SAND2015-6163C

University Days

Poster Session Abstracts 2015

Sand #: 2015-???

CASA
Center for Analysis Systems & Applications

Kai Anderson (DSU)

SAR Performance Monitoring and Visualization

SAR (Synthetic Aperture Radar) is a complex sensor and imaging system. The SAR system has a deep pipeline of a data processing that can be constrained by performance. The flexibility of image analysis algorithms, SAR configurations, and image resolutions is one of SAR's strengths in radar imaging. Monitoring the performance under all conditions and configurations is a necessity when optimizing the system and reporting performance. Using debugging logs and system monitoring tools performance data can be accessed and visualized in a meaningful ways that can be adapted to the needs of development teams.

Patrick Sullivan (MS&T), Emily Armstrong (MIT), Nathan Lin (Univ. of Arizona), Carson Stelzer (Univ. of Arizona), Forest Danford (Univ. of Arizona), Katherine Fackrell (Univ. of Arizona), Uen-Tao Wang (UCLA), & Andrew Wong (UCLA)

Big Data Analytics, Services, and Visualization

The Big Data Analytics, Services, and Visualization project contains several complementary modules in development that add broad improvements over the existing space-focused mission of CASA.

Big data such as TARDIS (Two Line Element database) and the Tycho-2 (star database) catalog offer immense amounts of data without reasonable method of access. CASL is a project for organizing these catalogs into ElasticSearch databases that can be quickly queried and easily maintained. WEASEL is an in-browser visualization tool for viewing satellite flight paths using the STARGATE astrodynamics TLE data propagation library. A modern Scala implementation of WEASEL using the Play framework will expose the STARGATE data as a web service and API to other projects.

To provide a unique data source for this project, the SOHBRIT software uses an automated telescope system to collect images of satellites and track their orbits. A web interface, database, and data pipeline were designed to extract information from the telescope images and allow users to access and query that information. Additionally, SELFIE is an automated image processing pipeline that implements custom satellite streak detection, segmentation, and endpoint identification algorithms. The end result of the pipeline is the RADEC coordinates for the satellite streak end points.

To enable all the pieces of this project to be quickly put together, the team leveraged SkyPunch, a full implementation of OpenStack which provides for rapid deployment, scaling, and clustering of anything from rapid prototyping projects to massive scaling of extant systems. The majority of the applications developed under this summer intern project were stood up on virtual machines on Skypunch.

Elizabeth Lee

Comparing Circuit Topologies using an Abstract Data Model

Netlists, circuit modeling files are unique to each simulator. In some software, if a circuit component is added, changed, or removed, custom names may be reverted to default values. For this reason, an abstract data model may be used to read in two netlists and compare the topologies of these circuits to determine if they differ in name only. This ability to compare circuit topologies will reduce engineering rework involving translating circuit models from commercial tools such as Cadence OrCAD into the Sandia modeling tool, Xyce. The comparison algorithm involves creating strings of circuit components, generating fuzzy hashes to compare the strings, and reducing a matrix of fuzzy hashes using the Hungarian algorithm. Future work on this project will involve modifying the algorithm in order to accommodate more complex circuit topologies and reduce the processing time.

CCD
Center for Cyber Defenders

Julie Calandro (Missouri S&T) & Wesley Folz (Univ. of Arizona)

Ad Hoc Mobile

The most common routing protocols for Mobile Ad Hoc Networks, such as Dynamic Source Routing and Ad Hoc On-Demand Distance Vector Routing, perform poorly in large-scale networks with variable connectivity. The Efficient Spreading with Backtracking Protocol (ESPB) was developed to solve these problems by using a geographic/geometric routing approach, which improves routing performance in densely-populated regions.

Nick Hilbert (Missouri S&T)

Firewheel

Emulytics^{TM} is the combination of emulation and analytics and is a way to emulate a real system through virtualization. Sandia National Laboratories has been furthering the development of Emulytics^{TM} recently and has created two distinct research tools: Firewheel and Minimega. Each has its own advantages: Firewheel has automated topology and experiment generation and Minimega has a nice GUI and easy-to-use controls. My project is to combine both these tools so that the benefits of each tool can be leveraged and so that customers previously familiar with only one of these tools can expand their capabilities by utilizing the features of the other tool.

Wesley Folz (Univ. of Arizona)

MACCS Animations

Scientists require software tools to help them visualize and assess the impact of radiological events and disasters. MELCOR Accident Consequence Code System (MACCS) Animations will assist scientists who are analyzing the safety and potential risks from operating a facility and planning responses to radiological incidents.

John Jacobellis (Carnegie Mellon)

Weaselboard

The Weaselboard is an embedded Debian computer that will monitor Programmable Logic Controller (PLC) traffic across the PCL backplane. Before the Weaselboard can be deployed, the Debian installation must be secured. I used a Security Technical Implementation Guide (STIG) to create a script which will run on the Weaselboard and secure the Debian installation. The script automates the application of almost 300 STIG rules. The STIG I used was for Red Had Linux, because there is no Debian STIG. This means I had to analyze the STIG rules to adapt them to Debian Linux. The finished script will save time because the Weaselboards will no longer have to be manually secured, and they will be able to be safely deployed to the field.

Nathan Burow (Purdue University)

Kodak: Snapshots for Distribution Systems

As distributed systems become larger, more prevalent, and more complicated, it has become impractical to study them by hand in an ad hoc manner. Kodak aims to solve this by providing an automated distributed system analysis platform. It provides a novel snapshot primitive that preserves network packets and other I/O, while scaling to thousands of nodes. Analysts can use the snapshot feature to fork the system and examine its behavior under different scenarios.

Raewyn Duvall (Tufts University)

Flush and Reload: an L3 Cache Timing Attack

This project was an implementation of Yarom and Falkner's "FLUSH+RELOAD: a High Resolution, Low Noise, L3 Cache Side-Channel Attack" to review the security risks in GnuPG RSA encryption/decryption. We used C and inline x86-64 Assembly to time access to memory during decryption and we were able to obtain the secret key by observing which functions were called. Though this topic is out of date, it works as a jumping off point to find and fix other cache side-channel attacks that could be exploited.

Tyler Morris (Emery Riddle)

ThunderBird Cup 2015

The purpose of this project is to help develop the needed skills and talents for NNSA's technical workforce, and to enhance education and research at minority serving institutions. Our approach is to educate minority students via the ThunderBird Cup, a cyber-security awareness exercise created by Sandia National Laboratories. The program uses hands on training and competition to engage students in the exciting field of cyber security in the hope of leading them to further their education in STEM related fields. This benefits the community by diversifying the pipeline to fields like STEM and gives teachers the materials required to educate the students on the topic.

Alex Mitsdarfer (Univ. of Illinois) & Allen Webb (Texas A&M Univ.)

Determining Wireless Perf. Of Mobile Devices for Ad Hoc Networking

Typically networks rely heavily on permanent infrastructure or only operate over limited areas. In emergency situations infrastructure may be inoperable. We investigate a possible alternative which enables emergency communication without relying on static infrastructure.

Jacek Skryzalin (Stanford University)

Analyzing Distributed Word Representations

The GloVe algorithm, which assigns a low-dimensional vector to each word encountered in a large corpus, has recently enjoyed much success in the natural language processing community. However, in its raw form, GloVe is hindered by polysemy and homonymy. We attempt to address these shortcomings by training GloVe on various communities of Wikipedia extracted via the Louvain Method.

Michael Schena (Utah State Univ.)

Blind Source

In order to perform blind signal characterization, the signal should first be isolated in frequency and time. To accomplish this task, this project aims to detect and isolate signals from a full band input stream using an embedded software defined radio. To achieve this goal, signal processing functions that have been implemented in Matlab were written in C++ to be compatible with the embedded system. Then to ensure correctness, the C++ functions were verified against the original functions using Matlab Executable (MEX) files.

Jeffrey Bigg (Univ. of Illinois) & Scott Watson (Florida State Univ.)

LinkShop – Automated Linkograph Creation and Analysis Tool

This project creates linkographs, temporal graphs which help to understand the behavioral structure of security event data. We create these linkographs in an automated fashion through an intuitive, interactive web interface that allows on-the-fly editing of the parameters necessary for linkograph creation and interpretation. It is our goal to use this interface to expedite the ability to create linkographs and discover their properties.

Kelly Luk Bounsawat (Texas A&M Univ.) & Allison Campbell (Southern Illinois Univ.), & Andrew Chu (Albuquerque Academy High School)

ICS-CERT Visualization Panel

Network attacks are ever present, and ill-prepared entities risk serious damage to critical infrastructure. Often times, network administrators and monitors are not prepared to handle malicious activity on complex control systems. Our team modifies Kibana source code to add a custom network connection visualization panel to be integrated with Elasticsearch, Logstash, and Bro. It will be used with Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team's (ICS-CERT) Supervisory Control and Data Acquisition (SCADA) system. This interactive, visual tool will allow the team to more effectively monitor critical infrastructure.

Lance Chao (Virginia Tech), Rain Dartt (Rose-Hulman Institute of Technology), Russell Van Dam (New Mexico Tech)

Emulating Network Isolation Zones

The concept of Isolation Zones in network security has been deemed valid, but testing the concept on a large, topologically complex network is currently not practical. By using Minimega to create an arbitrarily sized network of virtual machines with varying topologies, we make testing Isolation Zones on a large scale feasible.

Jeffrey Bigg (Univ. of Illinois) & Anthony Dust (Univ. of Illinois)

Network Host Discovery (NetHD)

Red Team personnel utilize several reconnaissance tools to map the topology of a target network. NetHD aims to tie together available network tools in a modular way, gather their output, and merge their output together into a common, exportable data format. NetHD is written in Python and requires little additional knowledge to extend its functionality.

Corey Miner (Univ. of Arizona)

Neuromorphic Computing

Standard neural networks have historically been challenging to implement with learning hardware because they learn through backpropagation. Adaptive Resonance Theory (ART) networks learn without back propagation and are easily implemented with hardware. We are creating a deep convolutional neural network that uses ART to learn the image template features instead of backpropagation. This new neural network architecture will improve the capability of neural networks working with hardware and will recognize a wider range of features which will result in improved categorization.

Marcus Dominguez-Kuhne (Albuquerque Academy) & Alex Mitsdarfer (Univ. of Illinois)

PEDs Alert

Portable Electronic Devices (PEDs) must comply with rules of use in restricted access areas. Of concern are radio frequency (RF) transmitters, such as Wi-Fi and Bluetooth. Our goal was to create an Android application that acts as a fail-safe in case a device is brought into a restricted area.

Zachary Thomas (Mississippi State Univ.) & Scott Watson (Florida State Univ.)

Analyzing with Oxide: Matching Architectures

Oxide is a modular malware analysis tool heavily focused on industrial control system firmware. Because of the great variation in potential architectures running on industrial control systems, it is not often apparent which architecture a particular piece of malware is targeting. The focus of the project is to design and implement a process for determining the target architecture of a raw binary blob. After identification of the malware's target architecture, specialized tools can be utilized to mitigate the malware's impact on an industrial control system.

Kais Kudrolli (Carnegie Mellon Univ.) & Emily Donahue (Cornell Univ.)

Sasquatch

Our project addresses the demand for computer vision applications on a variety of devices and architectures. Such applications benefit from device-agnostic frameworks that make it easy to train and use neural networks and utilize parallel-processing hardware such as graphics processing units (GPUs). Thus, our objective is to port the existing open-source implementation of the Caffe deep learning framework from CUDA to OpenCL. Our approach is divided into porting, testing, optimization, and deployment phases. The finished product can run on OpenCL-supported GPUs to speed up neural network training on many different architectures.

Lance Chao (Virginia Polytechnic Institute), Khiem Tang (Univ. of Texas Austin), & Marcus Dominguez (Albuquerque Academy High School)

THEARTICLES: TrafficSoup

Network security research typically involves a Red team, a Blue team, and a test network. For cost-efficiency purposes, these test networks often are virtual network simulations rather than physical ones. Unfortunately, using a virtual network makes it trivial for the Blue team to notice activities because there is no traffic inside of a test network. The goal of Traffic Soup is to make the network simulation more realistic for both the Red and Blue teams by providing real traffic data.

Andrew Chu (Albuquerque Academy High School)

TracerFIRE 6: Game Description Editor

This project originated from the need to quickly and effectively adjust flow of progression in the TracerFIRE challenges through editing of a state/transition game description JSON file. Previous construction of such file was only possible through hard-coding previously existing skeleton values, resulting in a repetitive and tedious process of creation. As an answer to this task, an interactive, visual "drag and drop" JSON builder was made utilizing jqTree, a jQuery widget for displaying a tree structure in HTML. At a finished state, this editor aims to aid the TracerFIRE team in educating individuals and groups about possible real life cyber threats, as well as the steps necessary to detect, counter, and prevent future breaches.

Justin Cox (Utah State Univ.), Rain Dartt (Rose-Hulman Institute of Technology), & John McCloud (NM Institute of Mining & Technology)

Technology Testing with Emulytics

Many technologies are built to deal with the ever-changing needs of digital security; however, they must be tested for performance and efficacy in several environments. Such testing is done as part of the Transition to Practice (TTP) Project. In our testing suite, we employed Emulytics™ to simulate large networks with multiple environments. This allows us confirm performance claims of technology providers, while ensuring issues in these technologies do not affect live systems. These technologies, after review, will be used to help mitigate security risks.

Allen T. Webb (Texas A&M Univ.) & Johahn Wu (Univ. of Texas)

Verifying the Usefulness of Experimental Data from Virtual Test Beds

Emulation-based models are useful tools for understanding complex systems. However, unlike more model rich domains, cyber science is lacking in established Verification and Validation (V&V) techniques. In order to determine if conducting experiments in virtual experiments answer questions of interest for real environments, we created an end-to-end V&V system to help determine the accuracy of cyber emulation systems.

John Jacobellis (Carnegie Mellon Univ.)

Hardware Analysis Infrastructure Improvements

Current lab tools don’t have the precision or high resolution needed for the sensitive hardware analysis being performed. The lab has acquired new high-precision Lecroy oscilloscopes that can collect the needed measurements, but they have not been integrated into the lab infrastructure. These scopes needed to be integrated into the lab infrastructure so that a user can acquire data from the oscilloscopes onto a desktop computer. This involves developing a Python interface for the oscilloscopes’ API. The Python interface will be integrated into existing code bases.