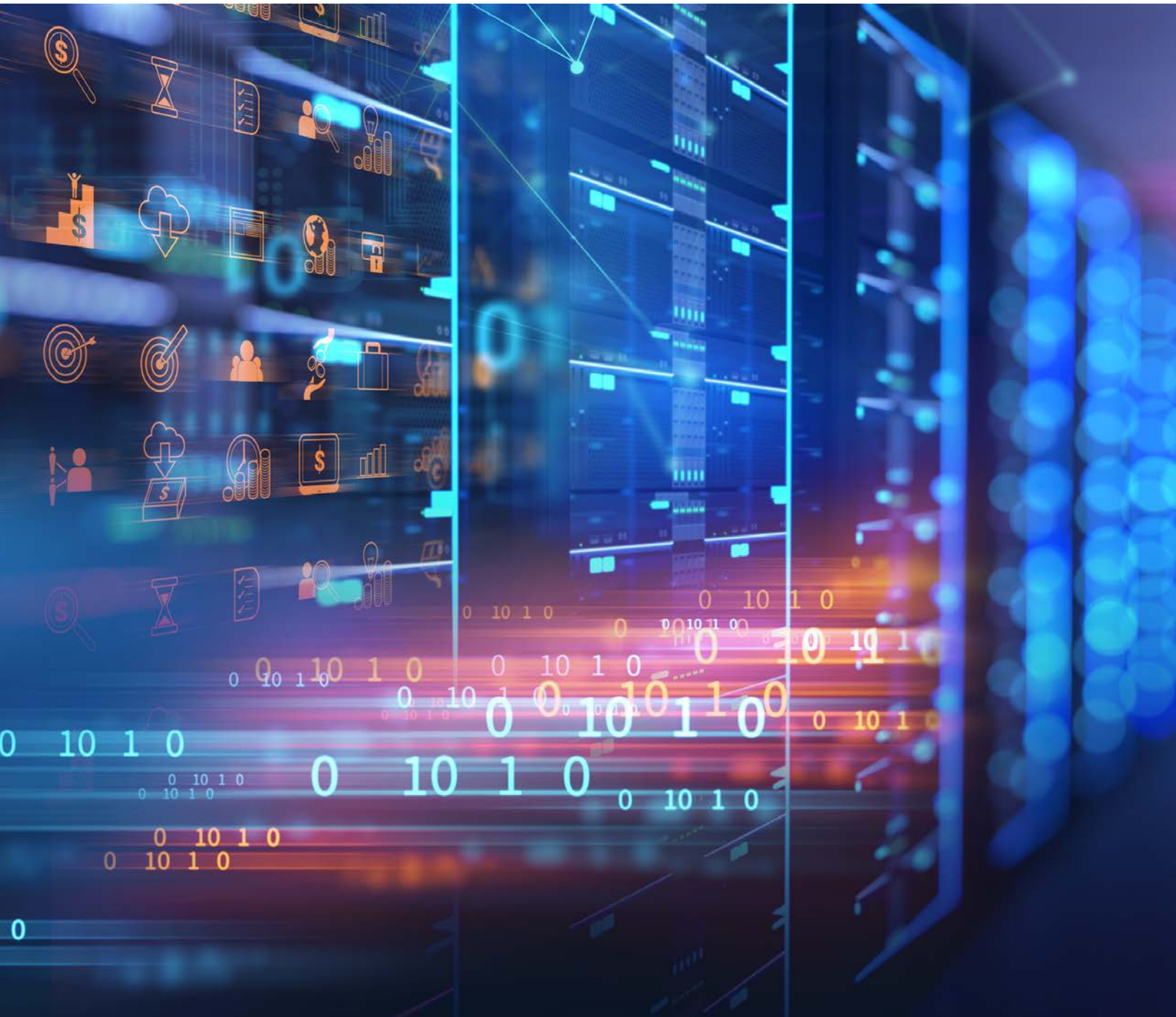
THE UNIVERSITY of TULSA

Tulsa Enterprise for Cyber Innovation, Talent and Entrepreneurship (TECITE)

Cyber District



Tulsa is poised to become the nation's cyber center in research, innovation and entrepreneurship.

Cybersecurity at TU

A leader in cybersecurity research and education for more than 20 years

NATIONAL SECURITY AGENCY CENTERS OF EXCELLENCE

- *Information Assurance and Cyber Defense Education* since 2000; one of the first 14 institutions awarded this distinction
- *Information Assurance Research*
- *Cyber Operations*
- One of the few universities awarded all 3 distinctions

PATENTS

U.S. Patent No. 9,471,789, issued Oct. 18, 2016. Compliance method for a cyber-physical system. Inventors: J. Hale, P. Hawrylak, and M. Papa.

U.S. Patent No. 9,038,155, issued May 19, 2015. Auditable multi-claim security token. Inventors: R. Gamble and R. Baird.

U.S. Patent No. 6,732,180, issued May 4, 2004. A method to inhibit the identification and retrieval of proprietary media via automated search engines utilized in association with computer compatible communications networks. Inventors: J. Hale and G. Manes.

EDUCATIONAL OPPORTUNITIES

- Cyber Corps
  - NSF Scholarship-For-Service and DoD Information Assurance Scholarship Programs
  - More than 350 graduates placed in government positions
- MS in Cybersecurity Professional Track degree offered online along with a traditional residential program
- Undergraduate Exposure in Cybersecurity
  - Substantial curriculum offerings
  - Research engagement through funded support and the Tulsa Undergraduate Research Challenge
  - Minor that attracts undergraduate students from computer science, engineering and business

RESEARCH

- Interdisciplinary research projects funded by AFRL, DHS, DOE, NSF and private industry
  - Wearable and Internet of Things (IoT) Device Security
  - Security Assurance for Autonomous and Self-Adaptive Systems
  - Heavy vehicle cybersecurity research
  - U.S. Critical Infrastructure Protection Research (oil & gas, nuclear, and the power grid)
  - Security Economics Lab
  - Institute for Information Security (iSec)

Tulsa's Cyber District

BUSINESS CONCEPT FOR FOUR CO-LOCATED CYBER CENTERS OF EXCELLENCE

EXECUTIVE SUMMARY – A new war is underway. A war fought among nations, organized terror cells and individual hackers, against our national defense systems. A war against our banking, retail, health and energy business sectors. The sophistication of these attacks continues to advance. Currently 350,000 cyberdefense positions are available in the United States with projections for exponential growth in needed cyberdefense workforce. For many of these cyber positions, the candidates must meet Top Secret Security Clearance level standards. There is a need to expand cyber research, innovation and entrepreneurship to stay well ahead of the "bad guys." There is great need to ensure the quality of cyberservices, vendors and products in supply chains, manufactured products and cyber insurance ratings.

This proposal asks for the creation of a Tulsa Enterprise for Cyber Innovation, Talent and Entrepreneurship (TECITE.) The backbone of this enterprise is a set of co-located cyber centers of excellence that link industry, federal agencies and The University of Tulsa in a united effort in defense of our information systems. The proposal takes advantage of Tulsa's low cost of living, ability to recruit and retain young talent and the near downtown Tulsa Opportunity Zone along 6th Street. The proposal leverages The University of Tulsa's 20-year history as the lead supplier of Top Secret Security Clearance talent to federal agencies and as a national center of excellence in cyberdefense education and research. All of this is an effort to significantly grow additional cyber workforce and innovations in Tulsa.

Specifically, we propose four co-located Centers of Excellence; an Engineering Research Center at The University of Tulsa focused on cybersecurity, a Multi-Federal Agency Cybersecurity Center of Excellence, a Cybersecurity Insurance Institute to gather and analyze data on cyber risks, and a Consortium of Business Sectors in banking, energy, retail, health and transportation focused on cyber defense research and innovation. We propose the co-location of these centers of excellence along the 6th Street Opportunity Zone Corridor, linking downtown Tulsa with The University of Tulsa.

Business concept for a Tulsa cyber district

PROBLEMS TO BE SOLVED.

Our country's military, energy, financial, retail, insurance and health digital information infrastructure face ever-increasing cyber-related attacks from foreign governments, rouge hackers and terrorist organizations with the potential for disastrous impact on the defense of our nation, including our economy. The sophistication of these cyberattacks continues to advance alongside these ever-increasing number of attacks, requiring a robust cyber research and innovation enterprise to stay steps ahead of these attackers.

The quality of cyberprotection services, vendors and products is without a rating system. For example, within the Department of Defense supply chain vendor contracts, a signed attestation of meeting the Defense Federal Acquisition Regulation Supplement (DFARS) cyberstandards is the current state of quality assurance.

There is an inadequate cyber-trained workforce to meet these challenges with an estimate of 350,000 open cyber positions across the United States. One estimate is that by 2021, more than 3,000,000 cyberdefense jobs will be needed. The announcement of Amazon's HQ2 to the Washington, D.C. area will pull existing computer science and cyberworkforce talent from D.C. area federal agencies to higher paying Amazon jobs while driving up housing and living Belt-way costs.

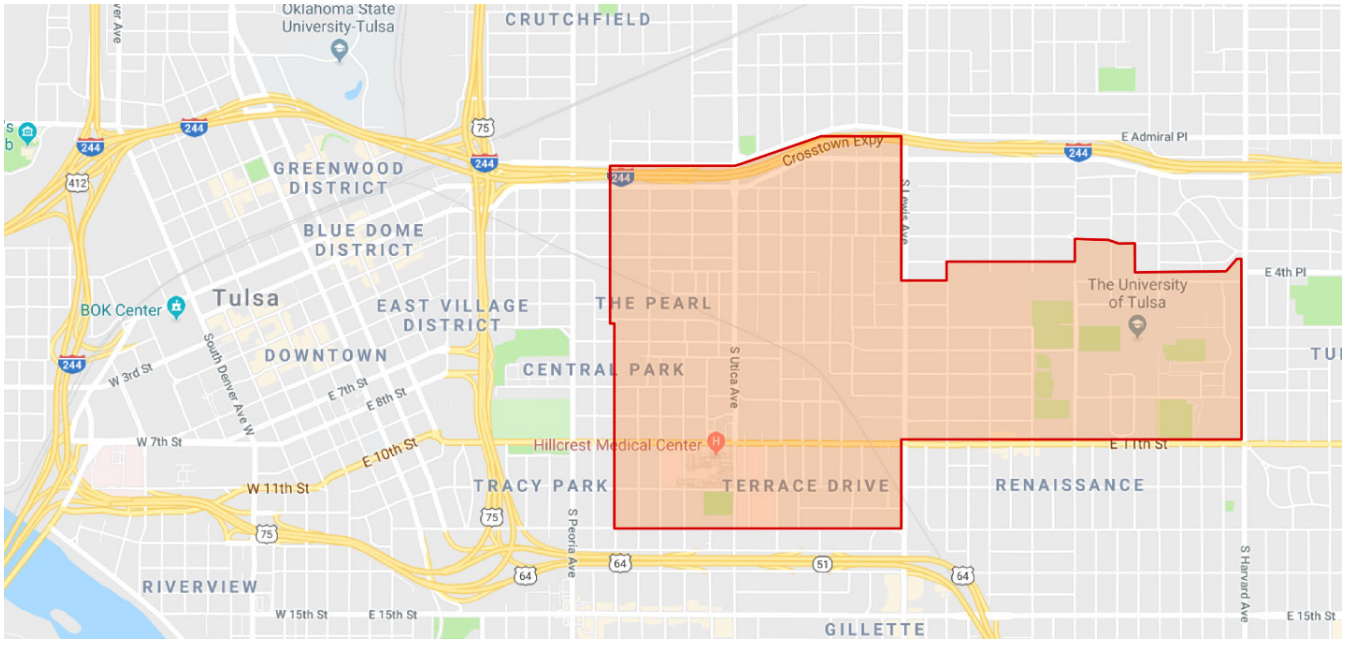
Decision makers at major corporations and public institutions across the United States are not adequately informed in cyber-related issues to protect their companies and institutions.

UNIQUE SOLUTIONS TO THESE PROBLEMS:

The Proposed Tulsa-based Tulsa Enterprise on Cyber Innovation, Talent and Entrepreneurship (TECITE)

The University of Tulsa has a long-standing reputation for excellence in cybersecurity with programs on campus supported by the National Security Administration, the Secret Service, the U.S. Department of Defense, the U.S. Department of Energy, the U.S. Department of Transportation, the Federal Bureau of Investigation and the Defense Advanced Research Project Agency (DARPA).

TULSA'S 6TH STREET CORRIDOR OPPORTUNITY ZONE



With the cyberinformation security needs of our nation dramatically increasing, we propose a bold, Tulsa-based cyber-focused enterprise that brings together industry and federal agencies around cybersecurity centers of excellence and takes advantage of:

- The University of Tulsa's long-standing expertise in cyberdefense.
- The University of Tulsa's proven ability to train a cyberworkforce that secures top secret security clearances. We estimate that The University of Tulsa has trained the greatest number of NSA cyber experts by a factor of 3 over the next leading university. We have sent nearly 350 TU cyber graduates to work in federal agencies.
- Tulsa's available workforce from The University of Tulsa's expanding programs in the digital sciences.
- Tulsa's low cost of living – currently 11% lower cost of living than the national average.
- Tulsa's emerging reputation for young talent recruitment and retention and start ups.
- The inclusion of The University of Tulsa in an Opportunity Zone.

This bold initiative serves to solve the following problems:

- Increase workforce with talent in cybersciences.
- Increase workforce with credentials to achieve top secret security clearance status.
- Increase research and innovations in the cybersciences.
- Create new Tulsa-based startups and scaleups in cyber-related industries.
- Protect existing business sectors with specific cyberprotection programs.

We propose to solve these problems through the creation of Tulsa's Cyber District and a new Tulsa Enterprise on Cyber Innovation, Talent and Entrepreneurship (TECITE). This enterprise, located in the Cyber District, would have seven anchors:

1. **Academic; with The University of Tulsa as an Academic Anchor** – with cyber-affiliated undergraduate, graduate and certificate programs. Includes TU's Computer Sciences, Electrical Engineering, Computer Engineering, Computer Information Systems, Industrial Organizational Psychology, Entrepreneurship, Finance, Data Analytics and Quantitative Finance programs.

2. **Federal Research Support;** with funded programs as an anchor in growing cyber-related research, workforce and entrepreneurship in Tulsa – this includes National Science Foundation (NSF) supported programs such as Engineering Research Center grant support (up to $6,000,000 per year), Small Business Innovation Research (SBIR) grants, Small Business Technology Transfer (STTR) grants and the NSF Innovation Corps (I-Corps) Program.

3. **Federal Agency Support; with a proposed U.S. Government Multi-agency Cyber Center of Excellence in Tulsa as a Federal Anchor** – partnered with The University of Tulsa on Cyber research, defense, and workforce expansion would be several federal agencies such as U.S. Department of Defense, U.S. Department of Homeland Security, U.S. Department of Energy, U.S. Department of Transportation, the U.S. Department of Commerce and their National Institute of Standards and Technology and the Manufacturing Extension Program.

4. **Insurance Institute for Cyber Safety(IICS) Anchor** – In 1894, U.S. insurance companies came together to create the Underwriters Laboratories (UL), with headquarters in Northbrook, IL, to provide safety analyses and safety ratings of new technologies. Insurance companies collaborated again in 1959 to create the Insurance Institute for Highway Safety (IIHS) with headquarters in Arlington, VA, to rate motor vehicle safety. The proposed Insurance Institute for Cyber Safety (IICS) would again bring together insurance companies to assess and rate cybersecurity risk.

5. **Business Sector Consortium on Cyberprotection Anchor** – The University of Tulsa has alumni and trustees in leadership positions in energy, banking, credit rating and financial security, global retail, trucking and aviation. This consortium would allow these business sectors to regularly inform cybersecurity system developers of their risks and needs.

6. **City of Tulsa Anchor** – The 6th Street Corridor between downtown Tulsa's East Village, to the Pearl District to the Kendall Whittier Neighborhood to The University of Tulsa's Cyber District is primed for further redevelopment. It is close to downtown and The University of Tulsa, has lower priced land values and allows a mix of housing, retail, startup businesses, scaleup businesses as well as new cyber training and research facilities.

7. **Opportunity Zone Investment** – Created through the Tax Cut and Jobs Act of 2017 and the Investing and Opportunity Act, Opportunity Zones are a new 10-year national community investment opportunity with the potential for a 15% capital gains tax reduction as a key incentive. State and local governments have recently established official Opportunity Zones with a large track identified from downtown Tulsa to The University of Tulsa with 6th Street as a central "back bone" to this corridor.

Tulsa market analysis

This is the right time for investment in this Tulsa-based focused expansion. Past private and public investments have provided Tulsa with great momentum to develop, attract and retain young talent for the knowledge economy:

DOWNTOWN TULSA AND BROKEN ARROW ROSE DISTRICT – These downtown cores have been redeveloped with world-class sports and entertainment venues, a vibrant arts district, new restaurants, new museums and many more housing and hotel options.

VIBRANT NEIGHBORHOODS FOR YOUNG PEOPLE – The Brookside, Cherry Street and Florence Park neighborhoods are thriving with young adult residents.

RECREATION – The River Parks System and Turkey Mountain Urban Wilderness have all been redeveloped.

A WORLD-CLASS PARK – The Gathering Place has exceeded even the loftiest expectations in bringing Tulsa area residents together.

IMPROVING TRANSPORTATION – New transportation options have arrived including improved bikeways, e-scooters and soon Rapid Bus Transit.

COST OF LIVING – Tulsa's housing costs are 11% below the national average and continue to be far less expensive than regions popular among young talent e.g. Portland, Seattle, Bay Area Los Angeles, Austin, Boston, Denver and New York. The 6th Street Corridor has numerous properties that are of low cost and close to downtown neighborhoods undergoing revitalization and The University of Tulsa.

TU is uniquely positioned among universities for this work

Experience – The University of Tulsa has been a leader in information security for the past 20 years.

Expertise – The University of Tulsa carries three NSA Center of Excellence delegations including Information Assurance and Cyber Defense Education, Information Assurance Research and Cyber Operations. These three designations place TU among a small handful of research universities.

Established Federal and Industry Partnerships – The University of Tulsa has joint programs in place with the U.S. Department of Defense, U.S. Department of Energy, the National Security Administration, the Department of Homeland Security, the United States Air Force – Tinker Air Force Base, DARPA, and the National Motor Freight Trucking Association. As well, TU hosts energy research consortia with large global corporate partners including Chevron, Exxon Mobil and Phillips 66.

Multiple Business Sector Cyber Platforms – TU has established cyber-related research programs in Cyber Defense and Offense, Cell Phone Forensics, Information Security Economics, Critical Infrastructure Security – including pipelines, electrical grid, nuclear power plants, Heavy Vehicle Cyber Security, Applied Center for the Cloud of Things and Human Behavioral Vulnerabilities in Information Security.

Multiple Cyber Education Pathways – TU has expanded its education pathways in cyber-related majors. This includes: bachelor's degrees in computer science, data analytics or computer information systems linking to a minor in cybersecurity, residential and online master's degrees in cybersecurity and scholarships for service programs through the National Security Agency and National Science Foundation.

Beyond excellent timing, there is an urgency to this initiative:

FEWER COLLEGE ELIGIBLE HIGH SCHOOL GRADUATES – The United States is facing a 20% drop in college eligible high school graduates beginning in 2025. By 2029, the U.S. workforce will face a 20% drop in college graduates. It is imperative that Tulsa attracts high school graduate talent from across the nation to TU and their computer science, data analytics, cyber, energy and engineering programs as a source of knowledge economy talent for the region. This initiative is part of an expansion at TU that will rapidly add 1,000 students at The University of Tulsa.

TAX INCENTIVES SUNSET – The guide referenced above notes that the Opportunity Zone program has the potential to deploy hundreds of billions of re-investment dollars but this tax incentive sunsets in 10 years.

Potential investors and consortium members in the cyberdistrict

Cities with successful Opportunity Zones feature joint efforts and investments of Qualified Opportunity Funds alongside corporate, civic, philanthropic and university interests. Listed here are the types of agencies and companies with cyberdefense needs and strong connections to Tulsa and TU that are potential investors for the Tulsa Enterprise for Cyber Innovation Talent and Entrepreneurship.

- National Defense
- Insurance
- Transportation – Trucking
- Transportation – Aerospace
- Banking
- Energy – Pipeline Integrity
- Energy – Grid Protection
- State of Oklahoma
- Small Business

Tyler Moore

Tyler Moore is the Tandy Associate Professor of Cybersecurity and Information Assurance in the Tandy School of Computer Science at The University of Tulsa. His research applies methods from economics to improve cybersecurity. For example, his research collects and analyzes cybercrime data to quantify the costs and benefits of investments into security controls. Moore's *Science* article, co-authored with Ross Anderson, is recognized for providing a canonical introduction to applying economics to explain cybersecurity challenges. He is leading a $1.5 million, three-year joint effort with Carnegie Mellon University and Delft University of Technology to develop a better understanding of the relationship between cybersecurity spending and secure outcomes. This project, funded by the Department of Homeland Security and set to begin in January 2019, will also involve collaborations with private industry partners at Fox-IT, SecurityScoreCard and CyberCube. Moore also seeks to explain how attackers and defenders operate through empirical observation. One such effort is an investigation into how security shocks affect cryptocurrency markets. In collaboration with economists from Tel Aviv University, the NSF-BSF funded project (awarded 2017) has identified how price manipulation has inflated the price of Bitcoin, documented pump-and-dump schemes targeting thinly traded cryptocurrencies and examined the impact of denial-of-service attacks on currency exchanges. Broadly speaking, his research is aimed at making cybersecurity more scientifically grounded. His NSF CAREER project (awarded 2017) is focused on developing more robust indicators of cybercriminal activity. These indicators are being collected longitudinally in order to more reliably establish whether defenders are making quantifiable improvements to security over time.

SELECTED PUBLICATIONS IN CYBERSECURITY

R. Anderson and T. Moore, The Economic of Information Security, *Science*, 314(5799):610--613, 2006.

N. Gandal, J.T. Hamrick, T. Moore, and T. Obermann. Price manipulation in the Bitcoin ecosystem, *Journal of Monetary Economics*, 95:86--96, May 2018.

S. Tajalizadehkhoob, T. van Goethem, M. Korczyński, A. Noroozian, R. Böhme, T. Moore, W. Joosen, and M. van Eeten. Herding vulnerable cats: A statistical approach to disentangle joint responsibility for web security in shared hosting, In *ACM SIGSAC Conference on Computer and Communications Security* (CCS '17), 2017.

M. Vasek, J. Wadleigh, and T. Moore. Hacking is not random: a case-control study of webserver-compromise risk, *IEEE Transactions on Dependable and Secure Computing*, 13(2):206--219, 2016.

R. Böhme, N. Christin, B. Edelman, and T. Moore. Bitcoin: Economics, technology, and governance, *Journal of Economic Perspectives*, 29(2):213--38, 2015.

Rose Gamble

Rose Gamble is the Tandy Professor of Computer Science & Engineering in the Tandy School of Computer Science at The University of Tulsa. As director of the Software Engineering and Architecture Team, her research activities involve security assurance for autonomous and self-adaptive systems funded by the Air Force Research Laboratory Information Directorate (AFRL-ID), drone coordination and path planning for mission success funded under a separate program at AFRL-ID, heavy vehicle cybersecurity testbed development funded by the National Science Foundation (NSF), human subjects studies in trust and suspicion funded by the Air Force Research Laboratory Human Performance Wing (AFRL-HPW). Gamble has just begun leading a new effort with collaborators from Michigan State University on certifying at runtime that self-healing software programs maintain compliance with security constraints. This effort will extend her work on wearable and IoT device self-protection to autonomous robots. Gamble holds a patent for an Auditable Multi-Claim Security Token that allows forensic analysis of message exchanges by aggregating identity-related information that is transmitted among composed web services. She established the university's Applied Research Center for the Cloud of Things in January 2016 that collaborates with industry partners to develop client-based platforms and scenarios for experimentation, implement cloud services for internet-enabled devices, and perform security and predictive analytics on proprietary data. The algorithms developed under those contracts provide value-added to the supporting industries in terms of predicting mechanical degradation to ensure timely maintenance and reduce monetary losses, intrusion detection on network communications from a well site to an online dashboard for operations analysis, and more recently blockchain verification of IoT firmware device updates to aid in supply chain tracking. In addition to support from AFRL and NSF, Gamble's research program has been funded by the U.S. Air Force Office of Scientific Research, DARPA, the Department of Energy, the state of Oklahoma and local industry.

SELECTED PUBLICATIONS IN CYBERSECURITY

M. Hale, K. Lofty, R. Gamble, C. Walter, and J. Lin, Developing a platform to evaluate and assess the security of wearable devices, *Digital Communications and Networks*, Oct. 2018.

C. Walter, I. Riley, and R. Gamble, Securing Wearables through the Creation of a Personal Fog, in the *Proceedings of the 51st Hawaii International Conference on System Sciences*, nominated for Best Paper Award, Jan. 2018.

M. Hale and R. Gamble, Semantic Hierarchies for Extracting, Modeling, and Connecting Compliance Requirements in Information Security Control Standards, *Requirements Engineering*, pp. 1-38, Dec. 2017.

S. Alqahtani and R. Gamble, Verifying the Detection Results of Impersonation Attacks in Service Clouds, *Advances in Science, Technology, and Engineering Systems*, 2(3): 449-459, 2017.

M. Hale, C. Walter, J. Lin, and R. Gamble, A Priori Prediction of Phishing Victimization based on Structural Content Factors, *International Journal of Services Computing* (IJSC), 5(1), 2017, pp. 1-13.

John Hale

John Hale holds the Tandy Endowed Chair in Bioinformatics and Computational Biology as a Professor in the Tandy School of Computer Science at The University of Tulsa. He is a founding member of the TU Institute of Bioinformatics and Computational Biology (IBCB), and a faculty research scholar in the Institute for Information Security (iSec). His research has been funded by the U.S. Air Force, the National Science Foundation (NSF), the Defense Advanced Research Projects Agency (DARPA), the Army Research Office (ARO), National Security Agency (NSA), the National Institutes of Health (NIH) and the National Institute of Justice (NIJ). These projects include research on neuroinformatics, cybertrust, information privacy, attack modeling, secure software development, high performance computing and cyberphysical system security. He has testified before Congress on three separate occasions as an information security expert, and in 2004 was awarded a patent on technology to thwart digital piracy on file sharing networks. In 2000, Hale earned a prestigious NSF CAREER award for his educational and research contributions to the field of information assurance.

SELECTED PUBLICATIONS IN CYBERSECURITY

B. Brummel, J. Hale and M. Mol, Training Cyber Security Personnel, *The Psychosocial Dynamics of Cyber Security Work*, S. Zaccaro, R. Dalal, and L. Tetrick (Eds.), Routledge, Boca Raton, FL, 2015.

M. Hale, R. Gamble, J. Hale, M. Haney, J. Lin, and C. Walter, Measuring the Potential for Victimization in Malicious Content, in the *Proceedings of the 22nd IEEE International Conference on Web Services*, pp. 305-312, June 2015.

P. Hawrylak, C. Hartney, M. Papa and J. Hale, Using Hybrid Attack Graphs to Model and Analyze Attacks against the Critical Information Infrastructure, *Critical Information Infrastructure Protection and Resilience in the ICT Sector*, S. Bologna, P. Theron (Eds.), IGI Global, Hershey, PA, pp. 173-197, 2013.

K. Clark, E. Singleton, S. Tyree and J. Hale, Strata-Gem: risk assessment through mission modeling, in the *Proceedings of the Fourth ACM workshop on Quality of Protection*, pp. 51 - 58, Alexandria, Virginia, USA, October, 2008.

J. Hale, M. Papa and S. Shenoi, Programmable access control, *Journal of Computer Security*, vol. 11, no. 3, IOS Press, Amsterdam, The Netherlands, pp. 331-351, 2003.

Mauricio Papa

Mauricio Papa is an Associate Professor in the Tandy School of Computer Science at The University of Tulsa and Director of the Institute for Information Security (iSec). Papa received his bachelor of science in electrical engineering from Universidad Central de Venezuela in 1992 and his master of science in electrical engineering and doctorate in computer science from TU in 1996 and 2001, respectively. His primary research area is critical infrastructure protection. His team has designed and constructed process control testbeds to support cybersecurity efforts in critical infrastructure protection. As part of his efforts in that area, he has focused his work in the development of situational awareness tools as well as extending traditional IT solutions for intrusion detection systems and firewalls for their use in process control systems as supported by an industry contract through the Applied Research Center for the Cloud of Things. He also conducts research in network security and intelligent control systems. More recently, he developed an interest in IoT devices and the use of machine-learning and data analytics to help model multiphase flow properties in collaboration with The University of Tulsa Fluid Flow Projects group.

SELECTED PUBLICATIONS IN CYBERSECURITY

W. M. Nichols, P. J. Hawrylak, J. C. Hale and M. Papa, Methodology to estimate attack graph system state from a simulation of a nuclear reactor system, in the *Proceedings of Resilience Week* (RWS) 2018, pp. 84-87, August 2018.

W. Nichols, P. Hawrylak, J. Hale and M. Papa, Introducing Priority into Hybrid Attack Graphs, in the *Proceedings of 12th Annual Cyber and Information Security Research Conference*, Article No. 12, April 2017.

J. Nivethan and M. Papa, On the use of open-source firewalls in ICS/SCADA systems, *Information Security Journal: A Global Perspective*, Taylor & Francis, ISSN: 1939-3555 (Print), 1939-3547 (Online), 2016.

J. Nivethan and M. Papa, A Linux-based firewall for the DNP3 protocol (Best Paper Award), in the *Proceedings of the IEEE International Symposium on Technologies for Homeland Security*, May 2016.

J. Nivethan and M. Papa, Dynamic rule generation for SCADA intrusion detection, in the *Proceedings to the IEEE International Symposium on Technologies for Homeland Security*, May 2016.

Jeremy Daily

Jeremy Daily is an Associate Professor in the Department of Mechanical Engineering at The University of Tulsa. His funding for research and education in heavy vehicle cybersecurity to address transportation as a critical infrastructure concern comes from both public and private sources. Both the Department of Defense (DoD) and the National Science Foundation (NSF) currently provide support. The heavy vehicle industry represented by the National Motor Freight Traffic Association (NMFTA) has recognized TU as a performer in talent generation for the cybersecurity workforce needs of the transportation industry. The NMFTA and other industry partners currently fund the Student CyberTruck Experience (CyTeX) that teaches engineering students interested in transportation fundamental skills related to cybersecurity with hands-on research activities. This exclusive Tulsa program has successfully placed engineers into automotive cybersecurity jobs. Creating the CyberTruck Challenge, administered by TU for the first time in 2017, was a significant achievement toward broadening participation in cybersecurity training across the United States and Canada. Students gain skills through lectures and exercise those skills on actual vehicles provided by the original equipment manufacturers, like Cummins and PACCAR. The CyberTruck Challenge was such a success that it became a self-sustaining nonprofit organization after the first year. Another exciting contribution to the heavy vehicle cybersecurity ecosystem is a company, Synercon Technologies, started by TU students and faculty using their intellectual property. It provides digital forensics solutions for heavy vehicle event data recorders with customers all over the United States and Canada. Synercon Technologies was founded by Daily in 2013 and sold to the Dearborn Group in Michigan in 2018.

SELECTED PUBLICATIONS IN CYBERSECURITY

J. Daily, and B. Gardiner, Cyber security Considerations for Heavy Vehicle Event Data Recorders, in the *Proceedings of the 6th ESCAR USA - The World's Leading Automotive Cyber Security Conference*, June 2018.

J. Daily, U. Jonson, and R. Gamble, Talent Generation for Vehicle Cyber Security, *5th ESCAR USA - The World's Leading Automotive Cyber Security Conference*, June 2017.

S. Mukherjee, H. Shirazi, I. Ray, J. Daily, and R. Gamble, Practical DoS Attacks on Embedded Networks in Commercial Vehicles, In: Ray I., Gaur M., Conti M., Sanghi D., Kamakoti V. (eds) Information Systems Security. ICISS 2016. *Lecture Notes in Computer Science*, vol 10063. Springer, Cham, 2016.

J. Daily, R. Gamble, S. Moffitt, C. Raines, et al., Towards a Cyber Assurance Testbed for Heavy Vehicle Electronic Controls, *SAE Int. J. Commer. Veh*. Best Paper Award, 9(2):339-349, 2016.

J. Daily, J. Johnson, and A. Perera, Recovery of Partial Caterpillar Snapshot Event Data Resulting from Power Loss, SAE Technical Paper 2016-01-1493, *SAE World Congress*.

Peter J. Hawrylak

Peter J. Hawrylak is an Associate Professor in the Department of Electrical and Computer Engineering at The University of Tulsa. His research area focuses on hardware design and wireless system development, with an emphasis on cybersecurity for those systems. He is also active in the high-performance computing community in the area of reconfigurable logic and heterogeneous computing. Hawrylak currently holds 13 patents in the areas of Radio Frequency Identification, wireless systems, energy harvesting, and cybersecurity; several of which have been commercialized. His research has been funded by the U.S. Department of Defense (DoD), U.S. Army, U.S. Department of Energy (DOE), National Science Foundation (NSF), U.S. Department of Transportation (DOT) and private industry. These research efforts are focused on building smart infrastructure, designing tools to help secure the next generation of nuclear reactors, and developing cyberattack modeling and analysis tools to theorize new attack vectors and countermeasures to those attack vectors. Hawrylak is a senior member of the IEEE and IEEE Computer Society. He is currently secretary of the Tulsa Section of the IEEE. He served as chair of the RFID Experts Group (REG) of Association for Automatic Identification and Mobility (AIM) in 2012-2013. Peter received AIM Inc.'s Ted Williams Award in 2015 for his contributions to the RFID industry. Hawrylak is publication chair of the International IEEE RFID Conference and is editor-in-chief of the *International Journal of Radio Frequency Identification Technology and Applications* (IJRFITA), a journal published by InderScience Publishers, which focuses on the application and development of RFID technology. Hawrylak is also editor-in-chief of the *IEEE RFID Virtual Journal*, which provides a single source for high-quality and high-impact publications in the areas of RFID and Internet of Things (IoT).

SELECTED PUBLICATIONS IN CYBERSECURITY

W. Nichols, P. J. Hawrylak, J. Hale, and M. Papa, Methodology to Estimate Attack Graph System State from a Simulation of a Nuclear Research Reactor, *Resilience Week* (RWS), pp. 84-87, 2018.

J. Trewitt, P. Hawrylak, and M. Keller, Time delay tags for commercial ground penetrating radars, *IEEE Radar Conference* (RadarConf18), pp. 1466-1471, 2018.

R. Raval, A. Maskus, B. Saltmiras, M. Dunn, P.J. Hawrylak and J. Hale, Competitive Learning Environment for Cyber-Physical System Security Experimentation, in the *Proceedings of the 1st International Conference on Data Intelligence & Security* (ICDIS), pp. 211-218, 2018.

W. Nichols, Z. Hill, P. Hawrylak, J. Hale, and M. Papa, Automatic Generation of Attack Scripts from Attack Graphs, in the *Proceedings of the 1st International Conference on Data Intelligence & Security* (ICDIS), pp. 267-274, 2018.

Z. Hill, W.M. Nichols, M. Papa, J.C. Hale, and P.J. Hawrylak, Verifying Attack Graphs through Simulation, *Resilience Week* (RWS), pp. 64-67, 2017.

Ido Kilovaty

Ido Kilovaty is the Frederic Dorwart Endowed Assistant Professor of Law at The University of Tulsa. He comes to the College of Law after two years as a Research Scholar in Law at Yale Law School. At Yale, he was a Cyber Fellow at the Center for Global Legal Challenges, and a Resident Fellow at the Information Society Project, where he remains an affiliated fellow. Kilovaty is also a 2018-19 Cybersecurity Policy Fellow at New America. He specializes in the intersection of technology, law and society, with a focus on cybersecurity – both domestic and international. His specific areas of research include cybersecurity law, internet governance, and domestic and global technology regulation. His recently authored "Freedom to Hack," which proposes a solution of ethical hacking for the improvement of smart-device security is forthcoming in the *Ohio State Law Journal* and "Legally Cognizable Manipulation" which explores the relationship between novel breach-related harms and data-breach law is forthcoming in the *Berkeley Technology Law Journal.* His work has also appeared in the *Harvard National Security Journal, Michigan Telecommunications and Technology Law Review, Duke Law & Technology Review, Columbia Science and Technology Law Review* and more. Kilovaty's op-eds and essays appeared at Harvard Law Review Blog, Lawfare, Just Security, WIRED, and TechCrunch.

SELECTED PUBLICATIONS IN CYBERSECURITY

I. Kovalty, Legally Cognizable Manipulation, to appear in the *Berkeley Technology Law Journal*, 2019.

I. Kovalty, Freedom to Hack, to appear in the *Ohio State Law Journal*, 2019.

I. Kovalty, Doxfare – Politically Motivated Leaks and the Future of the Norm on Non - Intervention in the Era of Weaponized Information, *Harvard Law School National Security Journal,* vol. 9, pp. 146-179, 2018.

I. Kovalty, Virtual Violence - Disruptive Cyberspace Operations as "Attacks" under International Humanitarian Law, *Michigan Telecommunications & Technology and Law Review*, vol. 23, no. 1, pp. 113-146, 2016.

I. Kovalty, ICRC, NATO, and the U.S. - Direct Participation in "Hacktivities" - Targeting Private Contractors in Cyberspace Under the Law of Armed Conflict, *Duke Law & Technology Review*, vol. 15, no. 1, pp. 1-38, 2016.

Bradley Brummel

Bradley Brummel is an Associate Professor of Psychology at The University of Tulsa. He received his PhD in Industrial-Organizational Psychology from the University of Illinois at Urbana-Champaign. He conducts research on training and development in the workplace with a special focus on simulation methods, professional development coaching and ethics. His research has been funded but the National Science Foundation (NSF) and the U.S. Air Force Office of Sponsored Research. Dr. Brummel's research has been published in journals such as the *Journal of Applied Psychology, Human Relations, Journal of Management,* and *Personnel Psychology.*

SELECTED PUBLICATIONS IN CYBERSECURITY

B.J. Brummel, Decision-making Cues Related to Trust. Invited presentation at the Organizational Sciences and Cybersecurity Workshop, July 2018.

B.J. Brummel, D. Cosley, R. Dalal, B. Fidler, and S. Straus, Interdisciplinary Funding and Publications. *Panel Discussion at the Organizational Sciences and Cybersecurity Workshop,* George Mason University, April 2018.

B.J. Brummel, J. Hale, and M.J.Mol, Training cybersecurity personnel, in, *The Psychosocial Dynamics of Cyber Security*, S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, & J. A. Steinke (Eds.), pp. 217-239, New York: Routledge, 2016.

R.E. Beyer, and B.J. Brummel, Implementing effective cybersecurity training for end users of computer networks, in *Society for Human Resource Management and Society for Industrial and Organizational Psychology Science of Human Resource Series: Promoting Evidence-Based HR,* 2015.

J. Staggs, R. Beyer, M. Mol, M. Fisher, B. Brummel, and J. Hale, A perceptual taxonomy of contextual cues for cyber trust, *Journal for The Colloquium for Information System Security Education* (CISSE), vol. 2, pp. 152-169, 2014.

Sal Aurigemma

Sal Aurigemma is an Assistant Professor of Computer Information Systems where he teaches Telecommunications, Information Security, and Business Programming Concepts for the Collins College of Business School of Accounting and Computer Information Systems at The University of Tulsa. A Navy veteran of more than 20 years (both on active duty and the reserves), he served as a submarine officer on the USS PINTADO (SSN 672) and later as a Naval Intelligence Officer deployed to Afghanistan in support of Operation Enduring Freedom. After leaving active duty, he worked more than a decade in the Information Technology field supporting the U.S. Department of Defense (DoD), serving in a variety of roles from system administration, project management, and system architecture analysis and design. A major emphasis of his IT work dealt with managing the fusion of disparate geospatial information systems and tactical data links and sharing data securely across multiple security domains and infrastructures. His research explores employee information security policy compliance, improving end-user and small business information security practices, and end-user computing focusing on business spreadsheet error detection. He has published in *Computers & Security, Information and Computer Security, Decision Support Systems,* the *Journal of Organizational and End User Computing,* and the *Journal of Information Systems Security* and was awarded the Collins College of Business Mayo Teaching Excellence Award for 2015-2016.

SELECTED PUBLICATIONS IN CYBERSECURITY

S. Aurigemma, T. Mattson, and L. Leonard, Evaluating the Core and Full Protection Motivation Theory Nomologies for the Voluntary Adoption of Password Manager Applications, *AIS Transactions on Replication Research*, April 2018.

S. Aurigemma and T. Mattson, Exploring the Effect of Uncertainty Avoidance on Taking Voluntary Protective Security Actions, *Computers & Security*, vol. 73, pp. 219-234, March 2018.

S. Aurigemma and T. Mattson, Privilege or Procedure: Evaluating the Effect of Employee Status on Intent to Comply with Interactive Security Controls, *Computers & Security*, vol. 66, pp. 218-234, May 2017.

S. Aurigemma and T. Mattson, T. (2017) Deterrence and Punishment Experience Impacts on ISP Compliance Attitudes. Information and Computer Security 25(4).

S. Aurigemma and L. Leonard, The Influence of Employee Affective Organizational Commitment on Security Policy Attitudes and Compliance Intentions, *Journal of Information System Security*, 11(3), 201-222, 2016.

Security assurance for self-adaptive and autonomous systems

RUNTIME ADAPTATION AND HEALING CAN ADDRESS ENVIRONMENTAL UNCERTAINTIES AND SECURITY THREATS

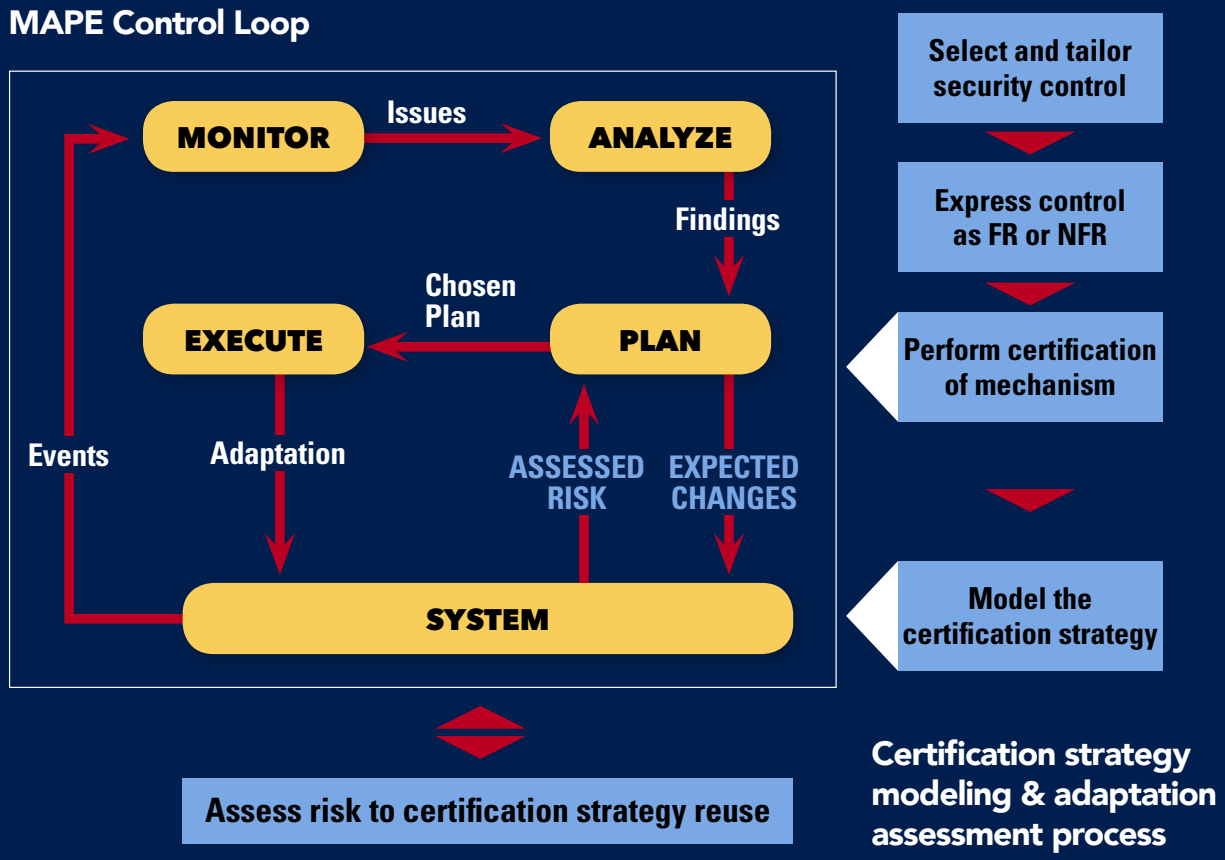
- Continuous monitoring provides situational awareness
- Cloud-based and embedded decision analysis

MAIN OBJECTIVE

- Perform runtime assessment of an adaptation's risk to violate critical security controls

RESULTS

- Model the security V&V&C processes with confidence levels as security control contracts
- Connect contracts through dependent constraints
- Embed model with utility functions for runtime risk assessment of potential adaptations and patches
- Reassign security constraint compliance confidence values post adaptation



Blockchain to secure oil & gas supply chain

OIL & GAS SUPPLY CHAIN IS VULNERABLE TO COUNTERFEIT MATERIALS OR PRODUCTS AND THEFT

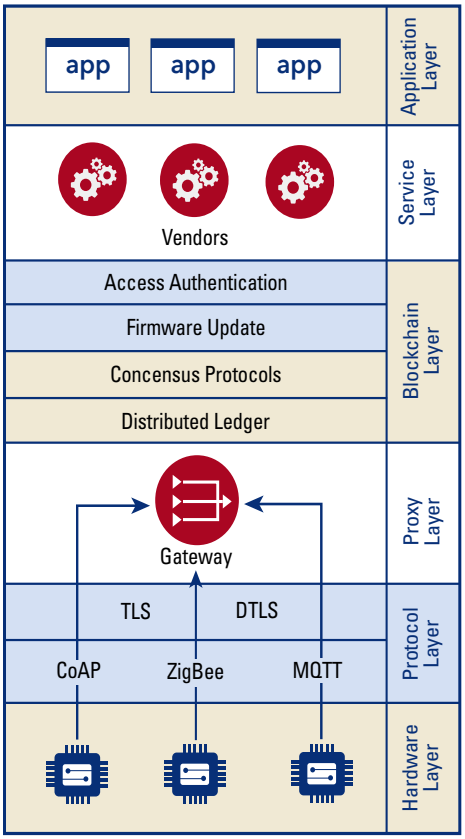
- Lacks assured logistic tracking mechanisms along the value chain

MAJOR CHALLENGES

- Monitoring raw materials and products with IoT devices
- Providing IoT device firmware security during OTA updating

INVESTIGATIONS

- Adopt blockchain technology to secure reliable IoT firmware update with blockchain across supply chain
  - IoT device to vendor service authentication
  - Firmware update verification
- Determine appropriate supply chain sector integration into blockchain network
  - Well site reservoir-related IoT device meter readings
  - Petroleum crude oil and raw natural gas transportation
  - Process and purification



Wearable security

WEARABLE DATA IS NOT SECURE

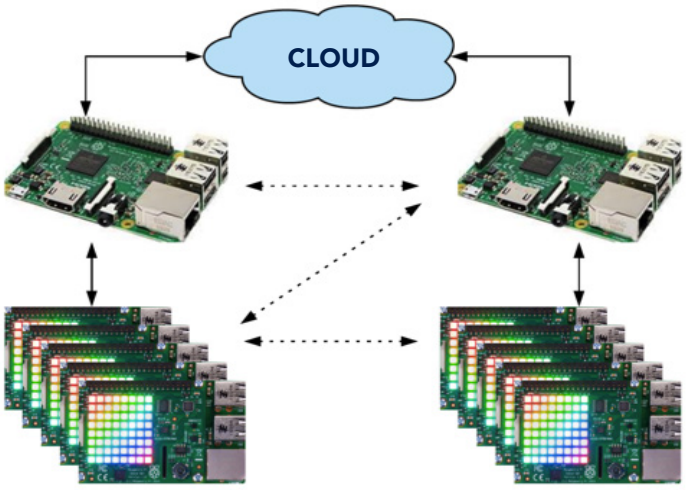
- Bluetooth Communication is easy to intercept and decrypt
- Wearables do not implement sufficient security measures
- Sniffing, tracking, and injection can occur to
  - Gather intel
  - Disable device

SIMULATED WEARABLE TESTBED

- Allows for experimentation with attacks at the network edge
- Allows for the development and testing of mitigation strategies to secure wearables at runtime
- Assesses new network architectures to secure data transmissions

RESULTS

- Wearables choose how to self-adapt their security posture at runtime based on embedded knowledge of critical requirements
- App development allows for secure communication among peer wearables



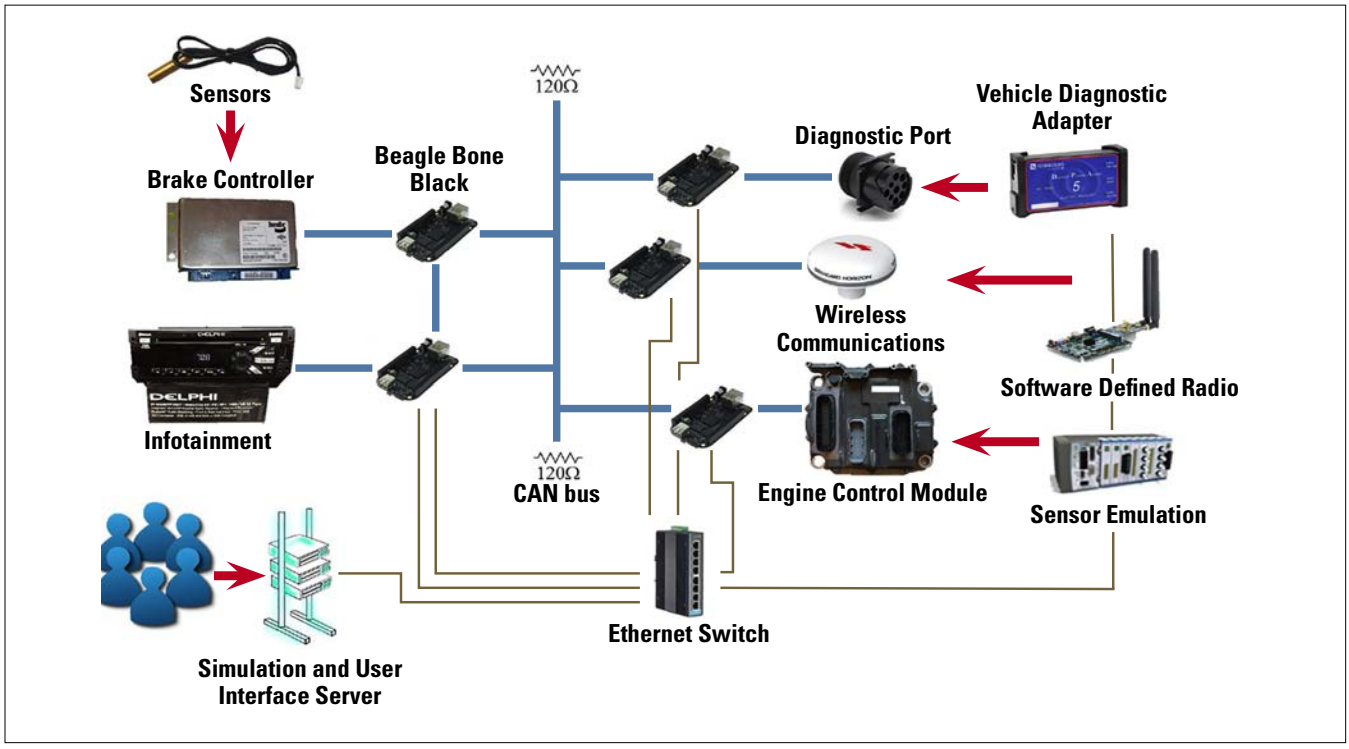
Heavy vehicle cybersecurity

DIGITAL FORENSICS OF HEAVY VEHICLE ELECTRONIC CONTROL UNITS
HEAVY VEHICLE TESTBED DESIGN AND IMPLEMENTATION

- Allows for remote experimentation

CAN DATA COLLECTION AND ANALYSIS
EDUCATIONAL INITIATIVES

- Student CyberTruck Experience
- TU co-founded the CyberTruck Challenge



SCADA operations monitoring

OIL & GAS WELLS USE VULNERABLE NETWORKS, REQUIRING

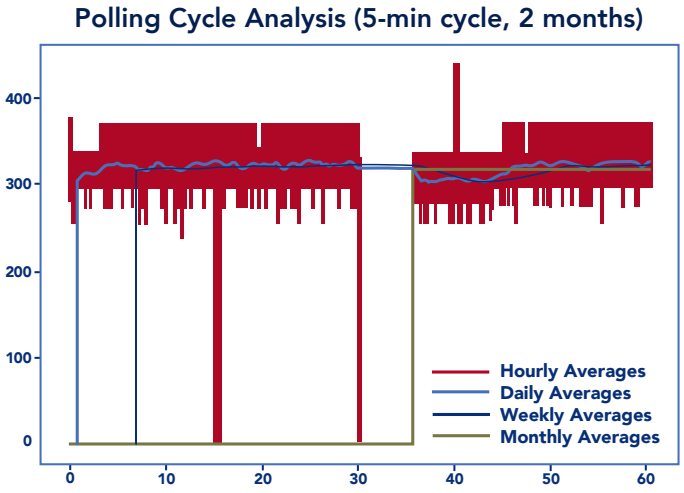
- Situational awareness (MODBUS)
- Traditional IDS techniques for real-time anomaly detection
- Statistical modeling and machine learning for pattern analysis
- Modified file-based session analysis for online use

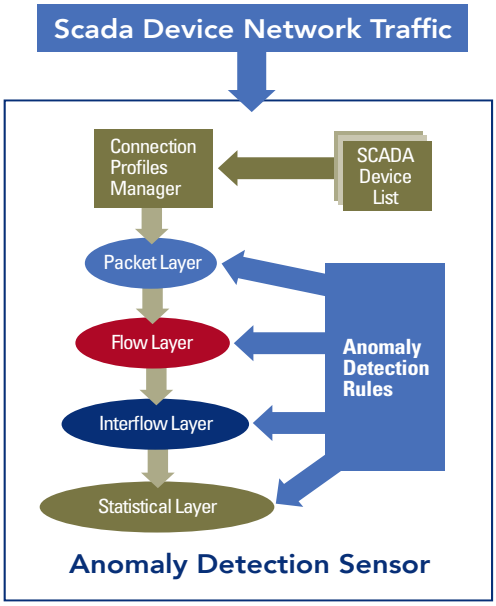
REAL TIME AND OFFLINE TESTING

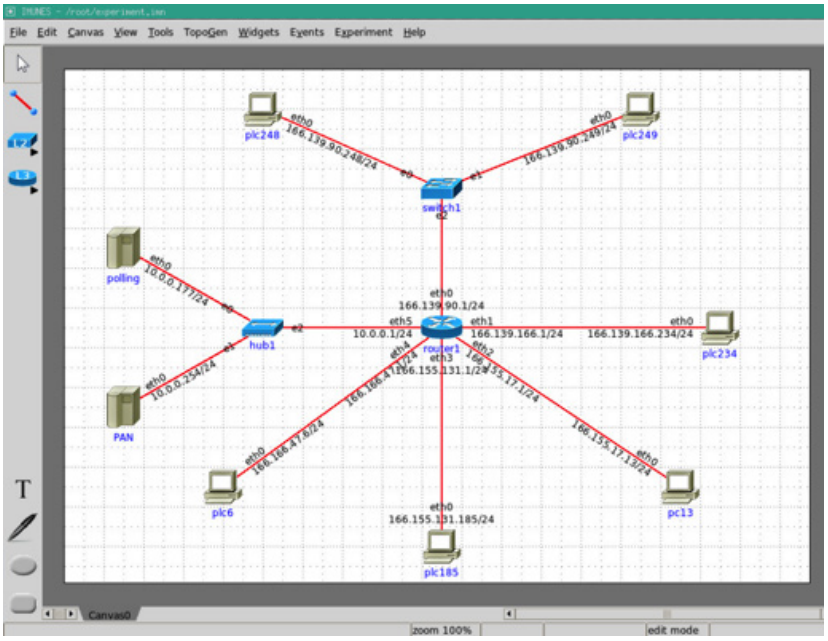
- Actual packet captures moved off site
- Network emulator replays captures
- 1+ year's worth of operational data

CHALLENGES TO ADDRESS

- Scalability
- Command and control







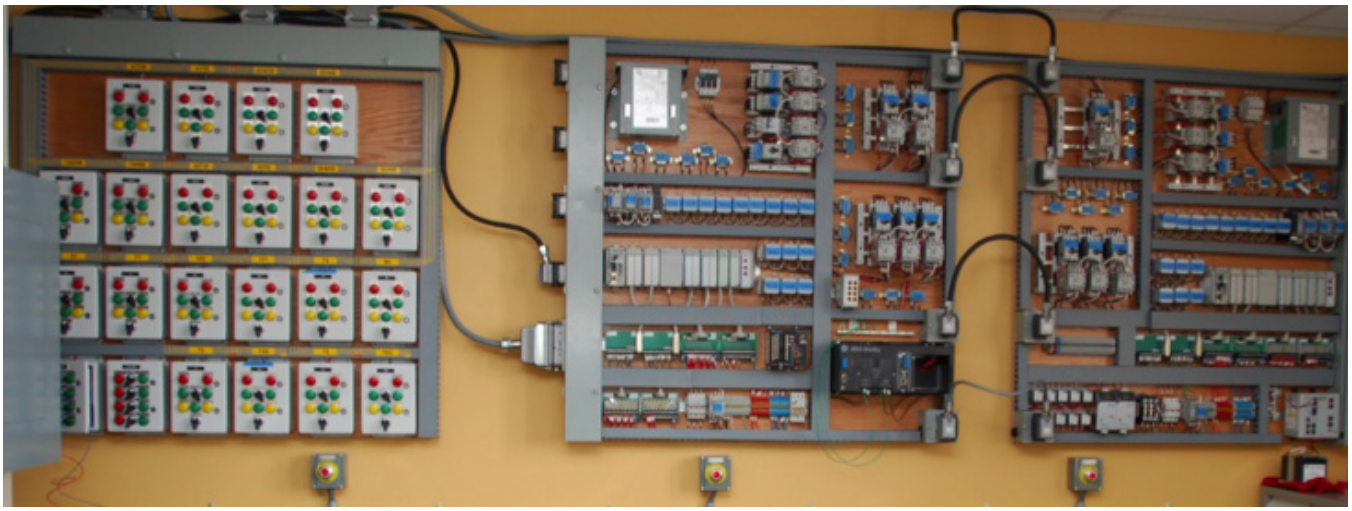
Critical Infrastructure Protection Lab

APPLIED RESEARCH AND EXPERIENTIAL LEARNING

- Cyberphysical systems security
- Improved intrusion detection
- Event monitoring in energy plants
- Integrity and auditing for settings on SCADA devices

ELECTRIC POWER SUBSTATION

- Dual 208V 3 phase inputs (ring structure), 3KVA Max. Power
- 2 PLCs, fully networked (using DNP3 over Ethernet for control)

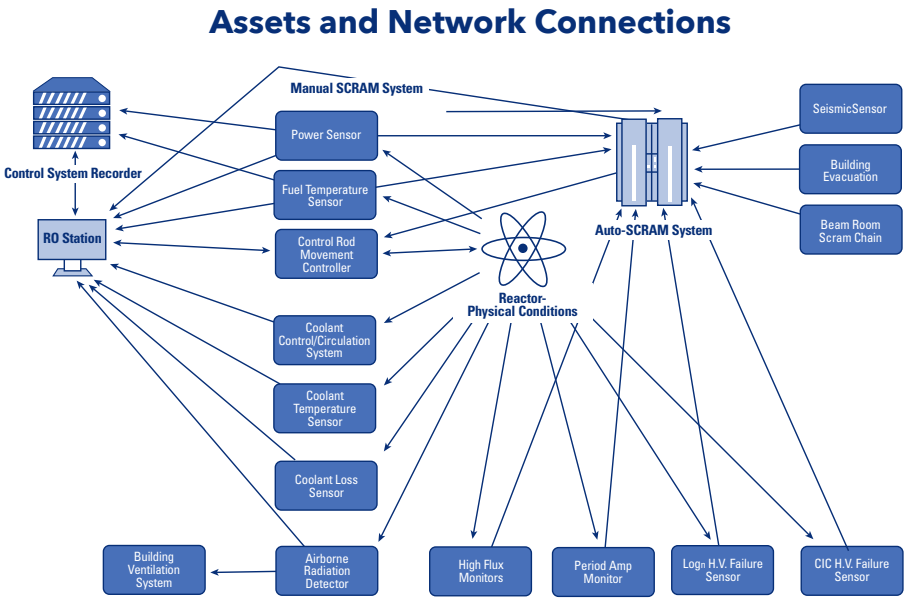


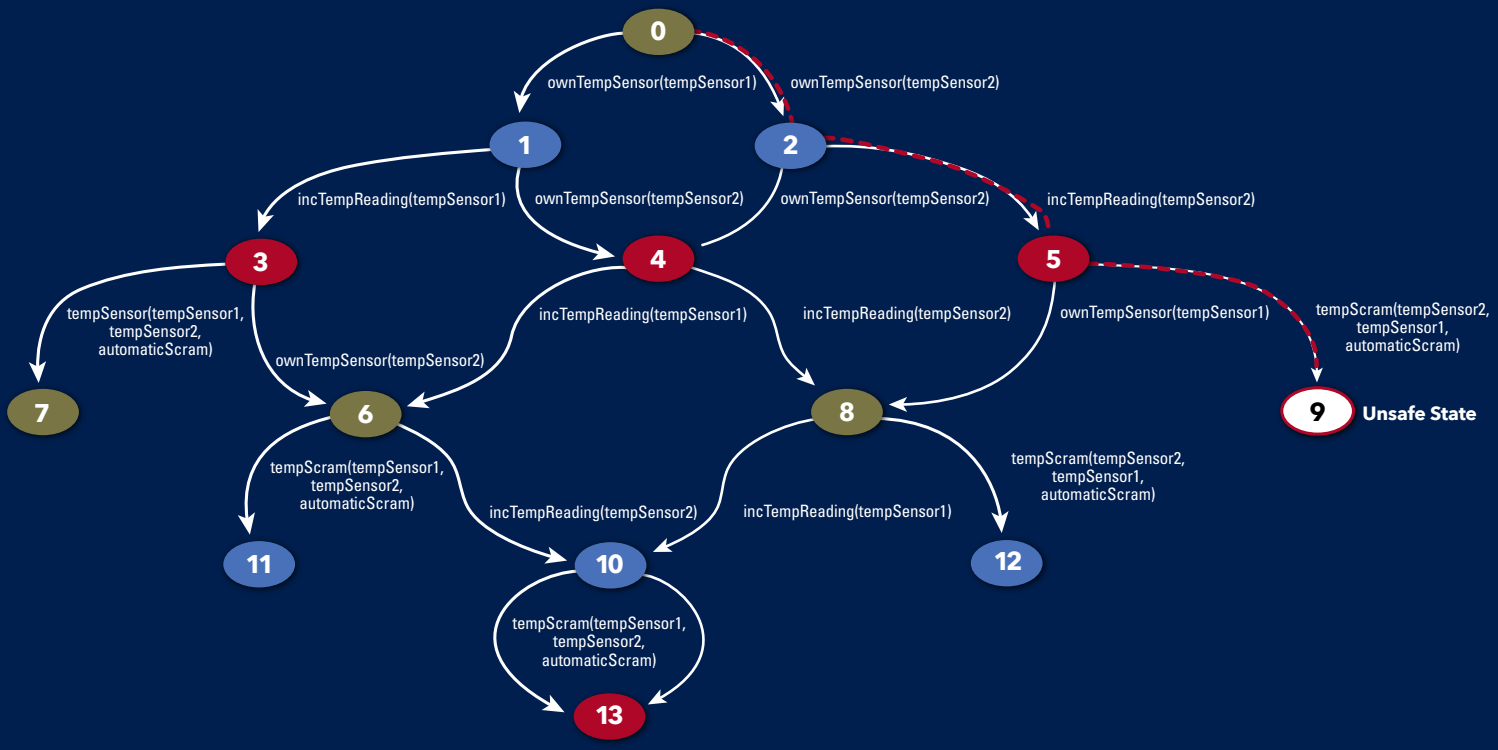
Cyberphysical system security: theory

Develop techniques and solutions for practical formal analysis of security properties in cyberphysical systems (CPSs)

HYBRID ATTACK GRAPHS (HAGS): CAPTURE ALL POSSIBLE ATTACK VECTORS FOR CPSS

- Modeling and generation – Automatic model acquisition and scalable generation
- Analysis – Critical paths, reachability, minimal cost hardening



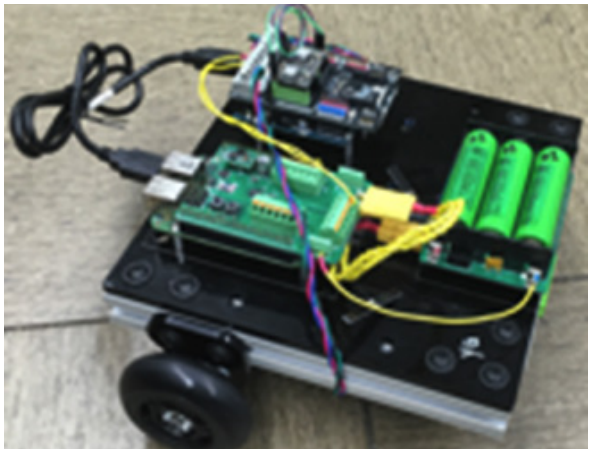


Cyberphysical system security: testbed

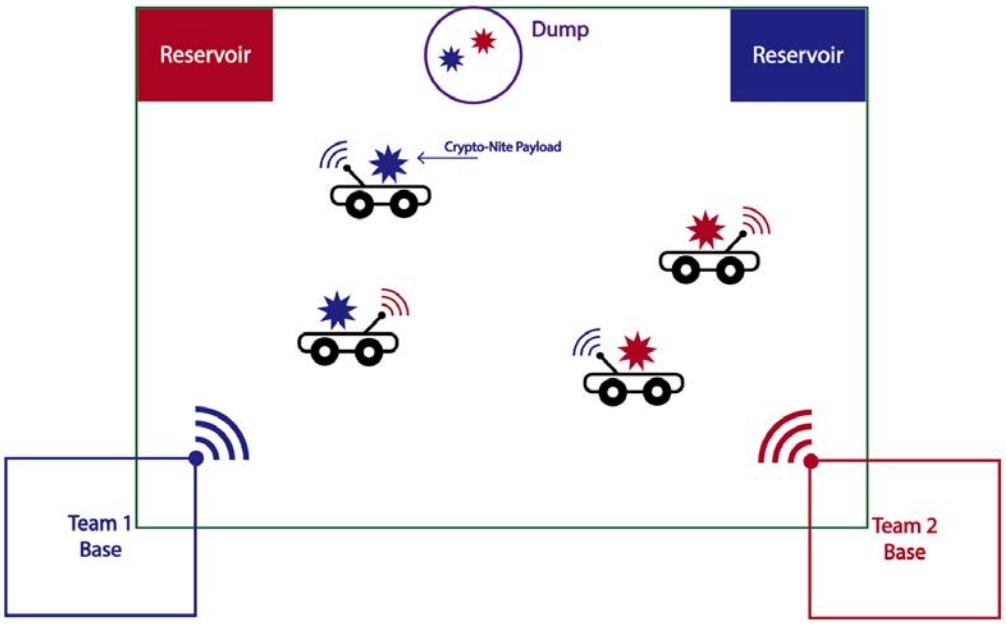
CONSTRUCT A CPS TESTBED TO SUPPORT SECURITY RESEARCH AND EXPERIENTIAL LEARNING

CPS COMPETITIVE LEARNING ARENA – A FULLY INSTRUMENTED, HACKABLE GAME ENVIRONMENT USING ROBOTIC CARS PLAYING "CAPTURE THE FLAG"

- Technologies – Wi-Fi, NFC, Windows, Linux, Teensy, JavaScript, Electron, TCP/IP
- Blended attack vectors: Cyber – Network, wireless, OS, API; Physical – Battery, Temperature, Kinetic, Spatial



Arena



Cybersecurity analysis for nuclear reactor control systems

CYBERSECURITY RECOMMENDATIONS AND GUIDANCE

- New nuclear reactor designs
- Upgrades of existing plants and nuclear research reactors

NUCLEAR REACTOR TESTBED

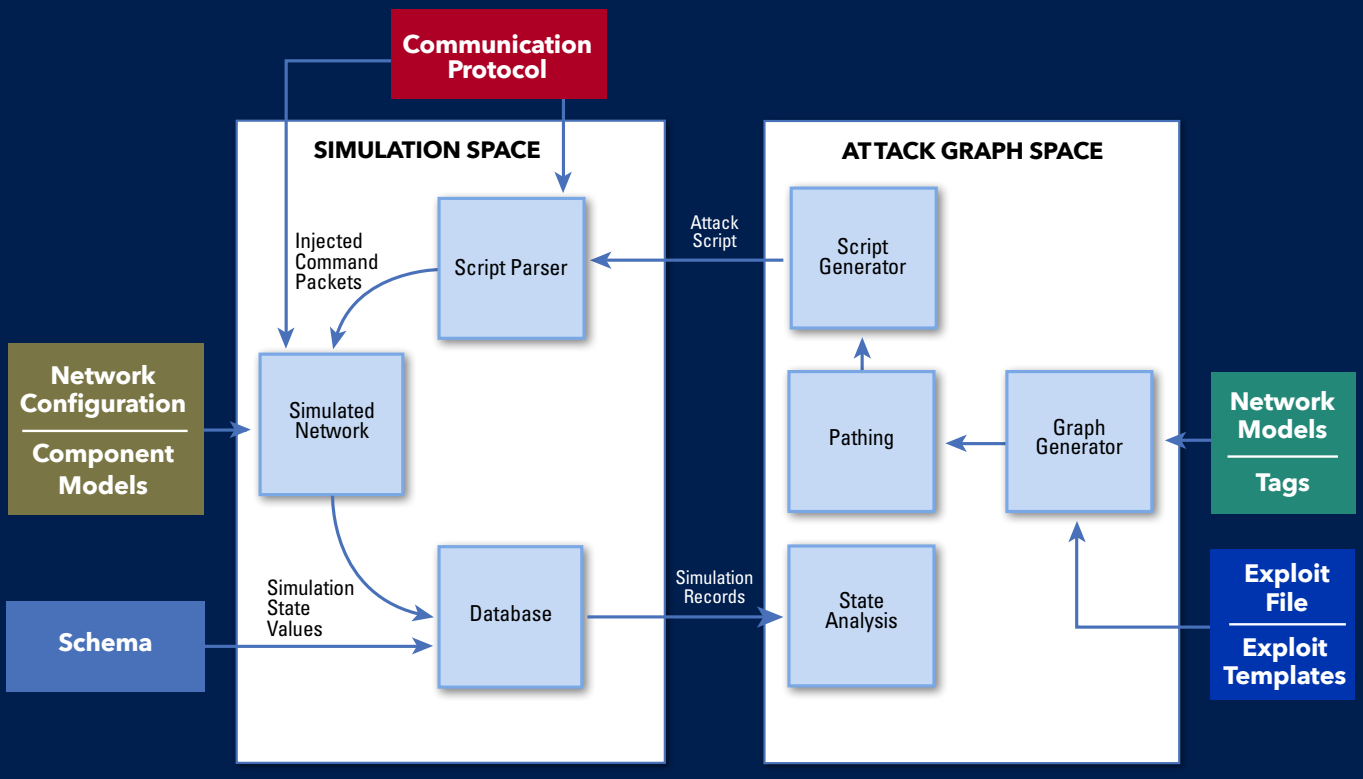
- Evaluate impact of cyberattacks
- Quantify effectiveness countermeasure

TOOLS TO IDENTIFY CYBERATTACK VECTORS AND POSSIBLE COUNTERMEASURES

- Map attack surface
- Countermeasure requirements

TOOL TO IDENTIFY CRITICAL ASSETS (CAS) AND CRITICAL DIGITAL ASSETS (CDAS)

- Saves hundreds of man-hours of effort
- Provides an audit trail with evidence



stopbadware.org

EDUCATES USERS AND WEBSITE OPERATORS ABOUT MALWARE

- Public clearinghouse lets anyone query whether websites are compromised
- 2M+ annual visits to stopbadware.org

LARGEST FREE WEB MALWARE TESTING AND REVIEW PROGRAM

- Anyone can request independent review of URLs blacklisted for malware by StopBadware's data providers: Google, ThreatTrack Security, and NSFocus
- StopBadware has helped de-blacklist 200,000+ websites
- Malware testing and review carried out by TU undergraduate researchers

DATA USED AS INPUT TO RESEARCH

Cybersecurity policy

SECURITY ECONOMICS – COLLECT AND ANALYZE CYBERCRIME DATA TO

- Quantify costs and benefits of cyber investment
- Explain how attackers and defenders operate
- Make cybersecurity more scientifically grounded

PROFESSOR MOORE REGULARLY BRIEFS LEADERS IN GOVERNMENT ON CYBERSECURITY

- Testimony on harms arising from the Equifax breach to U.S. Senate Committee of the Judiciary's Subcommittee on Privacy, Technology and the Law
- "Lessons from the Economics of Cybersecurity": JASON Summer Study on Cyber S&T
- Panel on incentives to invest in cybersecurity for Federal Trade Commission Hearing on Data Security

Judiciary
Subcommittee
SD-226

THE UNIVERSITY of TULSA

PROPOSED CAPABILITIES FOR THE UNIVERSITY OF TULSA (TU) INSURANCE INSTITUTE FOR CYBERSECURITY

- **Host Cyber Insurance ISAC (Information Sharing and Analysis Center)**
  Currently, ISACs are sector-specific (financial services, automotive, health, etc.) and are dedicated to sharing information about threat trends and coordinating sectoral responses. Insurers have interests in all of these sectors, face shared challenges in understanding emerging threats, and could benefit from sharing experiences and data. A cyber insurance ISAC, hosted by TU, could meet this unmet need.

- **Identifying Insured Risk Factors Better by Pooling Proposal Form Responses**
  Proposal forms seek to establish the cybersecurity posture and risks facing prospective insured firms through structured questions about security controls, data held, etc. To date, insurance companies have struggled to identify questions that reliably predict whether a claim is more or less likely to be subsequently made. This challenge could be for two reasons: (1) the questions need to be refined or (2) additional claims data is required. TU can provide the mechanisms to address both concerns. First, by aggregating proposal form responses and claims data across companies and conducting statistical analysis to identify discriminating questions. Second, by suggesting how to refine questions in light of the analysis.

- **Clearinghouse for Loss Data**
  Cyber insurance claims take varied forms, many of which are rapidly changing in response to evolving attacker and defender strategies. Yet the data on different types of cyber claims are frequently spotty, necessitating reliance on loss distributions borrowed from other types of coverage. Insurers can benefit from improved data on cyber losses. With the clearinghouse hosted at TU receiving anonymized loss data from multiple insurers, TU can create technology that uses the data to build better loss distribution models. The resulting models would then be shared with Institute participants.

- **Bridging the IT-Actuary Data Gap**
  While insurers regularly lament the lack of reliable cyberdata, it is not always obvious which additional data would be helpful. This is due in large part to a lack of mutual understanding between what the data IT specialists can collect (often operational in nature, only indirectly related to security posture or loss magnitude) and what actuaries need. TU can help break through this impasse by designing standardized methods for collecting relevant cyberdata when claims do occur. This standardization can in turn be used to coordinate data collection across insurers and then the Institute can analyze the data to draw insights on what factors truly affect risk of making cyber claims.

- **Public Incident Data Repository**
  When cybersecurity incidents occur at public companies, they are often reported on in the media or in regulatory filings. TU can collect a curated, ongoing list of publicly-reported cyber incidents by automatically mining various sources. This data can be used by center supporters to improve their own offerings.

- **Cybersecurity Training for Underwriters**
  It is essential for underwriters to stay abreast of the changing threat landscape, available security controls and defensive best practices. TU can offer regular training courses (online or on-campus) with curriculum that is customized to the needs of underwriters.

- **Cybersecurity Training for Boards/Leadership of Insured Clients**
  Insurance companies can mitigate their own risks by ensuring their clients are educated and well-informed on how to manage cyber risks. TU can offer regular training courses (online or on-campus) with curriculum that is targeted to the executive and board levels.

800 SOUTH TUCKER DRIVE • TULSA, OK 74104

engineering.utulsa.edu/cyber