Net-Centric & Cloud Software & Systems I/UCRC

Semi-Annual Highlights of Industry/Academic Cooperative Research Projects

http://netcentric.unt.edu

Issue 4, February 2016

In this issue

Understanding Security Service Level Agreements

Information security risk assessment has enormous relevance to the mitigation of large-scale attacks on data such as those reported over the past two years by Target, Home Depot, JP Morgan Chase, and others. These attacks have resulted in over 600 breaches that have exposed more than 78 million personal records. In early 2015, health insurance provider Anthem Inc. said hackers had breached its computer system and the personal information of as many as 80 million customers and employees was potentially placed at risk.

Reports of cybersecurity attacks, lapses in auditing security of public and private Cloud-based systems, and discovery of new vulnerabilities of IT systems are becoming more common. Mitigation of risks associated with data security breaches is recognized as critical to national security. In a January 2015 speech at the Federal Trade Commission, US President Obama outlined proposals aimed at improving student data protection and protecting Americans' financial health.

Engineers at UNT have developed ontologies for reported security vulnerabilities of hardware and software systems and reported cyber-attacks on IT systems. The system is extensible to include newly discovered vulnerabilities, suspected attacks, or any other information that is relevant to the security of IT systems reported in Security Information and Event Management (SIEM) documents. Using the system, called Nemesis, it is possible to quantify security threat levels faced by IT systems. The system can also recommend alternate IT systems and proper configuration of software to mitigate threat levels, or approaches such as software rejuvenation to sweep hidden and unknown malware from a system.

Combining a Security SLA and vulnerability, Ontologies can be used to both negotiate and monitor the levels of security provided by Cloud and other IT systems. It also allows one to quantify security risk levels as well as define the degree of compliance with regulations. For example, HIPAA only states that any transmitted information that contains patient Protected Health Information (PHI) should be encrypted, but says nothing about the quality of encryption used. Nemesis can use quantitative measures with different encryption techniques so that the strength of compliance can be measured and used by clients to evaluate and select a service provider with the strongest security SLA. ■

Advances in Feature Extraction Directly from Compressed Imagery

Compressive sensing of multi-dimensional image data offers advantages in terms of lower cost and lower data rate acquisition, especially in the infrared wavelengths. In the past, work in this area has focused on reconstruction algorithms, with little focus on development of techniques for higher-level tasks such as target detection and tracking.

Traditional target detection and tracking algorithms focus on analysis in the image domain. In the past year, researchers at ASU have made significant progress in bridging this gap. Researchers have developed foundational tools based on optical flow and smashed filtering that enable effective algorithms for detection and tracking, while working directly on the *compressed* measurements. This approach avoids the computationally costly signal reconstruction process.

Research results indicate that one can estimate optical-flow as well as estimate correlational features for target detection. By integrating these correlational features in a track-before-detect based system, one can successfully track simple targets without performing compressive sensing reconstruction.

To date, ASU has developed a compressive sensing framework enabling direct feature extraction. Single-frame and multi-frame reconstruction algorithms have been implemented and alternate reconstruction methods, involving difference frames and robust PCA, have also been implemented and evaluated. New algorithms for feature detection and extraction show encouraging early results for deep network based feature extraction and classification. ■

The 2015 Paper Award was awarded to Ph.D. student, Bob Santucci, and faculty advisor, Andreas Spanias, at the ASU NCSS Site. The award is for a paper associated with digital pre-distortion algorithms for energy-efficient but non-linear class AB RF Amplifiers.

The paper describes the development of advanced algorithms and software to implement realistic RF amplifier models. Several software implementations are described including those that enable advanced simulations for research and education purposes. Current related research at the ASU site which may be of potential interest to NCSS members includes distributed estimation in the presence of amplifier compression resulting from the energy-efficient but non-linear class AB operation. The digital pre-distortion scheme is utilized to fit the amplifier at each sensor to a mathematically tractable, soft compression function that roughly mimics the compression region of the amplifier. The approach has benefits over linear amplifier operation including improved transmitter efficiency and reduced sensitivity to heavy-tailed distributions. ■

Ransomware on the Rise

Ransomware is a type of malicious software that prevents a user's PC from being accessed until a ransom payment is made to the malware author. If the ransom is paid, the author may (or may not) remove the infection. Although ransomware has been observed in the wild since 2005, it has become more pervasive over the last three years as reported by Symantec in their *2015 Internet Security Threat Report (ISTR20)**.

Ransomware attacks are generally delivered during a drive-by visit to an infected web page or via a browser exploit. The malware takes one of two forms, encrypted or non-encrypted, with the former rendering a user's files undecipherable until the ransom fee is paid, after which a decryption key is provided to unlock the user's files, although this would be at the whim of the malware author. The ransom fee is often several hundred dollars and payable via wire transfer, online payment voucher service, bitcoins, or other methods. Some ransomware implementations may present the user with an intimidating splash screen giving the illusion that the FBI or other law enforcement agency is the source of the ransom demand. Some variants can even take control of the PC's webcam to get a picture of the user and superimpose it on the splash screen to add an additional scare factor. ■

*Reference: http://www.symantec.com/security_response/publications/threatreport.jsp

Using GPS to Control Ground Based Mobile IoT Devices

The Internet of Things (IoT) consists of a number of distributed physical objects with embedded devices such as RFID chips that permit the objects to interact with the environment and other embedded devices. IoT greatly increases the potential for significantly enhancing the operation of underlying systems, including incorporation of more automation, coordination of various entities to minimize operational costs, and increasing the possibility of proactive dependability assurance, etc.

These advantages are leading the way for development of innovative systems for many important applications. One challenge for several of these emerging classes of IoT applications is that they involve different types of mobile devices that need to navigate from one place to another to perform their tasks. Examples include smart agriculture systems, smart vehicle systems, and smart systems that monitor large-scale infrastructure elements such as bridges, buildings, tunnels, etc.

To ensure the safety and dependability of these systems, it is essential that all the mobile devices are able to move safely in a region of interest, avoid collisions with other objects in the environment, and coordinate their actions to achieve highly efficient and dependable operations.

To meet these safety-critical navigation objectives, researchers at UTD are developing an accurate positioning method using IR thermal imagers, ultrasound sensors, and other mechanisms on ground-based units to improve navigation accuracy. The system is further enhanced with autonomous learning and adaptation, and the use of commercial aerial drones to provide more precise positioning information to safely navigate mobile IoT units on the ground.

To achieve this capability, researchers propose to enhance GPS systems by using various IR imagers and ultrasound sensors to gather more accurate location information in real-time. Cloud computing resources are also leveraged to calculate the precise position and optimal trajectory of each ground unit to guarantee that each unit safely reaches its goal position without incident. This includes ensuring that the motion of each unit does not lead to collisions with other mobile units or with any stationary objects in the environment.

To date, this project has enabled the development of a Virtual Receptionist System (VRS) and a case study system based on one design of a Smart Home for Energy Conservation. The research team has also developed prototype robotic devices for Smart Agriculture applications and a preliminary version of a real-time intelligent control and power management system using cloud computing resources. Basic communication and control capabilities have been implemented for IoT systems including Bluetooth, Wifi, DC motors, BLDC motors, servos, and other sensors supported in REKAM1 (an open source virtual machine supporting rapid implementation of wireless connections). ■

Predicting Hidden Vulnerabilities in Cloud Systems

A recent article in Trend Micro on ”Zero Day Vulnerabilities 101” introduces the notion of a Zero Day vulnerability as a hidden flaw in a given IT product that leaves developers and users in the dark while attackers can find ways to exploit it for malicious intents. Since the OpenSSL Heartbleed vulnerability was disclosed in 2014, public awareness of zero day vulnerabilities has increased. Zero Day vulnerabilities raise a critical security question regarding how we can approach the problem of anticipating the presence of hidden vulnerabilities in any given IT Product.

UNT researchers have demonstrated a method for generating a dataset that represents product maturity in terms of base source code growth and vulnerability disclosure history. They have documented how to use such a dataset and have developed models that result in highly accurate predictions. The Azure Cloud-based ML framework is at the center of this model and has been validated for several popular IT products. A few other products are currently producing less accurate predictions, but experimentation will be broadened to extend the number of features to be included in the maturity dataset. Using the predictions on vulnerabilities, researchers estimated security risks associated with IT products and separated the risks due to both known and hidden vulnerabilities. For example, UNT collected details about product releases, the number of versions and the number of vulnerabilities already reported.

Students analyzed the source code for each released product version and computed 100+ software metrics for the code. Each release is identified using a Common Platform Enumeration (CPE) format as its unique identifier in the dataset. For each CPE, an Ontology Knowledge Database framework is used to discover and record all reported or known vulnerabilities for the release. Software source code is analyzed and metrics are stored for each released version. Since the size of the code base for each release can be very large, researchers leverage the capabilities of the SciTools Understand 3.1 tool for code analysis and metrics generation.

The Ontology Knowledge Database framework predicted 32 vulnerabilities for the OpenSSL code base (94 separate releases). The history of reported vulnerabilities for OpenSSL shows a decreasing trend through each minor release in terms of the number of vulnerabilities. The average number of reported vulnerabilities also spiked whenever the rate of minor releases was high following a major release. The newly discovered vulnerability in a current release affects previous releases (thus not discovered until after a new release).

Future work will focus on broadening experimentation and extending the number of IT product features to include in the dataset. Using predictions of vulnerabilities, security risks associated with IT products can be estimated and used as evaluation and selection criteria for choosing a secure cloud service provider. ■

National Science Foundation
WHERE DISCOVERIES BEGIN

NCSS Completes 2nd Year of NSF Supplement for Innovative Managing Director (IMD)

In 2013 the NSF released an RFP to develop a model for an Innovative Managing Director. The model had to be applicable to any I/UCRC and emphasize member recruitment, retention and building a vibrant I/UCRC ecosystem. The model had to be successfully implemented within the RFP respondent's own center.

The NCSS IMD Model, beginning its final year of development in 2016, seeks to define an Organizational Maturity Model (OMM) with Key Process Areas (KPAs) specific to I/UCRC's. This structured model and its component processes enable an I/UCRC to be run like a business. The IMD, site directors, and PI's have a kind of profit-and-loss responsibility. Success is measured by how well their research projects meet cost and schedule goals, deliver the work products they promise, and provide genuine leverage to their sponsors' Internal Research and Development (IR&D).

The need for more business rigor in the management and objective evaluation of I/UCRC performance is frequently mentioned by industry members as a desired area of improvement. To this end, the IMD model proposed by NCSS emphasizes the importance of project management by fact (i.e., using objective performance measures) and standardizing operational processes across the I/UCRC. A process taxonomy of key process areas derives from an introspective evaluation of existing organizational gaps and issues. Gaps come from NSF Evaluator Reports, IAB member surveys, and feedback from Center membership. The NCSS model seeks to define specific practices and guidelines, by role, to close the gaps and establish a repeatable and institutionalized process baseline. This replaces immature ad hoc methods that may exist at member academic sites.

The NCCS model defines KPAs for: project Evaluation, Selection and Management (ESM); Membership Recruiting and Marketing (MRM); and Site Cooperation (SCO). A compensated managing director role eliminates the need for principals of the Center to make pro bono work contributions in addition to the responsibilities they have to full-time employers (the latter being a frequently cited contributor to poor Center integration across sites.)

The NCSS IMD model implementation has so far produced and implemented processes and templates for the ESM and MRM KPAs. The SCO KPA and its component processes are designed to nurture a "one Center" mentality among the university members that results in: multi-university collaborative research projects; consistent use of common processes, methods and tools; broad awareness and support of Center-sponsored projects and initiatives; expanded networking opportunities; and a collective interest in growing the Center to achieve financial self-sustainment. Our current vision for the final version of the SCO KPA is to be deployed during the third and final year of the IMD Supplement. ■

ASU NCSS and Tech de Monterrey Collaboration on Sensor Networks

The ASU SenSIP NCSS Site signed an MOU for research collaboration with IInstituto Tecnológico de Monterrey (ITESM). The collaboration is between the ASU site and the Center for Development of Information Technology Industry in Mexico (CeDITIM) at ITESM.

Proposal development workshop for collaborative research between the ASU NCSS SenSIP site and the ITESM Center for Development of Information Technology Industry in Mexico (CeDITIM). The meeting was at the ASU University club in November 2014.

The collaboration agreement includes:

a) The exchange of visiting students, scholars, faculty and post-doctoral fellows;
b) The exchange of scholarly information including research papers, indices to theses, and books on relevant subjects;
c) The exchange of invitations to attend scholarly and technical meeting, forums and conferences;
d) Joint conferences, seminars, workshops and exhibitions; and
e) Review of other possible areas of cooperation in a variety of research and academic projects. ■

The Agribot - An Autonomous Agricultural Robotic System

Several students involved in the NSF NCSS I/UCRC Internet of Things (IoT) project have developed the first multifunctional agriculture robot system, called the Agribot. In addition to the team leader (Guang Zhou), the team included 2 undergraduate students (Juan Wu, Seungcheul Kim), 2 Plano ISD students (Raja Akula, Anita Dey), and 2 undergraduate students from Mexico (Orlando Barrera, Alejandro Canton). The IoT project is aimed at developing a framework to leverage cloud computing resources to significantly enhance the dependability and quality of critical IoT applications, such as healthcare, smart vehicles, smart homes, infrastructure monitoring, agriculture, supply chain management, etc. The Agribot system is designed to be created with home tools, a couple of microcontrollers, and to be fully controllable using the user's own smartphone!

Pictured from left to right: Orlando Barrera, Raja Akula, Juan Wu, Alejandro Morales Canton, Guang Zhou, (the team leader), and Anita Dey Barsukova.

The students have worked actively with researchers from TI in actually developing, deploying, and evaluating a prototype of this visionary Agribot system. The current version of the system uses a combination of sensors from smartphones and the robot to gather relevant information from the environment, analyze the information, and use the results to provide high quality successful instructions to guide the robot. This includes real-time instructions on where to turn, whether to go forward or backward, etc. All these instructions are designed to meet high assurance requirements to avoid collisions with any obstacles or other robots in the environment. The Agribot is GPS navigated and the user can setup way points in the app. It is compass and gyro stabilized to ensure that the robot operates properly along its designated path and even works indoors. In addition, it has ultra sound sensors mounted to ensure that it will work properly and safely even in tightly confined crop rows. Some information about the current version of the Agribot system is available at the following sites:

- GPS navigation video https://www.youtube.com/watch?v=PUuACgyLhow
- Obstacle avoiding combines with GPS navigation. https://youtu.be/ttheGXg3cYM?t=39
- It can mount different tools https://www.youtube.com/watch?v=tnEv3fy_w7k

Although this robot is currently focused on agriculture, the same principles of the Agribot may be applicable to other areas with the right conditions and with enough work. The students are very inspired by this research and would love to pursue the idea to transform and adapt their technology for other areas. ■

Patrick Kamongi is a computer science and engineering PhD student at the University of North Texas who is being supported by I/UCRC NCSS projects. His research work focuses on cloud computing security. Under his advisor, Dr. Krishna Kavi, he has gained invaluable research experience working on I/UCRC projects. His ongoing work has resulted in several published works.

This past summer, Patrick was offered and completed a competitive internship with the cyber threat intelligence security firm 'iSIGHT Partners'. He worked as a cyber threat researcher intern where his responsibilities included conducting malware research, collecting cyber threat data, and other tasks. Working independently and through collaborations with global researchers, he enjoyed the learning experience and was able to apply proven research techniques in an industry setting.

I/UCRC projects and internship experiences have allowed Patrick to put his ongoing education on a fast track. He has also made valuable professional connections that have opened new opportunities for him in both industry and academia.

Another of Dr. Kavi's PhD students, **Marko Scrbak**, was employed as a co-op/intern at Advanced Micro Devices, Inc. (AMD) from September to December 2015. His research explored use of processing in memory (PIM) and next generation high performance computing to understand how such systems can be optimized to deliver peak performance within a specified power budget. This included expanding the existing simulation infrastructure and collecting data for analysis.

The internship provided Marko with insights into how large companies perform research in areas that are typically explored only within the academic community. He also gained his first professional working experience and acquired skills including formal software engineering practices and new programming languages. The experiences gained during the course of the internship will be valuable to his future career and his doctoral dissertation since it directly involves heterogeneous systems and processing in memory. ■

Recent Publications on NCSS Related Research

M. Scrbak, M. Islam, K. Kavi, N. Jayasena and M. Ignatowski; ***Processing in Memory: Exploring the Design Space***, 28th International Conference on Architecture of Computing Systems (ARCS-2015), March 2015.

C-Y. Lee, K. Kavi, R. Paul; ***Ontology of Secure Service Level Agreement***, 16th IEEE International Symposium on High Assurance Systems Engineering (HASE 2015), January 2015.

P. Kamongi, M. Gomathisankaran, K. Kavi; ***Nemesis: Automated Architecture for Threat Modeling and Risk Assessment for Cloud Computing***; 6th ASE International Conference on Privacy, Security, Risk and Trust (PASSAT-2014).

L. Chung, T. Hill and N. Subramanian; ***Silverlining: A Cloud Forecaster Using Benchmarking and Simulation***, 26th Annual IEEE Software Technology Conference, Long Beach, CA, Mar. 29 - Apr. 3, 2014.

Wei She, I-Ling Yen, and Bhavani Thuraisingham; *Security-**Aware Service Composition with Fine-Grained Information Flow Control***, IEEE Transactions on Services Computing, Vol. 6, No. 3, July-September 2013, pp. 330-343

Upcoming Events

The semi-annual meeting of the NCSS Industrial Advisory Board will be held Wednesday and Thursday, March 2-3, 2016 at the Arizona State University.

For more information about the NCSS I/UCRC or how you can join our center, please contact:

Professor Krishna Kavi
Director of NCSS I/UCRC
Krishna.Kavi@unt.edu

or

Melanie Dewey
940-565-4764
Melanie.Dewey@unt.edu

Current NCSS Membership

University of North Texas (UNT)
University of Texas at Dallas (UTD)
Arizona State University (ASU)
AMD
Armor
Ashum Corp.
Boeing (not active)
Briggs Freeman Sotheby's International Realty
CompuMatrice
Endometric
Freescale
Interactive Flow Studies
Intel
Lockheed Martin Aeronautics
NTT Data
Poundra
Raytheon
Sprint
Texas Instruments