DREXEL UNIVERSITY
Cybersecurity Institute

Funded research project profile: **NSF CAREER (M. Stamm)**

Project title	CAREER: Scaling multimedia forensic algorithms for big data and adversarial environments
Funding agency	National Science Foundation
Program	Faculty Early Career Development Program (CAREER)
Investigator	Matthew C. Stamm (PI)
Dates	March, 2016 – February, 2021 (estimated)

M. Stamm

Research summary: Over the past decade, researchers have developed a new class of security techniques known as "multimedia forensics" to determine the origin and authenticity of multimedia information, such as potentially falsified images or videos. During this time, however, society has witnessed important social and technological changes such as the proliferation of smartphones and the rise of social media. These advances have moved the means of capturing and disseminating multimedia information from the hands of a small number of official sources to the public at large. As a result, the volume of multimedia information that must be forensically authenticated has exploded. By contrast, little multimedia forensics research has focused on improving the speed at which they operate, particularly on large data sets. At the same time, the adversarial capabilities of an information attacker have also grown dramatically. Sophisticated editing software allows forgers to perform complex manipulations of digital images and videos. Furthermore, researchers have recently demonstrated that an adversarial forger can design anti-forensic attacks capable of fooling forensic algorithms.

This project sets forth a research agenda aimed at scaling multimedia forensic algorithms to address these new challenges that have arisen due to the evolving technical and social landscape. The research efforts in this project are divided into three main aims: (1) Scaling forensic algorithms to meet big data challenges, (2) Scaling forensic algorithms to handle complex forgeries, and (3) Scaling forensics to meet increased adversarial capabilities. To accomplish these aims, this research will draw upon results from a wide variety of fields such as signal processing, estimation theory, statistical hypothesis testing, machine learning, optimization theory, and game theory.

DREXEL UNIVERSITY Cybersecurity Institute

Funded research project profile: **NSF CAREER (R. Greenstadt)**

Project title	CAREER: Privacy Analytics for End-Users in a Big Data World
Funding agency	National Science Foundation
Program	Faculty Early Career Development Program (CAREER)
Investigator	Rachel Greenstadt (PI)
Dates	February, 2013 – January, 2018
Award #	CNS-1253418
Link	`http://www.nsf.gov/awardsearch/showAward?AWD_ID=1253418`

R. Greenstadt

Research summary: Increasing amounts of data are being collected about users, and increasingly sophisticated analytics are being applied to this data for various purposes. Privacy analytics are machine learning and data mining algorithms applied by end-users to their data for the purpose of helping them manage both private information and their self-presentation. This research develops privacy analytics that help users answer three interconnected questions about their online persona (1) What data does the user consider sensitive, and in what contexts should one share it?; (2) What does the data say about the user; and (3) Who knows what? These privacy analytics introduce a novel, inverse data mining problem where users analyze their data to estimate the conclusions the data will produce when incorporated into larger data sets. This project designs new algorithms for quantitative and automated methods to detect privacy-related phenomena that have been observed qualitatively. These algorithms support the development of usable privacy enhancing technologies and will give users tools to cope with and manage their data in a complicated data environment. These tools will provide awareness to users about how their data is being used. These analytics will also help answer questions critical to the development of privacy law and policy.

This work involves approximately twenty-five undergraduates in research activities, exposing them to research methods and privacy issues. This project also develops novel educational materials including course offerings for an interdisciplinary master's program in security and educational tools for use by the general public to bridge the digital divide.

DREXEL UNIVERSITY Cybersecurity Institute

Funded research project profile: **NSF-SaTC (S. Weber)**

Project title	TTP: Medium: Securing the Wireless Philadelphia Network
Funding agency	National Science Foundation
Program	Secure and Trustworthy Computing Program (NSF-SaTC)
Investigators	Steven Weber (PI)
	Spiros Mancoridis
	Harish Sethu
	Kapil R. Dandekar
Dates	September, 2012 – August, 2016
Award #	CNS-1228847
Link	`http://www.nsf.gov/awardsearch/showAward?AWD_ID=1228847`


S. Weber


S. Mancoridis


H. Sethu


K.R. Dandekar

Research summary: The Wireless Philadelphia Network (WPN) is a metropolitan area network (MAN) consisting of thousands of Tropos 5210 wireless mesh routers distributed across the entire city of Philadelphia and connected by a fiber backbone. This project is employing this network as a testbed to investigate three diverse security challenges facing any large-scale wireless network servicing a heterogeneous population. The first challenge is in efficient network anomaly detection algorithms, and the proposed solution is to investigate the efficacy of both compressive sampling and distributed source coding based approaches in reducing the amount of data that must be transmitted to the anomaly detector. The second challenge is physical layer security in wireless networks, and the proposed solution is to use physical layer based encryption algorithms and user authentication. The third challenge is anomaly detection at the application layer, in particular for web servers, and the proposed solution is to develop software sensors on the hardware, operating system, virtual machine, and application server, and develop rules for identifying possible anomalies using these metrics. Besides the intellectual merit of these challenges, the project has several broader impacts. First, low-income residents gain Internet access through integration with the Freedom Rings Partnership. Second, students participate in community service based engineering design projects. Finally, curricular enhancements and the recruitment of women and minority graduate students improve the educational and diversity missions at our university.

DREXEL UNIVERSITY Cybersecurity Institute

Funded research project profile: **NSF-SFS (K.R. Dandekar)**

Project title	Capacity building: Development and dissemination of the Drexel University cybersecurity program
Funding agency	National Science Foundation
Program	CyberCorps Scholarship for Service Program (NSF-SFS)
Investigators	Kapil R. Dandekar (PI) Constantine Katsinis Steven Weber Chris Yang Rachel Greenstadt
Dates	November, 2012 – October, 2015
Award #	DUE-1241631
Link	`http://www.nsf.gov/awardsearch/showAward?AWD_ID=1241631`


K.R. Dandekar


C. Katsinis


S. Weber


C. Yang


R. Greenstadt

Research summary: The new interdisciplinary Master of Science in Cybersecurity degree program at Drexel University is educating a new breed of engineers and scientists trained to initiate and participate in multi-disciplinary and team-based research projects. The program is developing a new interdisciplinary cybersecurity curriculum, leveraging Drexel's National Security Agency (NSA) Center of Academic Excellence in Information Assurance Education along with faculty expertise from the Drexel College of Engineering, Goodwin College of Professional Studies, and the College of Information Sciences and Technology. The program is defined not only by the development of new courses, but also by minority student recruitment, integration of cooperative education, continuing education for both students and faculty, and the integration of research and teaching. The program addresses workforce driven needs as identified by the NSA to increase the number of graduates with deep technical cyber-skills. Teams of students participate in the innovative rotation-based research program, inspired by rotations in medical school, working on research projects in multiple sub-disciplines, cutting across conventional college/departmental barriers and traditional research groups. Students in the program also participate in Cybersecurity-related co-op opportunities and community service projects. Both the co-op program and the community service projects leverage on-going activities at Drexel. Drexel University serves as the lead institution of a consortium of universities as part of the Greater Philadelphia Region Louis Stokes Alliance for Minority Participation. The project uses these connections to help with student recruitment and dissemination of Cybersecurity-related teaching materials.

DREXEL UNIVERSITY
Cybersecurity Institute

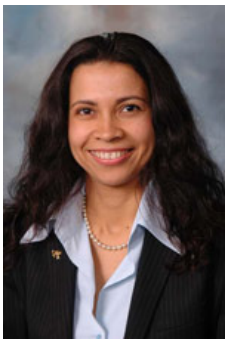
Funded research project profile: **ONR (K.R. Dandekar)**

Project title	Secure wireless control for future naval smart grids
Funding agency	Office of Naval Research (ONR)
Investigators	Kapil R. Dandekar (PI) Steven Weber Chikaodinaka Nwankpa Jaudelice de Oliveira Karen Miu Miller
Dates	November, 2015 – December, 2018
Award #	N000141612037


K.R. Dandekar


S. Weber


C. Nwankpa


J. de Oliveira


K. Miu

Research summary: There has been ongoing interest in installing and operating wireless networks aboard ships to realize communication and control functions. Unlike traditional wired networks, wireless communication can easily augment connectivity in existing spaces with relatively low cost and little disruption to the structure or watertight integrity of the bulkheads. Wireless networks have been proposed for monitoring, controlling and automating many operations aboard ships, particularly in engineering spaces. One of the key trends in the new approach to naval control system design is increased system automation through intelligent distributed systems. For example, maintaining power flow to vital loads following large scale fluctuations or component failure(s) is a central goal of power system management including electric shipboard distribution systems. While the increased level of automation reduces manning and enhances overall system reliability, it also requires complex communications infrastructure. This infrastructure presents new survivability concerns. Hardwired communication networks using copper wire or optical fiber are prone to failure when the ship sustains damage, and their installation and maintenance are costly and complex. A natural alternative that addresses both installation cost and survivability issues is to use wireless communication networks where possible. The use of wireless systems in naval applications raises several concerns, however. In the on-ship environment, there are potentially numerous sources of electromagnetic shielding (metallic bulkheads, equipment enclosures) and interference that could render an otherwise properly designed wireless system inoperable. Additionally, these networks are more vulnerable to security (i.e., eavesdropping and intrusion) and performance (i.e., data throughput, latency, and packet loss) issues.

DREXEL UNIVERSITY Cybersecurity Institute

Funded research project profile: **NSF (C. Yang)**

Project title	CIF21 DIBBs: DIBBs for Intelligence and Security Informatics Research Community
Funding agency	National Science Foundation
Program	Division Of Advanced Cyber Infrastructure (ACI)
Investigators	Hsinchun Chen (U. Arizona) (PI) Catherine Larson (U. Arizona) Mark Patton (U. Arizona) Chris Yang
Dates	October, 2014 – September, 2017
Award #	ACI-1443019
Link	


H. Chen


C. Larson


M. Patton


C. Yang

Research summary: The growing number of cyber attacks on the Internet and other critical infrastructure has led to an increased sense of urgency in developing a better understanding of the motivation and methods behind such incursions. This project develops a research infrastructure for the Intelligence and Security Informatics (ISI) community comprised of experts across the computer, information, and social sciences.

The infrastructure consists of online archives and analysis tools. The archives contain a wide array of open source data including: discussions in online forums run by hackers, data from botnet command and control servers used to stage computer attacks, video streams and tweets and news summaries from economically and politically unstable states and regions. The analysis tools developed for this project support a range of research investigations. The social network analysis tool allows researchers to study how organizations form and how people interact with one another both virtually and in person. The data visualization tools are important for helping researchers pick out important patterns and trends in large sets of data of different types and from disparate sources. A new tool for adversarial data mining and deception detection allows researchers to deepen their enquiries and analysis of the intentions behind cyber-attacks.

Integrating these divergent data sources allows the security research community to more easily collaborate with other members of the community, rapidly test hypotheses, evaluate detection techniques, track down malicious actors, and identify weaknesses in a cyberinfrastructure network.

DREXEL UNIVERSITY
Cybersecurity Institute

Funded research project profile: **Comcast (S. Mancoridis)**

Project title	Machine learning and big data analytics
Funding agency	Comcast and the University of Connecticut
Program	Center of Excellence for Security Innovation (CSI)
Investigators	Spiros Mancoridis (PI)
	Harish Sethu
	Naga Kandasamy
	Steven Weber
Dates	January, 2015 – December, 2016


S. Mancoridis


H. Sethu


N. Kandasamy


S. Weber

Research summary: Computing infrastructure continues to grow in both size and complexity, illustrated by recent trends including the rise of ultra-large-scale (ULS) systems. Due to their size and complexity, ULS systems present challenges in their design, evolution, orchestration, control, and monitoring. Monitoring is especially important for assessing the overall health of such systems to ensure their reliability and security. Three important problems in health monitoring are (1) determining user quality of experience (QoE), (2) detecting anomalies caused by changes in usage patterns or fault conditions, and (3) detecting malicious usage of the system.

The scale, heterogeneity, and distributed nature of ULS systems present challenges to effective monitoring. First, due to the scale of ULS systems, monitoring solutions typically produce large, multidimensional datasets. The high-dimensionality of the datasets, combined with the rate at which the data are collected, necessitate the use of processing and analysis techniques designed specifically for large datasets. Feature selection techniques such as recursive feature elimination (RFE) can be used to identify the smallest subset of sensors of features necessary for effective monitoring. Feature reduction techniques such as principal component analysis (PCA) and independent component analysis (ICA) can be used to reduce the dimensionality of the data to aid in processing.

The heterogeneity of the software and hardware subsystems in a ULS system present another set of challenges. Dithering software and hardware configurations place constraints on the types of data that can be monitored at each subsystem and the mechanisms that can be used for data collection. For example, data collected from servers can include operating system and application performance monitors, hardware sensors, system call traces, and security audit data. At the network level, data can be collected through deep packet inspection or at the network flow level.

The distributed nature of ULS systems complicate the collection of data at a centralized location. The centralized collection of data is desirable because leveraging data from multiple sources often provides better detection than is possible in a decentralized architecture. However, the network overhead incurred in transmitting the data is undesirable. Techniques for compressing, sampling, and quantizing the data can be used to enable centralized detection while minimizing network overhead.