilient to cyberattacks, hardware/software failures and/or accidents (natural or malicious);
- **Prediction of system operations and behaviors** that uses data mining, information theory, and statistical techniques to aggregate and correlate monitored features to detect and predict accurately any anomalous behavior that might have been triggered by attacks, faults and/or accidents or disasters; and
- **Automated management solutions** that will lead to significant reduction in operational cost and will also provide timely responses to anomalous events to stop and/or prevent rapid propagation of attacks/faults and mitigate their impacts on normal system operations and services.

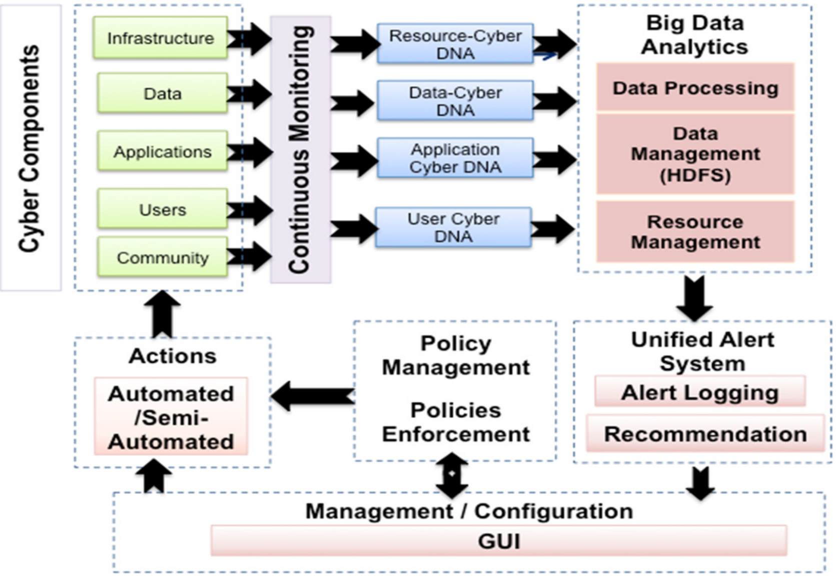


Figure 2. Autonomic Cyber Security (ACS) Development Approach.

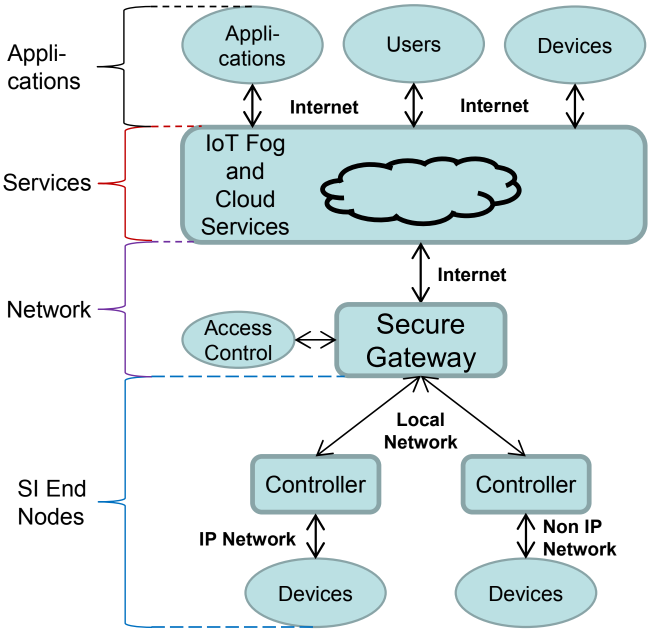
In the development of ACS, our objective is to integrate our Anomaly Behavior Analysis (ABA) methodology to perform data-driven analytics on operations of cyber components. This involved the development of runtime models to identify normal/malicious behaviors. To handle the exponential growth in data complexity, heterogeneity and size, we will use Big Data analytics engine to improve accuracy and scalability. Figure 2 shows the ACS development approach. First we monitor a cyber entity that could be an infrastructure, an application, user or data. The results of cyber component analytics is the creation of cyber DNA components such as Resource-Cyber DNA, Data-Cyber DNA, Application-Cyber DNA and User-Cyber-DNA data structures. Our big data analytics engine (e.g., Spark platform) handles the data processing, while Hadoop Distributed File System (HDFS) handles data management and resource management. The results from the Big Data Analytics are passed to the Unified Alert System where the alerts are logged and recommendations are displayed on the GUI. Finally, the current security and management policies determine what automated or semi-automated actions to take in order to respond in a proactive manner to the detected anomalous events.

IoT Security Framework for Smart Cyber Infrastructures

(http://nsfcac.arizona.edu/research/iot-security-framework.html)

By Jesus Pacheco

Advances in mobile and pervasive computing, social network technologies and the exponential growth in Internet applications and services will lead to the development of the next generation of Internet services (Internet of Things, IoT) that are pervasive, ubiquitous, and touch all aspects of our life. The IoT services will be a key enabling technology to the development of smart cities that will revolutionize the way we do business, maintain our health, manage critical infrastructure, conduct education, and how we secure, protect, and entertain ourselves. The integration of physical and cyber systems as well as the human behaviors and interactions (e.g., producers, consumers, and attackers) will dramatically increase the vulnerability and the attack surface of interdependent infrastructure ecosystems. The most common architecture to monitor and control smart infrastructures such as Smart Homes and Smart Buildings, are Building Automation Systems (BAS) and Supervisory Control and Data Acquisition (SCADA) systems. As BAS and SCADA systems become interconnected with Internet resources and services, they become easy targets to cyber adversaries, especially since they were never designed to handle cyber threats. This makes control system data vulnerable to falsification attacks that lead to incorrect information delivery to users, causing them to take wrong and dangerous actions. It also allows adversaries to potentially execute malicious commands on control systems and remote devices, causing harmful actions. Therefore, it is critically important to secure and protect the IoT operations against cyber-attacks.



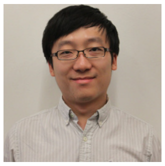
IoT Security Framework for Smart Cyber Infrastruc-

In this project, we introduce our IoT security framework for Smart Homes that consists of four layers (see figure above): end devices (nodes), networks, services, and applications. Then we present a methodology to develop a general threat model in order to better recognize the vulnerabilities in each layer and the possible countermeasures that can be deployed to mitigate their exploitation. In this project, we are developing an Anomaly Behavior Analysis Intrusion Detection System to detect anomalies that could be triggered by attacks against the sensors of the first layer (Smart Infrastructures (SI) End Nodes). We have evaluated our approach by launching several cyberattacks (e.g. Sensor Impersonation, Replay, and Flooding attacks) against our Smart Home testbeds. The results show that our IoT security framework can be used to develop security mechanisms to protect the normal operations of each layer. Moreover, our approach can detect known and unknown attacks for IoT end nodes, with high detection rate and low false alarms.

Collaborators

Clarisa
Grijalva

Pratik
Satam



Zhiwen Pan

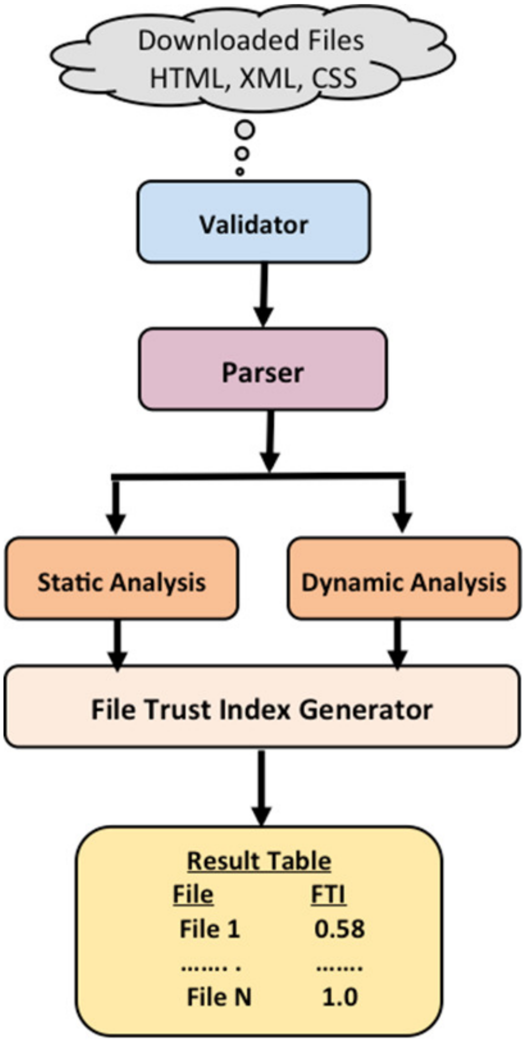
Anomaly Behavior Analysis of Website Vulnerability and Security

(http://nsfcac.arizona.edu/research/aba-website.html)

By Pratik Satam

The world wide web has grown exponentially over the previous decade in terms of its size, complexity, as well as with respect to the number of users. In fact, web use has become pervasive to touch all aspects of our life, economy and education. These rapid advances have also significantly increase the vulnerabilities of websites that are being hacked on a daily basis. The internet currently hosts more than a billion websites and has an even more in the number of daily users. A wide range of heterogeneous devices (mobile or stationary) access the internet for various functionalities and with the introduction of Internet of Things (IoT), the number is expected to grow to more than 50 billion devices. Most of the content on the internet is hosted on websites which are basically Hyper Text Markup Language (HTML) webpages. The resent advances in html protocol and the browser stacks allow the webpages to be accessed by any device that runs a browser software and has Internet connectivity. This rapid advances have also significantly increased the vulnerabilities of websites that are being hacked on a daily basis. The web vulnerability has provided unprecedented opportunities for cybercrime and malicious activities that can be launched by individuals, groups or government such as illegal financial transactions, data breaches, identity theft, stealing intellectual properties, etc. The web attacks range from phishing, using webpages to deliver malware to more complex attacks that include cross site scripting attacks, cookie poisoning attack etc. With no effective website security measures in place, one can expect the website security to be even more critical.

The main goal of this research project is to overcome this challenge by developing an online anomaly behavior analysis of websites (e.g., HTML files) to detect any malicious codes or pages that have been injected by web attacks. Our anomaly analysis approach (see figure) utilizes feature selection, data mining, data analytics and statistical techniques to identify accurately the web page contents that have been compromised or can be exploited by attacks such as phishing attacks, cross site scripting attacks, html injection attacks, malware insertion attacks, just to name a few. Our preliminary evaluation results validated the effectiveness of our approach when applied to more than 10,000 files. The results showed that our approach can detect malicious HTML files with a true positive rate of 99% and a false positive rate of 0.8% for abnormal files.



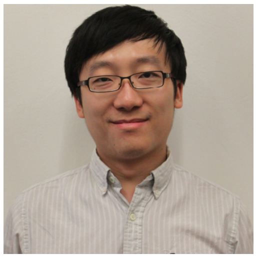
File	FTI
File 1	0.58
……. .	…….
File N	1.0

Collaborators

Alain Bazibuhe

Fabian De La Peña

Douglas Kelly (Avirtek)

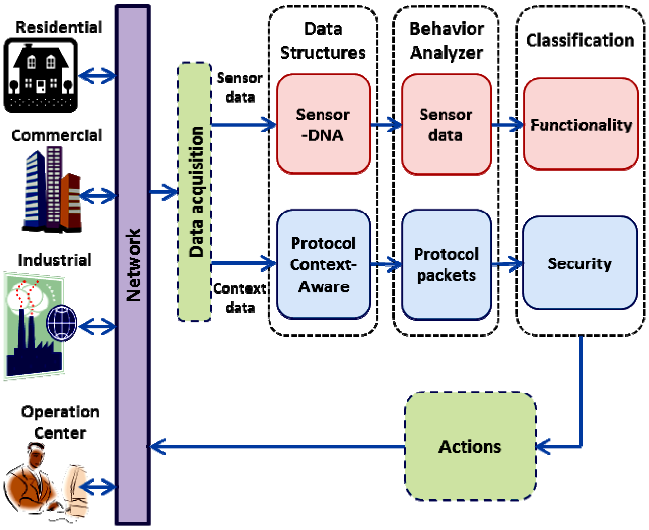


By Zhiwen Pan

Anomaly Behavior Analysis for Building Automation Systems

(http://nsfcac.arizona.edu/research/aba-bas.html)

Advances in mobile and pervasive computing, electronics technology, and the exponential growth in Internet applications and services extends Cloud computing and services to the edge of the network that we refer to as the Fog computing. Since Fog computing offers services at network edge, its advantages to offer these services with low service latency, high quality, support for mobility, awareness of location, and easier implementation of security measures. Building automation Systems (BAS) is an important service for IoT and Fog computing. BAS aims at integrating building equipment with sensors, actuators, and control devices to achieve reliable and efficient operations, and to significantly reduce operational costs. Its implementations range from services for occupants' comfort to critical services such as fire detection, physical access control, and power management. A recent trend of BAS is to construct interconnection between smart buildings and off-site partners such as equipment vendors, and energy service contractors, so that smart infrastructures can work together as Fog assets to ensure reliability. However, with the use IoT techniques in BAS, we are experiencing big challenges to secure and protect such advanced information services due to the significant increase in the attack surface. Even devices which are intended to operate in Local Area Network (LAN) are sometimes likely to be connected to the Internet. There is a huge risk that malicious users may compromise these devices, and launch attacks with high impact and severity. Common threats for BAS network (e.g. network sniffing, port scanning, packet injection, replay attack, Man-In-the-Middle, etc.) can cause disruptions, malfunctions, or even life threatening scenarios, e.g. the fire detection system can be stopped by using a Denial of Service (DoS) attack. Since there is no intrusion detection and prevention available for BAS networks, proposing a reliable security mechanism which can monitor the behavior of BAS assets, becomes a major research issue.



ABA-IDS Methodology

In this project, we are developing an intrusion detection system (IDS) for BAS protocols and sensors, based on the concept of anomaly behavior analysis (ABA). In our approach (see figure above), the information from BAS protocol is continuously monitored to extract its features (e.g. packet flow amount, header, payload, etc.) which are used to describe the behavior of BAS assets. The collected features are modeled into two types of data structures: Protocol Context Aware Data Structure (PCADS) and Sensor-DNA (s-DNA). Behavior analysis methods including Discrete Wavelets Transform (DWT) and rule based abnormal behavior analysis are implemented for detecting anomaly BAS behaviors based on the two models.

Collaborators

Jesus
Pacheco

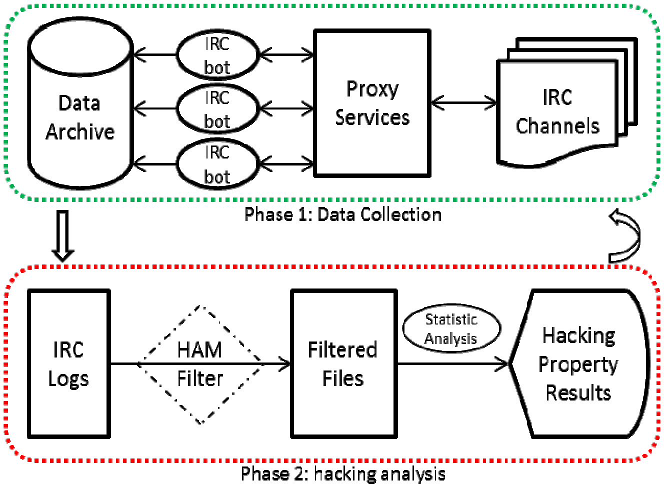
Pratik
Satam

Cihan
Tunc

Data Analytics of Hacker IRC Information

(http://nsfcac.arizona.edu/research/data-analytics-irc.html)

By Jiakai Yu



IRC Data Collection and Analysis System Design

Cyber security is a challenging research problem especially when one considers exponential growth in information technologies. As individuals, businesses, and government rely heavily on cyber infrastructure to meet their advanced information services and applications, cyber attacks have also been intensified in number, complexity and impacts. The main cyber security challenge involves the human side, where there has been a continuous growth and advancements in the technologies that can be exploited by hackers to commit cybercrime. Traditional cyber security techniques and tools have focused on the cyber infrastructures, protocols and applications. For example, vulnerability scanning tools (e.g., OpenVAS) analyze the vulnerabilities in computers, networks and applications. On the other hand, little work is done to protect against cybercriminal by focusing on the human side, cognitive behaviors and goals. Specifically, designing a system to protect our cyber infrastructure and information services against cyber adversaries is one of the unfulfilled tasks as highlighted in a 2011 report on cyber security published by the National Science and Technology Council (NIST). By focusing on the behavior and understanding the goals of cybercriminals, we can build comprehensive protection techniques and algorithms against cybercriminals.

Server	Channel
irc.anonops.com	#anonops
irc.evilzone.org	#evilzone
irc.evilzone.org	#securityoverride
irc.undernet.org	#cc-trade
irc.secfo.org	#hakologv
irc.freenode.net	#r_netsec
irc.freenode.net	##security
irc.freenode.net	#droidsec
irc.freenode.net	#corelan
irc.hak5.org	#hak5
Irc.efnet.org	#security
cfyfz6afpgfeist.onion	#agora
ixf6tm3pfbdv4n2b.onion	#anonet

Recent reports on the behavior of hacker groups that use IRC forums gave noteworthy data to cyber security experts. Investigation of the hacker IRC information helped discovering cybercriminal operations, their near-future activities, and enabled proactive cyber security measures against cyber-assaults; for example, researchers were able to recognize botnet administrators, check the spread of malicious tools and skills, and identify key members in hacker communities. The goal of our research is to expand the capabilities available to collect and analyze hacker IRC information. In this project, we are developing an automated approach to collect information about hackers, and attempt to understand their behaviors and goals as shown in the figure above. Internet Relay Chat (IRC) forums as shown in Table have been widely used by hackers to exchange data, tools and train new novice hackers. In our approach, we have implemented an automated framework that uses several bots to collect IRC messages from malicious forums and analyze them. A resilient botnet mechanism is utilized to ensure complete IRC data collection. In addition, we developed an intelligent hacking language module based on Stanford CoreNLP to analyze hacker activity. Our experimental results show that our botnets can be used to effectively monitor, analyze, and predict hacker activities and goals.

Collaborators

Dr. Cihan Tunc

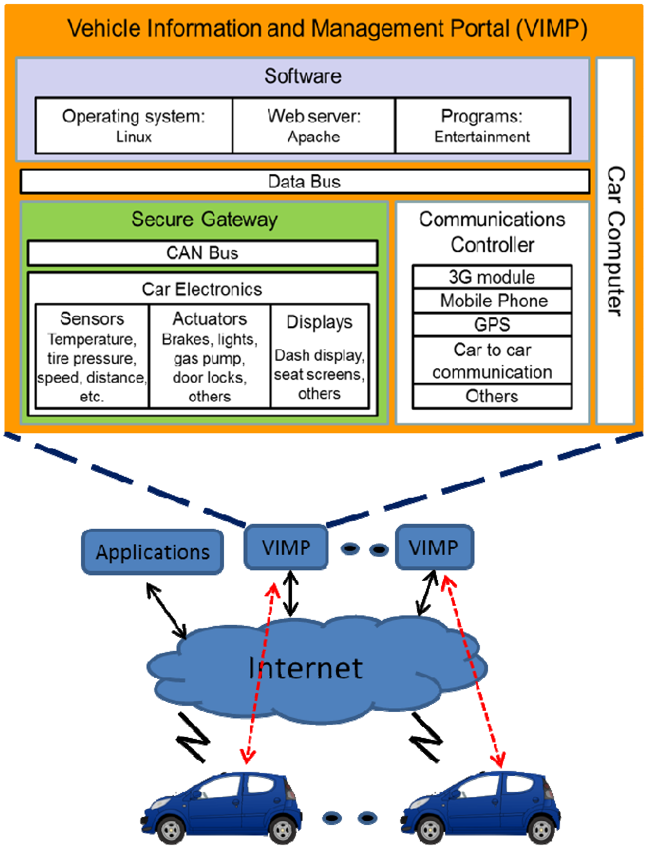
Dr. Rui Zhang
(IBM)

Vehicle Information and Management Portal (VIMP)

(http://nsfcac.arizona.edu/research/vimp.html)

By Shalaka Satam

Modern vehicles are controlled by complex distributed systems comprising large amount of heterogeneous nodes with rich connectivity provided by internal networks and Internet. With the exponential increase in vehicle intelligence and connectivity, security and privacy have become the main concerns for automotive systems. Researchers have shown that modern vehicles can be attacked from a variety of interfaces such as USB, and wireless channels. Furthermore, by compromising a single control unit, a capable attacker may gain access to other vehicle units via internal communication buses such as controller area network (CAN), and attack critical subsystems. As CAN gets interconnected with Internet of Things (IoT) resources and services, it becomes easy targets to cyber adversaries, especially since it was never designed to handle cyber threats. It allows adversaries to potentially execute malicious commands on control systems, causing harmful actions (e.g. Disable brake system). Therefore, it is critically important to secure and protect smart vehicle operations against any type of cyber-attacks.



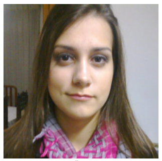
VIMP Architecture

In this project, we are developing a trustworthy Vehicle Information and Management Portal (VIMP) services to support smart car applications. The VIMP will make all the components and/or devices within a vehicle universally accessible by visiting the vehicle portal that will be unique for each car or vehicle. The VIMP uses cloud and internet technologies for communication (voice, video), entertainment, monitoring traffic, and emergencies. Furthermore, each VIMP is accessible in a similar way to the ubiquitous access to any internet website. For example, one IoT service allows auto manufacturers to continuously obtain test field data as well as provide on-line capability to update vehicle firmware at any time, and from any place. By connecting cars to VIMP services, we can offer revolutionary information services in entertainment, communication, collaboration, on-line monitoring to increase safety by proactively and reactively warning about the vehicle current dangerous conditions, continuous access to field data, on-line firmware update, just to name a few. In addition, we will show how our ABA methodology can be applied to secure and protect the VIMP services against a wide range of cyber-attacks that target vehicle sensors.

Collaborators

Jesus
Pacheco

Pratik
Satam



Helena
Berkenbrock

Dr. Nizar Al-Holou
(University of Detroit Mercy)

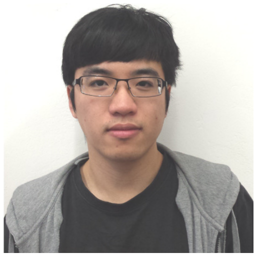
Mohammad
Horani
(Mitsubishi)

Ray
Doug
(Mitsubishi)

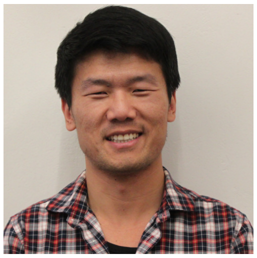
Gareth
Williams
(Mitsubishi)

An Autonomic Workflow Performance Manager for Weather Research and Forecast Workflows

(http://nsfcac.arizona.edu/research/autonomic-workflow.html)



by Shuqing Gu



and Likai Yao

Tropical cyclones (TCs) remain among the most economically and socially destructive phenomena. In the U.S. the high impacts associated with landfalling TCs can be attributed to increasing populations in vulnerable areas, more especially along the Gulf of Mexico. At this time, the only effective method to predict hurricane location plus the spatial extent of potential physical impacts is using numerical weather prediction models. One of the biggest challenges in hurricane forecasting is to maximize the use of multiple data streams coming in at rates much faster than the 6-hr initialization time of the forecast model. A system that can intelligently assess where observations will provide the most impact in the model initial fields and can continuously and automatically assess, and update, or even cancel and reinitialize model forecasts will better maximize resources and improve forecast skill, providing a tremendous advance in our ability to manage these types of disasters. Such a nonlinear system of forecast models requires a testbed to experiment with and evaluate innovative methods to continuously assimilate observations, assess forecast accuracy, and maintain an optimal number of ensemble members to be able to characterize the uncertainty in the model forecast. As a part of this research, we are developing an autonomic workflow performance manager (AWPM) to test an integrated dynamic hurricane modeling environment for an end-to-end predictive tool to inform interested actors of real hazards associated with a landfalling hurricane.

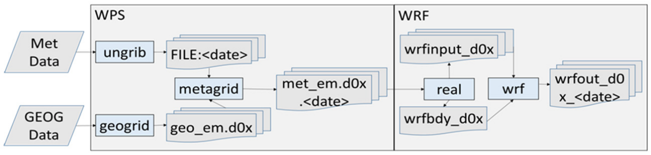


Fig 1. WRF modeling system dataflow

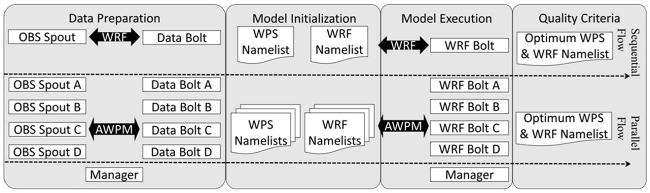


Fig 2. Stages of sequential and parallel workflow for weather forecast simulation and parameter selection with four nodes

The AWPM architecture consists of two main components, a cyber-physical system (CPS) and an autonomic runtime management (ARM). The CPS is implemented based on the Weather Research and Forecast (WRF) model shown in Figure 1 and the development environment utilizes Apache Hadoop big data analytics framework that includes a storage part (Hadoop Distributed File System - HDFS), a processing part (MapReduce), and a real-time data processing part (Apache Storm). This enables us to improve the process and reduce the time with which accurate models are identified. The CPS enables processing and analyzing observation data for real-time forecasting and assimilating the massive data streams. High throughput is achieved by methods that allow eliminating computations on observed data that do not meet the quality criteria. This in turn helps improve the accuracy of the predictions and trigger a new forecast prediction based on the observed data. The ARM enables monitoring and analyzing the interactions between physical systems so that the dynamically changing computation models and resource requirements are matched seamlessly. We have implemented the WRF workflow in parallel and compared its performance with sequential workflow execution as shown in Fig 2. Our preliminary results show significant speedup can be achieved by using our approach.

Collaborators

Dr. Cihan Tunc

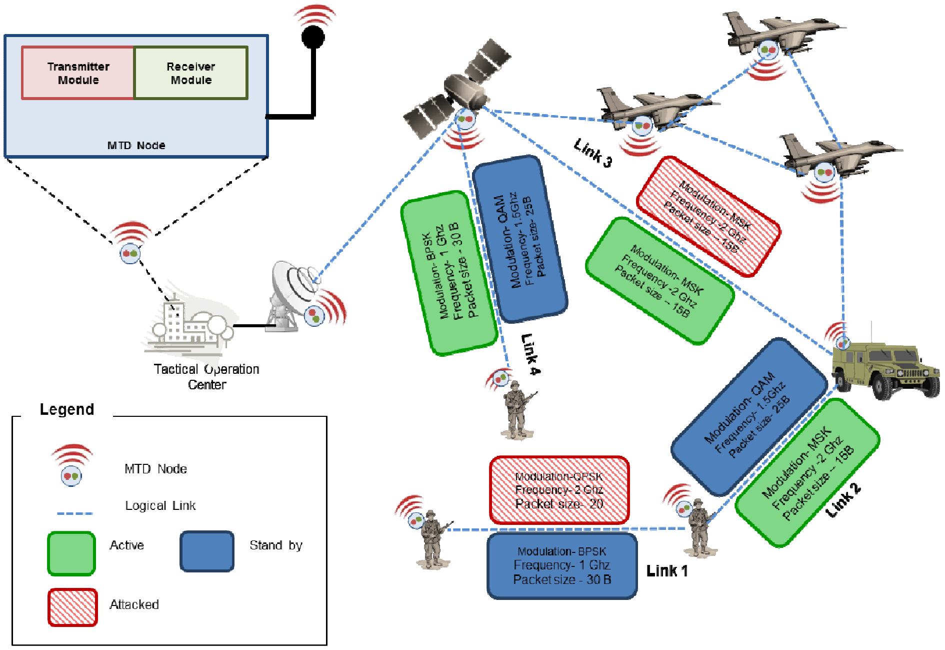
Dr. Ali Akoglu

by Firas Almoualem

Resilient Software Defined Radio Communications

(http://nsfcac.arizona.edu/research/resilient-radio.html)

As the use of wireless technologies increases significantly due to easy of deployment, cost-effectiveness and increase in bandwidth, there a strong need to make the wireless communications reliable, and resilient to attacks or faults (malicious or natural). Wireless communications are inherently prone to attack due the open access to the medium. However, current wireless protocols have addressed the privacy issues, but have failed to provide effective solutions against denial of service attacks, session hijacking and jamming attacks.


Transmitter Module
Receiver Module
MTD Node
Tactical Operation Center
Link 3
Link 4
Link 1
Link 2
Modulation- BPSK Frequency- 1 Ghz Packet size - 30 B
Modulation- QAM Frequency- 1.5Ghz Packet size- 25B
Modulation- MSK Frequency -2 Ghz Packet size – 15B
Modulation- MSK Frequency -2 Ghz Packet size – 15B
Modulation- QAM Frequency- 1.5Ghz Packet size- 25B
Modulation- MSK Frequency -2 Ghz Packet size – 15B
Modulation-QPSK Frequency- 2 Ghz Packet size- 20
Modulation- BPSK Frequency- 1 Ghz Packet size - 30 B
Legend
MTD Node
Logical Link
Active
Stand by
Attacked

In this project, we are developing a resilient wireless communications architecture based on Moving Target Defense and Software Defined Radios (SDRs). The approach achieves its resilient operations by randomly changing the runtime characteristics of the wireless communications channels between the different wireless nodes in order to make it extremely difficult to succeed in launching attacks. The runtime characteristics that can be changed include packet size, network address, modulation type, and the operating frequency of the channel. In addition, the lifespan for each configuration will be random.

To reduce the overhead in switching between two consecutive configurations, we use two radio channels, one will be designated as the active channel while the second acts as a standby channel as shown in figure above. The standby channel will be used as the active channel in the next time interval. This will harden the wireless communications because the attackers need to figure out how to exploit and launch attack before the current configuration changes to the standby one. Furthermore, in the unlikely case of a successful attack, it will be effective only for the remaining time in the current configuration because it will be changed in the next interval. We use Anomaly Behavior Analysis to detect attacks on the wireless links and to trigger the switch the standby channel. Configuration. We have implemented an SDR testbed and used GNU-Radio which is an open source software to provide the required tools to program the SDR components. We have evaluated the performance of our approach against wireless attacks such as jamming attacks. Our experimental results and evaluation show that our approach can tolerate a wide range of attacks against wireless networks.

Collaborators

Pratik Satam

Dr. Cihan Tunc

HeartCyPert: Design and Analysis of a Heart Cyber Expert System

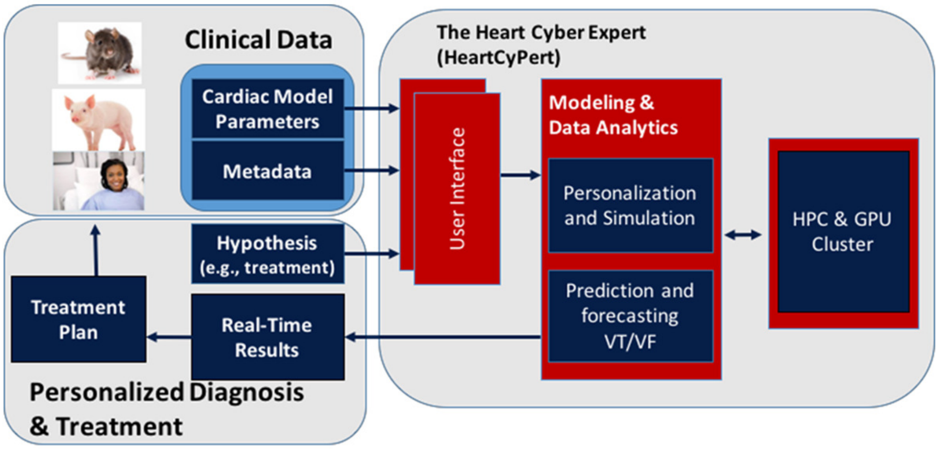
(http://nsfcac.arizona.edu/research/heartcypert.html)

By Ehsan Esmaili

And Talal Moukabary, Research Professor, M.D.

Chronic heart failure (CHF) is a leading cause of morbidity and mortality worldwide with over 600,000 new cases diagnosed annually in the United States alone, and the most common cause of sudden death in CHF patients are ventricular arrhythmias. We do not know how to predict which patients with CHF will die from sudden death except that they all have poor heart or left ventricular function.

The goal of this project is to develop a 3D computational model to predict if patients are at high-risk of a ventricular arrhythmia. Currently, developing a 3D model that characterizes the electrical activity in the heart is an extremely computationally challenging task; therefore, cardiac researchers have chosen to use less accurate models that are computationally tractable. In this project, we are developing a data-driven engine that uses data from animals and patients with CHF to gather parameters for a 3D cardiac model that can be used to predict if the patient is at high-risk of a ventricular arrhythmia, which will aid researchers in developing a personalized treatment plan.


Clinical Data
Cardiac Model Parameters
Metadata
Hypothesis (e.g., treatment)
Treatment Plan
Real-Time Results
Personalized Diagnosis & Treatment
The Heart Cyber Expert (HeartCyPert)
User Interface
Modeling & Data Analytics
Personalization and Simulation
Prediction and forecasting VT/VF
HPC & GPU Cluster

HeartCypert Architecture

The ultimate goal of our research is to develop a cognitive software environment, a Heart Cyber Expert (HeartCyPert, see figure), that can use IBM Watson-like cognitive computing, and data mining and search algorithms to help cardiac researchers, clinicians, and device industries develop new approaches to treat patients with CHF, and ultimately provide inference about whether a subject is of high risk of sudden cardiac death. HeartCyPert achieves this goal by using the clinical data collected from rats and pigs, beyond that of ejection fraction, to parameterized a personalized 3D electrophysiological model of the heart. The personalized 3D model can then be used to simulate new effects of new treatments on a subject in silico to verify if the treatment is safe.   The development of such a data analytics engine that provides a feedback loop for performing cardiac research with existing clinical data and mathematical models will significantly improve the time and resources of clinicians studying VT, and provide an accurate approach to correctly identifying subjects that are at high risk VT/VF.

Collaborators

Dr. Gregory Ditzler

Dr. Ali Akoglu

Dr. Salim Hariri

Dr. Steven Goldman
And
Dr. Elizabeth Juneman,
UA College of Medicine

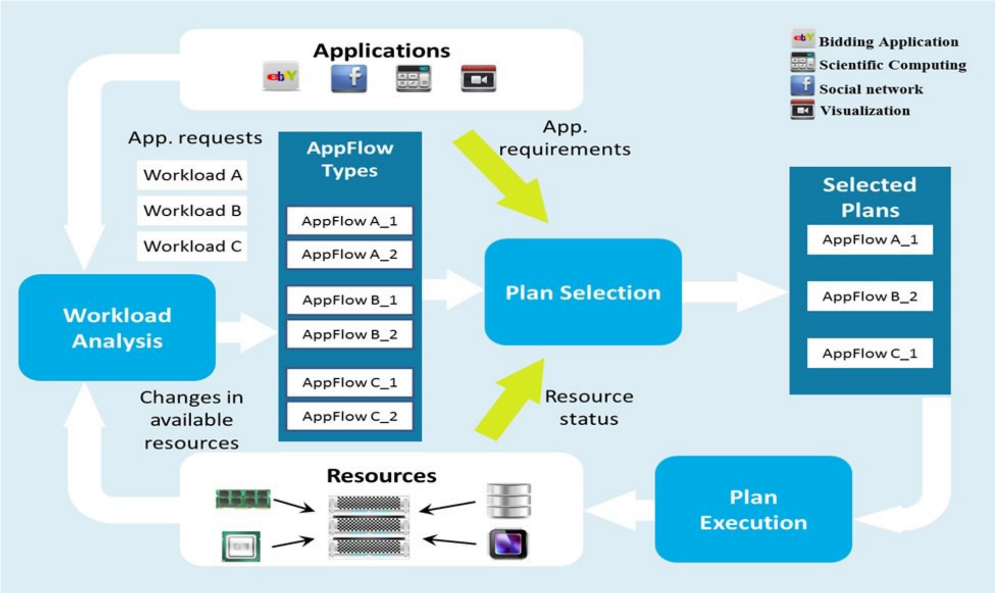
Autonomic Cloud Management System

(http://nsfcac.arizona.edu/research/autonomic-cloud.html)

By Cihan Tunc

And Farah Fargo

With the rapid growth of data centers and clouds, the power consumption and power cost for such systems have become critically important to be managed efficiently. Several research studies have shown that data servers typically operate at a low utilization of 10% to 15%, while their power consumption is close to those at peak loads. With this significant fluctuation in the workloads, an elastic delivery of computing services with an efficient power provisioning mechanism becomes an important design goal. Our work presents an autonomic power and performance management system that utilizes AppFlow-based reasoning to configure virtual machine (VM) resource allocation dynamically during runtime. Our approach, shown in figure below, continuously monitors the workload behavior to determine the current operating point of workloads and the VMs running these workloads, and then predicts the next operating point for these workloads. This enables the system to allocate the appropriate amount of VM resources to efficiently run the workloads with minimum power consumption. We have experimented with and evaluated our approach to manage the VMs running RUBiS bidding application. Our experimental results showed that our approach can reduce the VMs' power consumption up to 84% compared to static resource allocation and up to 30% compared to other methods with minimum performance degradation.



Autonomic Cloud Management Architecture

Collaborators

Dr. Ali Akoglu

Dr. Salim Hariri

Dr. Youssif Al-Nashif
Florida Polytechnic University

by Fabian De La Peña

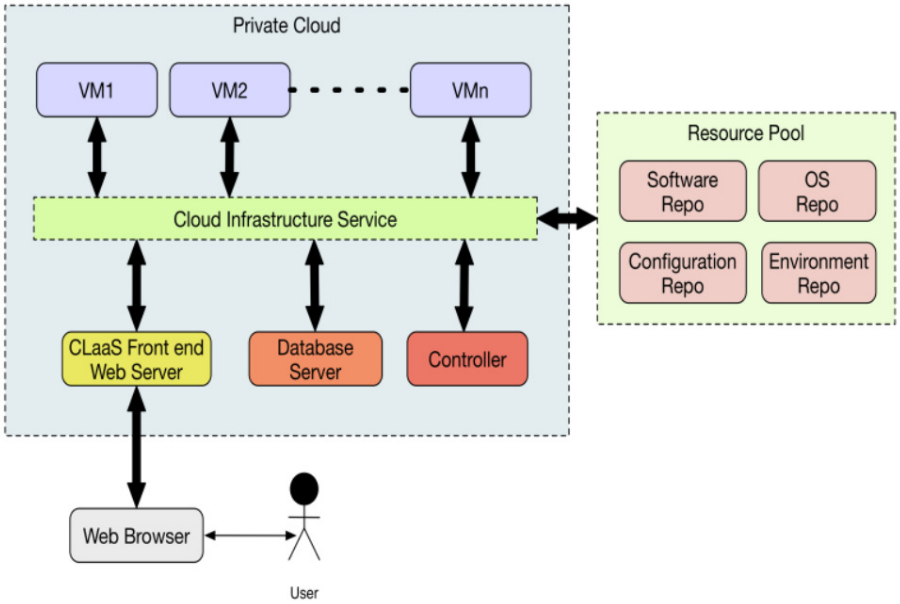
Cybersecurity Lab as a Service (CLaaS)

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

And Cihan Tunc

The explosive growth of IT infrastructures, cloud systems, and Internet of Things (IoT) have resulted in complex systems that are extremely difficult to secure and protect against cyberattacks which are growing exponentially in complexity and also in number. Overcoming the cybersecurity challenges is even more complicated due to the lack of training and widely available cybersecurity environments to experiment with and evaluate new cybersecurity detection and protection methods. Therefore, the goal of this research is to address the education, training, and experimentation challenges of the cybersecurity by exploiting cloud services.

In this work, we design, analyze, and evaluate a cloud service we refer to as Cybersecurity Lab as a Service (CLaaS), which offers virtual cybersecurity experiments that can be accessed from anywhere and from any device (desktop, laptop, tablet, or mobile device) with Internet connectivity. In CLaaS, we exploit cloud computing systems and virtualization technologies to provide virtual cybersecurity experiments and hands-on experiences on how vulnerabilities are exploited to launch cyberattacks, how they can be removed, and how cyber resources and services can be hardened or better protected.



CLaaS architecture using private cloud

Collaborators

Dr. Salim Hariri

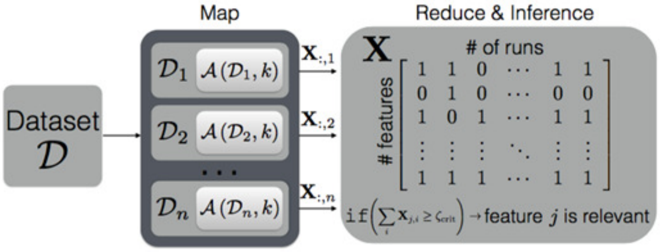
Scalable Feature Subset Selection and Learning in Dynamic Environments

(http://nsfcac.arizona.edu/research/feature-selection.html)

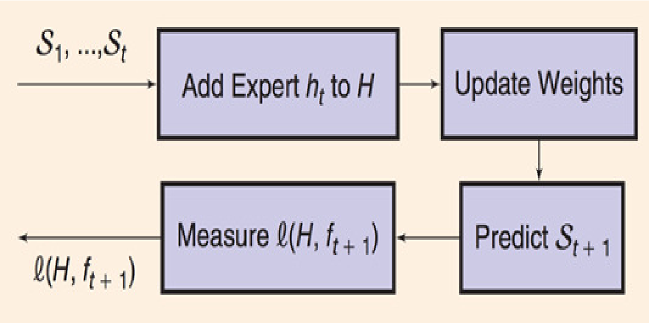
By Dr. Gregory Ditzler

And Heng Lui

Feature subset selection is an important step towards producing a classifier that relies only on relevant features, while keeping the computational complexity of the classifier low. Feature selection is also used in making inferences on the importance of attributes, even when classification is not the ultimate goal. For example, in bioinformatics and genomics feature subset selection is used to make inferences between the variables that best describe multiple populations. Unfortunately, many feature selection algorithms require the subset size to be specified a priori, but knowing how many variables to select is typically a nontrivial task. Other approaches rely on a specific variable subset selection framework to be used. The University of Arizona's Machine Learning and Data Analytics group examines approaches to feature subset selection that are scalable to large volumes of data. Our contributions include a Neyman-Pearson feature selection (NPFS) hypothesis test, which acts as a meta-subset selection algorithm. NPFS is a parallel feature selection algorithm that is scalable to a large volume of data, while allowing a user the choice of a filter-based objective function and identify the number of relevant features in a data set. Our research in feature selection has been used for data analytics in the life sciences.


Map
Reduce & Inference
Dataset $\mathcal{D}$
$\mathcal{D}_1$ $\mathcal{A}(\mathcal{D}_1, k)$
$\mathcal{D}_2$ $\mathcal{A}(\mathcal{D}_2, k)$
• • •
$\mathcal{D}_n$ $\mathcal{A}(\mathcal{D}_n, k)$
$\mathbf{X}_{:,1}$
$\mathbf{X}_{:,2}$
$\mathbf{X}_{:,n}$
$\mathbf{X}$
# of runs
# features
1 1 0 ⋯ 1 1
0 1 0 ⋯ 0 0
1 0 1 ⋯ 1 1
⋮ ⋮ ⋮ ⋱ ⋮ ⋮
1 1 1 ⋯ 1 1
if$\left(\sum_i \mathbf{x}_{j,i} \geq \zeta_{crit}\right)$ → feature j is relevant

Two of the more common assumptions that applied machine learning researchers make when using an algorithm is that: (1) the training & testing data are sampled from a fixed probability distribution, and (2) there are an equal number of samples from all classes. The former is referred to as concept drift (a.k.a., learning in non-stationary environments) when new data are presented over times, and the latter is known as class imbalance. Our research focuses on developing solutions multiple classifier systems that consider both theoretical and empirical observations for learning in dynamic and uncertain environments.



Collaborators

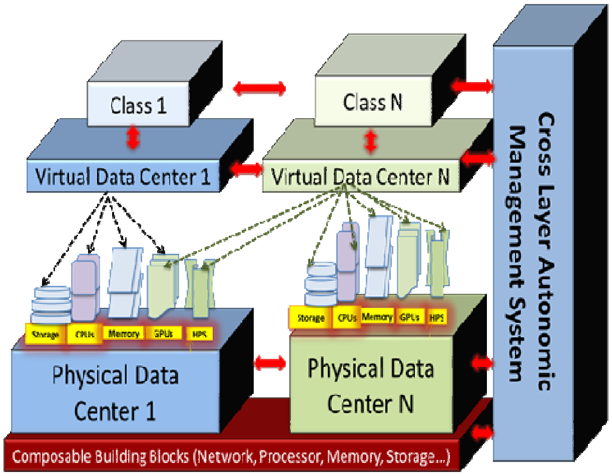
Dr. Salim Hariri

Just In Time Architecture (JITA): A New Paradigm for Designing Agile Data Centers

(http://nsfcac.arizona.edu/research/jita.html)

By Cihan Tunc

Data infrastructures such as Google, Amazon, and eBay are powered by Data Centers (DCs) that contain tens to hundreds of thousands of computers and storage devices running complex software applications. Traditional IT architectures are not equipped to provide an agile infrastructure to keep up with the rapidly evolving application demands as they have distinct system requirements. Next-generation applications are nonlinear scaling and relatively unpredictable growth as a function of inputs being processed. The dynamic changes in demand require the provisioning and re-provisioning of resources, which means considering new hardware designs that can enable distinct design principles for each workload. Minimizing the inefficiencies in the deployment and management of a physical DC infrastructure requires a composable system that utilizes a set of flexible building blocks that can be dynamically and automatically assembled and re-assembled to meet changing workload needs. A composable infrastructure breaks down the resources into storage, compute, and network fabric resources. Control software logically assembles the hardware required by the application from the resource pool, eliminating the costly process of physically configuring hardware to support a specific software application. A composable infrastructure allows matching the resource requirements of a given application with the resources from its pool. The software developer defines the application's requirements for physical infrastructure using policies and service profiles and then the software uses application programming interface (API) calls to create a Virtual Data Center (VDC) that can meet the application service level objectives. The physical location of the resources, is no longer a concern as they are treated as services. Shortened provisioning time and increased flexibility allow reducing both waste of resources and the time it takes to deploy a new application execution environment. A fully composable system requires the ability to assemble individual processors and memory automatically with low overhead and latency. True disaggregation of individual DC components is only feasible with a high speed interconnect technology and low latency. It has been shown that for building DCs, by dynamically composing their basic components (processors, storage, memory devices, GPUs, special hardware), to be feasible from a performance perspective, their interconnection network must operate in >100 Tbps while the latency must be in the <10 microsecond range to support disaggregated data center infrastructures. In this project, we are investigating the architectural support required to implement the JITA architecture shown in the figure above.



Collaborators

Dr. Salim Hariri

Dr. Ali Akoglu

Dr. Howard Siegel Colorado State University

Dr. Ivan Djordjevic

Nirmal Kumbhare

Resilient Applications as a Service (RAaaS)

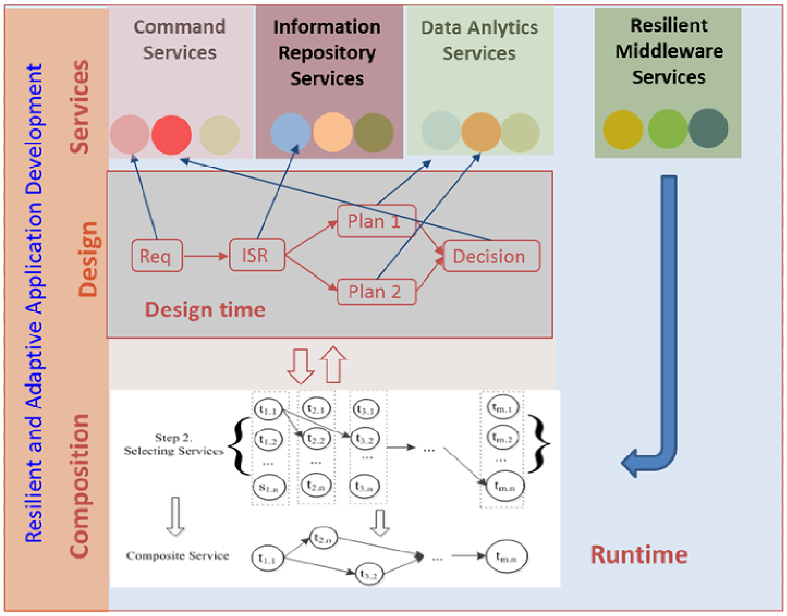
(http://nsfcac.arizona.edu/research/raaas.html)

By Salim Hariri

And Cihan Tunc

At the University of Arizona, Salim Hariri and Cihan Tunc have been working on the development of resilient cloud services with funding from AFSOR DDDAS program and from NSF Center for Cloud and Autonomic Computing. In this project, we aim to explore how to use Service Oriented Architecture (SOA) and Autonomic Computing to further advance this research project in collaboration with the NIST Information Technology Laboratory/ Advanced Network Technologies Division (ITL/ANTD) so we can offer resilient and adaptive applications as cloud services by leveraging the SOA paradigm. Specifically, the objectives of this projects are:

1. Develop an SOA based architecture to design adaptive and resilient cloud applications. 2. Develop Adaptive Resilient Cloud Algorithms: Continuous monitoring and analysis to identify existing vulnerabilities. Develop an analytics/simulation framework to quantify resilience. Based on the vulnerability analysiswe can quantify the resilience for a given resilient algorithm against the detected vulnerabilities. Adapt the resilient algorithm by leveraging the SOA paradigm. 3. Autonomic Control and Management: Adopt UA Autonomic Control and Management (AIM) engine to provide automated control and management of all the resources required to implement the resilient cloud services. In this effort, we will leverage the Autonomia and AIM technologies to implement these capabilities. Develop techniques to reduce the overhead and improve the performance of the Resilient cloud algorithms and techniques. 4. Experimental Testbed and Evaluation: Develop a public cloud testbed (Amazon) to experiment with and evaluate the algorithms and software tools developed in the project. Use the Supercloud testbed to implement the developed resilient cloud services. Explore the use of multiple technologies to implement the proposed resilient architecture such as Amazon AWS, VMware, Xen, KVM, Microsoft technologies, etc.


Resilient and Adaptive Application Development
Services
Design
Composition
Command Services
Information Repository Services
Data Anlytics Services
Resilient Middleware Services
Req
ISR
Plan 1
Plan 2
Decision
Design time
Step 2. Selecting Services
Composite Service
Runtime

The figure shows the architecture to develop resilient and adaptive cloud applications. In this architecture, we leverage the cloud service and SOA paradigms to combine the design stage with the runtime stage. The inseparability between design time and runtime makes it possible to deal with unpredictable events and enable prompt responses to confine and manage mitigation activities.

Collaborators

Dr. Abdella Battou
(NIST, USA)

Dr. Youakim Badr
(Claude Bernard University of Lyon 1)

Dr. Erik Blasch, AFRL

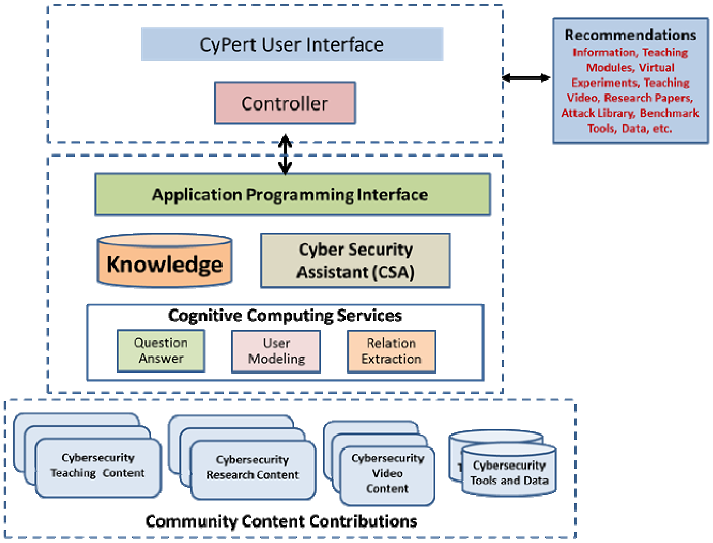
Cyber Security Assistant (CSA) Technology for Everyone

(http://nsfcac.arizona.edu/research/csa.html)

By Salim Hariri

And Cihan Tunc

Current high quality cybersecurity systems are designed for experts or those with huge operations and IT budgets. However, with the integration of Internet in all aspects of our life (e.g., Internet of Things (IoT)) and interdependencies among the cyberspace resources and services, it is well-established fact that the cybersecurity of everyone depends on everyone else. So solving current and future cybersecurity challenges requires developing revolutionary cybersecurity technologies and cyber-assistants (e.g., IBM Watson, Avatars) for all. The goal of this project is to build a Cyber Security Assistant (CSA) technology that will provide a 24/7 online protection seamlessly to all users and answers cybersecurity questions and concerns. In addition, it will provide a virtual Cybersecurity laboratory that can be accessed from anywhere and from any device (desktop, laptop, smart mobile device, etc.) with internet connectivity. It will also provide cybersecurity information, recommendations, and tools, just to name a few. The specific goals of this project are:


CyPert User Interface
Controller
Recommendations
Information, Teaching Modules, Virtual Experiments, Teaching Video, Research Papers, Attack Library, Benchmark Tools, Data, etc.
Application Programming Interface
Knowledge
Cyber Security Assistant (CSA)
Cognitive Computing Services
Question Answer
User Modeling
Relation Extraction
Cybersecurity Teaching Content
Cybersecurity Research Content
Cybersecurity Video Content
Cybersecurity Tools and Data
Community Content Contributions

1. Implement a real-time 24/7 automated cybersecurity's question/answering system (Ask CyPert) that will be powered by IBM Watson cognitive services. The question/answering system will be capable of giving accurate answers to questions about cybersecurity, how to identify vulnerabilities in computers and networks, how to harden cyber resources and services, and recommends virtual experiments to explain how attackers exploit vulnerabilities to launch attacks, and how to detect and protect against cyberattacks. The accuracy of the services will be improved over time as more users give the system feedbacks about the answers and the recommended virtual cybersecurity experiments.

2. Develop a Cybersecurity Lab as a Service (CLaaS) to allow any user to conduct sophisticated cybersecurity experiments without the need to acquire the physical resources and software required to build such experiments by exploiting cloud and virtualization technologies. The CLaaS virtual experiments will also be used by CSA to recommend virtual cybersecurity experiments that will provide users with hands-on experiences on how vulnerabilities are exploited to launch attacks, how can be removed, and how to harden cyber resources and services. The CLaaS will be made portable so that there will be a centralized repository of virtual machines, operating systems, configuration, and environments so that users at different sites can easily share their cybersecurity test environment and experiments.

Collaborators

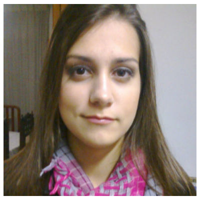
Dr. Salima Hassas
(Claude Bernard
University of Lyon 1)

International Collaborative Projects: Latin American Research Summer Program

by Clarisa Grigalva (Mexico)

Anomaly Detection in Internet of Things Sensors with Discrete Wavelet Transform

Advances in mobile and pervasive computing, social network technologies and the exponential growth in Internet applications and services will lead to the development of the next generation of Internet services (Internet of Things, IoT) that are pervasive, ubiquitous, and touch all aspects of our life. The amount of data being received in real time, from heterogeneous sources in the IoT, makes it extremely difficult to detect when a system is being compromised. In an IoT environment (e.g. Smart Buildings), key components are the sensors for representing the physical world in the digital world. Sensors have been an easy target for attackers because they are typically not well protected and can be easily exploited. Hence, it is critically important to proactively detect when a sensor is compromised, and to take recovery actions. We developed an algorithm to create a sensor-DNA data structure that uniquely defines the correct operations of the sensor and can be used to detect sensor compromises and attacks. We have a variety of sensors that each behaves in a unique manner. Their behavior can be obtained from its features (e.g. frequency and address). In our approach, we use Discrete Wavelet Transform (DWT) to create a reference model, which can be used to accurately characterize the normal behavior of the sensors. Our methodology involves two stages: 1) Offline Training, in which we use the information about sensor normal operations to create the reference data structure that we refer to as s-DNA; 2) Online Testing, where a runtime s-DNA is created to be compared with the reference data structure.



by Helena Berkenbrock (Brazil)

Security Development Framework for Building Trustworthy Smart Car Services

Modern and soon autonomous vehicles are controlled by complex distributed systems comprising large amount of heterogeneous nodes with rich connectivity provided by internal networks and Internet. With the exponential increase in vehicle intelligence and connectivity, security and privacy have become the main concerns for automotive systems. Researchers have shown that modern vehicles can be attacked from a variety of interfaces access such as USB, and wireless channels. By compromising a single control unit, a capable attacker may gain access to other vehicle units via internal communication buses such as controller area network (CAN), and attack critical subsystems. As CAN gets interconnected with Internet, it becomes easy target to cyber adversaries, especially since it was never designed to handle cyber threats. This makes CAN data vulnerable to falsification attacks that lead to incorrect information delivery to users, and thus causing them to take wrong and dangerous actions. It also allows adversaries to potentially execute malicious commands on control systems, causing harmful actions (e.g. Disable brake system). Therefore, it is critically important to secure and protect smart vehicle operations against any type of cyber-attacks. We are developing a trustworthy Vehicle Information and Management Portal (VIMP) services to support smart car applications. The VIMP will make all the components and/or devices within a vehicle universally accessible by visiting the vehicle portal that will be unique for each car or vehicle. The VIMP uses cloud and Internet technologies for communication (voice, video), entertainment, monitoring traffic, and emergencies. Furthermore, each VIMP is accessible in a similar way to the ubiquitous access to any internet website. By connecting cars to VIMP services, we can offer revolutionary new services in entertainment, communication, collaboration, on-line monitoring to increase safety by proactively and reactively warning about the vehicle current dangerous conditions, continuous access to field data, on-line firmware update, just to name a few. In addition, we show how VIMP services can be protected against a wide range of cyber-attacks. (See video at: http://askcypert.org/)

International Collaborative Project: Cyberspace Threat Identification, Analysis, and Proactive Response, Funded by Partner University Fund (PUF)

by Gwenael Ambrosino-Ilepo (France)

Big Data analytics applied to anomaly detection in user behavior

With increase threats of hackers, cybersecurity issues and account protection are a major priority in our society. That's why it's important to analyze users behavior in order to guard them from any malicious insider attacks. The goal of our project will be to create a user DNA using a dataset of his/her cyber activities and operations. In order to process billions of profiles, the approach that must be taken to solve this problem is based on using Big Data technologies such as Hadoop. This software environment provides a scalable framework to analyze huge amount of data by distributing it over a large cluster of high performance servers. A module of Hadoop called Spark is useful in this application, where its architecture allows it to run and process data much faster than Hadoop implementation. The approach took to resolve this problem was more mathematical, the first step taken was to reduce as much as possible the amount of data. Even with tools like Spark, Tera byte of data can take a long time. Hence, it's necessary to use a probability function to compute the probability for each user action to be suspicious. By using parameters from the user sessions, like his/her hours of connections, the number of times he/she connects to an address and a predictive model of his/her action, the user trustworthiness can be calculated

by Enzo Lebrun (France)

Creating a Model to Prevent Eventual Suspicious Activities on a User Account

I.P address, account information are the only things which are identifying people on internet. The problem is that these data are not trustworthy since they can be stolen, changed and people or algorithm can have illegal access to private information. That's why it's necessary to generate a DNA for each user. This model will be generated by using all the data that characterize normal cyber operations of a given user. For example, if the user is browsing on internet and after that he will check his mails, those facts (with many more) will be used to generate the cyber usage pattern for any user. Then if someone is using his computer or his session in significant different pattern from the known profile for that user, the system will trigger an alert. The detection algorithm needs to be tolerant for slight differences in the user behavior (because people doesn't always act the same, we are not robots!). This program will also need to be self-sufficient. If the comparison of the actions on the user sessions shows nothing suspicious at all, then the model will add those data in order to adapt to the actual user behavior.

Recent graduates

Farah Fargo

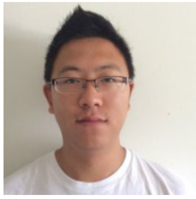
Ph.D. from the Electrical and Computer Engineering Department of the University of Arizona. She is associated with the Center for Cloud and Autonomic Computing (CAC) . Her research areas include autonomic power, performance, and security management for the cloud computing systems and data analytics. Currently she working as Senior HPC System Engineer at Intel Corporation.

Cihan Tunc

Ph.D. from the Electrical and Computer Engineering Department of the University of Arizona. He is associated with the Center for Cloud and Autonomic Computing (CAC). His research areas include autonomic power, performance, and security management for the cloud computing systems and data analytics. Currently he is working as Research Assistant Professor at The University of Arizona.

Pratik Satam

M.Sc. from the Electrical and Computer Engineering Department at the University of Arizona. As an active ACL and CAC member his research has been on cyber security and autonomous protection systems. During his masters, he has been involved in multiple research projects including Intrusion detection systems for distributed Wi-Fi networks, DNS protocol, and the HTTP protocol. Currently he is pursuing his Ph.D. at the ACL lab at the University of Arizona.



Jin Bai

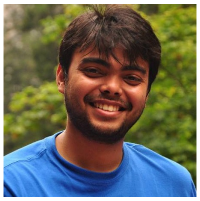
M.Sc. from the Electrical and Computer Engineering Department at the University of Arizona. He joined the Autonomic Computing Lab at the University of Arizona in January 2013 after he started his Masters in August 2012. As a part of his research he was involved in “Anomaly Based Detection of Attacks on DNP3 Protocol”. He is currently employed by Higgins Lab as a software developer.

Bilal Al Baalbaki

M.Sc. from the Electrical and Computer Engineering Department at the University of Arizona. As an active ACL and CAC member his research focus has been on cybersecurity and autonomic protection systems. Bilal has conducted research on the design and implementation of a ZigBee Autonomic Protection System (DNS-APS) and the Wireless Autonomic Protection System (WAPS). Currently he is working as Software Engineer in Data Analytics department in General Motors.

Hemayamini Kurra

Hemayamini graduated from the Electrical and Computer Engineering Department at the University of Arizona with Masters in computer engineering in May 2014 under the supervision of Dr. Salim Hariri. She joined the Autonomic Computing Lab at the University of Arizona in October 2012 after she started her Masters. As a part of her research she was involved in development of Moving Target Defense(MTD) for cloud security. She is currently technical team lead at IBM in Ohio.



Navin Chaganti

Navin graduated from the Electrical and Computer Engineering Department at the University of Arizona with Masters in computer engineering in May 2015 under the supervision of Dr. Salim Hariri. As a part of his research he was involved in "Hacker Web", which is focused on the behavior and motivations for hackers. He is currently employed by KPMG in New York City as a big data senior software engineer.

Nishant Prakash

Nishant graduated from the Electrical and Computer Engineering Department at the University of Arizona with Masters in computer engineering in May 2015 . As a part of his research he was involved in "Autonomous monitoring of human behavior to detect malicious internal users", which involved monitoring of different computers to identify the cyber-DNA of each of the users and hence prevent unauthorized machine usage. He is currently employed by Hewlett-Packard in Sacramento, California.

Shrivatsa Upadhye

Shrivatsa graduated from the Electrical and Computer Engineering Department at the University of Arizona with Masters in computer engineering in May 2015. As a part of his research he was involved in the initial development of Cybersecurity Lab as a service (CLAAS) now hosted on www.lab.askcypert.com. Currently he is employed by Netapp in California and is responsible for automation and orchestration in the VMware and NetApp ecosystem, with a focus on VMware PowerCLI.

Avinash Gudagi

Avinash graduated from the Electrical and Computer Engineering Department at the University of Arizona with Masters in computer engineering in May 2015. He joined the Autonomic Computing Lab at the University of Arizona in August 2013. As a part of his research he was involved in the quantification of the resilience of "cloud" in a Moving Target Defense Environment. Currently he is employed by Intel in Hillsboro Oregon, as a software developer in the Software and services group.

Alumni Corner

Youssif Al-Nashif

Year of Graduation: Ph.D., 2008

Affiliation: Florida Polytechnic University, Associate Professor

Contact: yalnashif@flpoly.org

Huoping Chen

Year of Graduation: Ph.D., 2008

Affiliation: Microsoft/Research Software Design Engineer

Contact:

huoping.chen@microsoft.com

Ishtiaq Hossain

Year of Graduation: M.S., 2010

Affiliation: Telenav

Contact:

ishtiag.jishan@gmail.com

Jang-Geun Ki

Visiting Scholar: 2002 & 2010

Affiliation: Konglu National

University, South Korea

Contact: kjg@kongju.ac.kr

Fahd Rasul

Year of Graduation: M.S., 2005

Affiliation: MBA 2010-2011, Cranfield School of Management

Contact: fahdrasul@gmail.com

Traian Avram

Year of Graduation: M.S., 2006

Affiliation: EXL Service ROMANIA

Contact:

traian.avram@exlservice.com

Mohamed Djunaedi

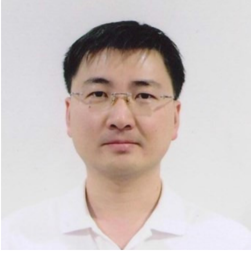
Year of Graduation: M.S., 2001

Affiliation: EMC Corporation

Contact:

djunaedi_muhamad@emc.com

Byoung Uk Kim



Year of Graduation: Ph.D., 2008

Affiliation: Senior Research Engineer, Ridgetop Group, Inc

Contact:

kimbu0219@gmail.com

Subhra Saha

Year of Graduation: M.S., 2003

Affiliation: Adtran Inc

Contact:

subhrasaha@gmail.com

Weiming Wang

Visiting Scholar: 2001-2002

Affiliation: Dean, Zhejiang Gongshang University

Contact:

wmwang@mail.zjgsu.edu.cn

Alumni Corner

Dong xiangdong

Visiting Scholar: 2001-2002

Affiliation: Beijing, China

Contact:

dongnansheng@hotmail.com

Yan Wang

Year of Graduation: M.S., 2006

Affiliation: Qualcom

Contact:

yanw@qualcomm.com

Mohamed Tabris

Year of Graduation: M.S., 2010

Affiliation: Test Engineer, Texas Instru- ments, Tucson

Contact:

mohamedf@email.arizona.ed

Ram P Viswanathan

Year of Graduation: M.S., 2009

Affiliation: Software Engineer at Qualcomm

Contact: www.linkedin.com/in/rampv

Samer Fayssal

Year of Graduation: Ph.D., 2008

Affiliation: World Avenue Inc., Florida

Contact: samerfayssal@gmail.com

Warren Zhang

Year of Graduation: Ph.D, 2007

Affiliation: Google

Contact:

webinfinite@gmail.com

Don P Cox

Year of Graduation: Ph.D., 2011

Affiliation: Raytheon

Contact:

dcox@email.arizona.edu

Sankaranarayanan Veeramoni Mythili

Year of Graduation: M.S., 2009

Affiliation: University of Arizona, CS, PhD student

Contact:

sankar@email.arizona.edu

Guangzhi Qu

Year of Graduation: Ph.D., 2005

Affiliation: Associate Professor, Department of Computer Science and Engineering, Oakland University

Contact: gqu@oakland.edu

Tushneem Dharmagadda

Year of Graduation: M.S., 2003

Affiliation: Sr. Intellectual Property Design and Software Applications Engineer, Analog Devices Inc.

Contact: tushneem@gmail.com

Alumni Corner

Samer Fayssal

Year of Graduation: Ph.D., 2008

Affiliation: World Avenue Inc., Florida

Contact: samerfayssal@gmail.com

Sridhar H

Year of Graduation: M.S., 2001

Affiliation: Sr. Engr. at Silicon Labs, Austin, TX

Contact: sridhar_125@hotmail.com

Aarthi Arun Kumar

Year of Graduation: M.S., 2007

Affiliation: Program Manager, Microsoft Corp

Contact: aarthi28@gmail.com

Prasad Nellipudi

Year of Graduation: M.S., 2000

Affiliation: Technical Marketing Engineer, CISCO

Contact: prasnell@yahoo.com

Prasad Vadlamani

Year of Graduation: M.S., 2004

Affiliation: Texas Medicaid, Data/BI Architect

Contact : prasadvadlamani@yahoo.com

Richard Wang

Visiting Scholar: 1998-2002

Affiliation: ITPOINTS

Contact: wangwei@nj.gov.cn

George Zantis

Year of Graduation: M.S., 2007

Affiliation: Network Security Engineer

Contact: gczenator@gmail.com

Tushneem Dharmagadda

Year of Graduation: M.S., 2003

Affiliation: Sr. Intellectual Property Design and Software Applications Engineer, Analog Devices Inc.

Contact: tushneem@gmail.com

Bihika Khargharia

Year of Graduation: Ph.D., 2008

Affiliation: CISCO

Contact : bkhargha@cisco.com

Kiran Kumar Modukuri

Year of Graduation: M.S., 2006

Affiliation: NetApp Inc.

Contact: kiran.modukuri@gmail.com

Samantha Quadros

Year of Graduation: M.S., 2001

Affiliation: NetFlix, Sr. Software Engineer

Contact : samquadros@yahoo.com

Radhakrishnan Vijay

Year of Graduation: M.S., 2002

Affiliation: Nokia Siemens Networks, Development Manager

Contact: vijayr13@yahoo.com

Jingmei Yang

Year of Graduation: M.S., 2006

Affiliation: Care Everywhere

Contact: jmyanglei@gmail.com

Yaser Jararweh,

Year of Graduation: Ph.D., 2010

Affiliation: Computer Science Department, Jordan Univ. of Science and Technology

Contact: yaser.amd@gmail.com

Alumni Corner

Glynis Dsouza

Year of Graduation: M.S., 2012.

Affiliation: IBM, Tucson.

Contact: glynisdsouza@gmail.com

Venkata Krishna Nimmagadda

Year of Graduation: M.S., 2011

Affiliation: Firmware Engineer at Intel Corporation, Hillsboro, Oregon.

Contact: vkn@email.arizona.edu

Sri Harsha

Year of Graduation: M.S., 2010

Affiliation: University of Arizona

Contact: sriharsh@email.arizona.edu

Yeliang Zhang

Year of Graduation: Ph.D., 2007

Affiliation: Software Engineer, Yahoo.

Hamid Reza Alipour

Year of Graduation: Ph.D., 2012

Affiliation: Software Developer, Mi- crosoft, Seattle.

Contact: hra@email.arizona.edu

Haoting Luo

Year of Graduation: M.S., 2011

Affiliation: Design Engineer at Marvell Semiconductor.

Contact: hluo@email.arizona.edu

Srividhya Subramanian

Year of Graduation: M.S., 2007

Affiliation: UMG Firmware Development Engineer, Intel Corp.

Srinivas Singavarapu

Year of Graduation: M.S., 2003 Affiliation: Sr. MTS at VMware

Contact: www.linkedin.com/pub/srinivas- singavarapu/2/6ba/505

The University of Florida, the University of Arizona and Rutgers, the State University of New Jersey, have established a national research center for autonomic computing (CAC). This center is funded through the Industry/University Cooperative Research Center program of the National Science Foundation, CAC members from industry and government, and university matching funds.

Benefits of NSF CAC Membership

CAC members will have access to leading-edge developments in autonomic computing and to knowledge accumulated by academic researchers and other industry partners. New members will join a growing list of founding members that currently includes BAE Systems, EWA Government Systems, IBM, Intel, Merrill-Lynch, Microsoft, Northrop-Grumman, NEC, Raytheon, Xerox, Avirtec, Imaginestics, and ISCA Technologies. Benefits of membership include:

- ◊ Collaboration with faculty, graduate students, post-doctoral researchers and other center partners;
- ◊ Choice of project topics to be funded by members' own contributions;
- ◊ Formal periodic project reviews along with continuous informal interaction and timely access to reports, papers and intellectual property generated by the center.
- ◊ Access to unique world-class equipment, facilities, and other CAC infrastructure;
- ◊ Internships and recruitment opportunities among excellent graduate students.
- ◊ Leveraging of investments, projects and activities by all CAC members.
- ◊ Spin-off initiatives leading to new partnerships, customers or teaming for competitive proposals to funded programs

Funding

Per NSF guidelines, industry and government contributions in the form of annual CAC memberships ($35K/year per regular membership), coupled with baseline funds from NSF and university matching funds, directly support the Center's expenses for personnel, equipment, travel, and supplies. Memberships provide funds to support the Center's graduate students on a one-to-one basis, and thus the size of the annual membership fee is directly proportional to the cost of supporting one graduate student, while NSF and university funds support various other costs of operation. Multiple annual memberships may be contributed by any organization wishing to support multiple students and/or projects. The initial operating budget for CAC is projected to be approximately $1.5M/year, including NSF and universities contributions, in an academic environment that is very cost effective. Thus, a single regular membership is an exceptional value. It represents less than 3% of the projected annual budget of the Center yet reaps the full benefit of Center activities, a research program that could be significantly more expensive in an industry or government facility.

To Become a Member Contact us at

Director: Salim Hariri (520) 621-4378 (hariri@ece.arizona.edu)
Research Director: Cihan Tunc (cihantunc@email.arizona.edu)
ECE Dept. 1230 E. Speedway Tucson, AZ 85721-0104
http://nsfcac.arizona.edu

Universities

The University of Arizona

Texas Tech University

Mississippi State University

University of Detroit Mercy