DREXEL UNIVERSITY

Isaac L. Auerbach Cybersecurity Institute

Institute Overview

Author: Steven Weber, Director
Jiho Yoo, Institute Student Coordinator

Date: September 22, 2017

September 22, 2017

This overview of the Isaac L. Auerbach Cybersecurity Institute (ILACI) provides an in-depth view of the state of the art cybersecurity research, cybersecurity teaching, and cybersecurity community engagement being conducted by our world-class faculty.

To briefly summarize our capabilities, I've chosen to focus this cover letter on the relevance, innovation, and breadth of Drexel cybersecurity research, although our cybersecurity educational programs and cybersecurity community engagement have been no less impactful.

Relevance. One measure of research impact is the diversity of funding sources supporting Drexel's cybersecurity research and innovation: Drexel research is clearly in alignment with the cybersecurity research priorities of both government and corporate funding agencies. Recent government funding sources include

1. National Science Foundation Secure and Trustworthy Computing (SaTC) - 2012–2016
2. National Science Foundation Division of Advanced Cyber Infrastructure (ACI) - 2014–2017
3. National Science Foundation Cybercorps Scholarships for Service (SFS) - 2012–2015
4. NSF Faculty Early Career Development Program (CAREER) - 2013–2018, 2016–2020
5. Defense Forensics and Biometrics Agency (DFBA) - 2015–2016
6. Defense Advanced Research Projects Agency (DARPA) Active Authentication Program - 2012–2013
7. Defense Advanced Research Projects Agency (DARPA) Integrated Cyber Analysis System (ICAS) Program - 2013–2014
8. Office of Naval Research (ONR) - 2015–2018
9. Air Force Research Labs (AFRL) - 2011–2014
10. National Security Agency (NSA) - 2013–2015
11. Department of Justice (DoJ), Office of Justice Programs, Bureau of Justice Assistance - 2012–2013
12. Department of Justice (DoJ) and the National Institute of Justice (NIJ) - 2009–2011

Innovation. The innovativeness of Drexel's research is evident from the prestigious and broad collection of journals and conferences in which our work is published. Recent conference venues include

1. 2017 IEEE Wireless Communications and Networking Conference (WCNC)
2. 2016,2017 Conference on Information Sciences and Systems (CISS)
3. 2017 IEEE Transactions on Information Forensics and Security
4. 2017 IEEE Transaction on Computer
5. 2016 IEEE International Symposium on Circuits and Systems (ISCAS)
6. 2016 IEEE Systems Journal
7. 2016 IEEE/ACM Great Lake Symposium on VLSI (GLSVLSI)
8. 2015 IEEE International Workshop on Information Forensics and Security (WIFS)
9. 2015 Usenix Security Symposium
10. 2015 Information Security Solutions Europe (ISSE)
11. 2015,2017 International Conference on Malicious and Unwanted Software (MALCON)
12. 2015 International Conference on Quality, Reliability, and Security (QRS)
13. 2015 IEEE International Symposium on Software Reliability Engineering (ISSRE)
14. 2014 ACM SIGCOMM Software Radio Implementation Forum (SRIF)
15. 2014 ACM Conference on Data and Application Security and Privacy (CODASPY)

Recent journal publications include the *IEEE Systems Journal*, the *ASIS Security Journal*, and the *IEEE Transactions on Information Forensics and Security*.

Two recent examples of Drexel faculty leadership in the cybersecurity research communities include *i*) Matthew Stamm served as general chair of the June, 2017 ACM Workshop on Information Hiding and Multimedia Security and *ii*) Rachel Greenstadt served as a co-editor in Chief of the Proceedings on Privacy Enhancing Technologies and a program chair of the Privacy Enhancing Technologies Symposium.

Breadth. Cybersecurity research today is a far cry from its original focus on network protocols and cryptography. Today's cybersecurity challenges require an incredibly diverse collection of interdisciplinary approaches, including machine learning, big data, signal processing, algorithm design, computer hardware and software, biometrics, and many others. The scope of research topics pursued by Drexel's cybersecurity faculty illustrates this diversity. A brief list of topics includes

1. Cyber crime and online identity theft (Anandarajan and D'Ovidio)
2. Adversarial stylometry (Greenstadt)
3. Sentiment analysis and security informatics (Yang)
4. Network and host anomaly detection (Sethu, Kandasamy, Mancoridis, Weber)
5. Biometric user authentication (Greenstadt and Weber)
6. Media forensics and anti-forensics (Stamm)
7. Wireless jamming and key generation (Dandekar)
8. Hardware security and trust (Savidis, Taskin, Stamm),
9. Malware detection, classification, and mitigation (Mancoridis and Balduccini)

As evident in the following pages, Drexel faculty are developing solutions to address the cybersecurity challenges of both today and tomorrow. Please feel free to contact us.

Steven P. Weber

Steven Weber
Director, Isaac L. Auerbach Cybersecurity Institute

Contents

1 Mission Statement

The mission statement of the Drexel Isaac L. Auerbach Cybersecurity Institute is:

> To establish Drexel University as a leading institution with regard to cybersecurity research, education, and community engagement.

2 Governance

The ILACI is advised internally by the ILACI Members Council, the members of which are shown in Fig. 1. The council includes representations from the five Drexel colleges and schools deemed to have the greatest interest in Drexel cybersecurity:

1. College of Computing and Informatics (CCI, represented by Spiros Mancoridis and Ali Shokoufandeh)
2. College of Engineering (CoE, represented by Kapil Dandekar)
3. College of Arts and Sciences (CoAS, represented by Rob D'Ovidio)
4. LeBow College of Business (represented by Murugan Anandarajan)
5. Thomas R. Kline School of Law (represented by Daniel Filler)

The ILACI Director, Steven Weber, reports directly to the Senior Vice Provost for Research, Aleister Saunders, who also sits on the Members Council.

Aleister Saunders
Senior Vice Provost for Research

Murugan Anadarajan
Department Head of Management, Decision Science & MIS
LeBow College of Business

Kapil R. Dandekar
Associate Dean of Research and Graduate Studies
College of Engineering

Rob D'Ovidio
Associate Dean for Humanities & Social Science Research & Graduate Education
College of College of Arts and Sciences

Daniel Filler
Dean
Thomas R. Kline School of Law

Spiros Mancoridis
Technical Fellow
Isaac L. Auerbach Cybersecurity Institute

Ali Shokfoufandeh
Senior Associate Dean of Research
College of Computing and Informatics

Steven Weber
Director
Isaac L. Auerbach Cybersecurity Institute

Figure 1: The ILACI Members Council.

The ILACI is advised externally by the ILACI Senior Advisory Board, the members of which are shown in Fig. 2. This group held its inaugural meeting on March 10, 2015, in an all-day meeting on the Drexel University campus.

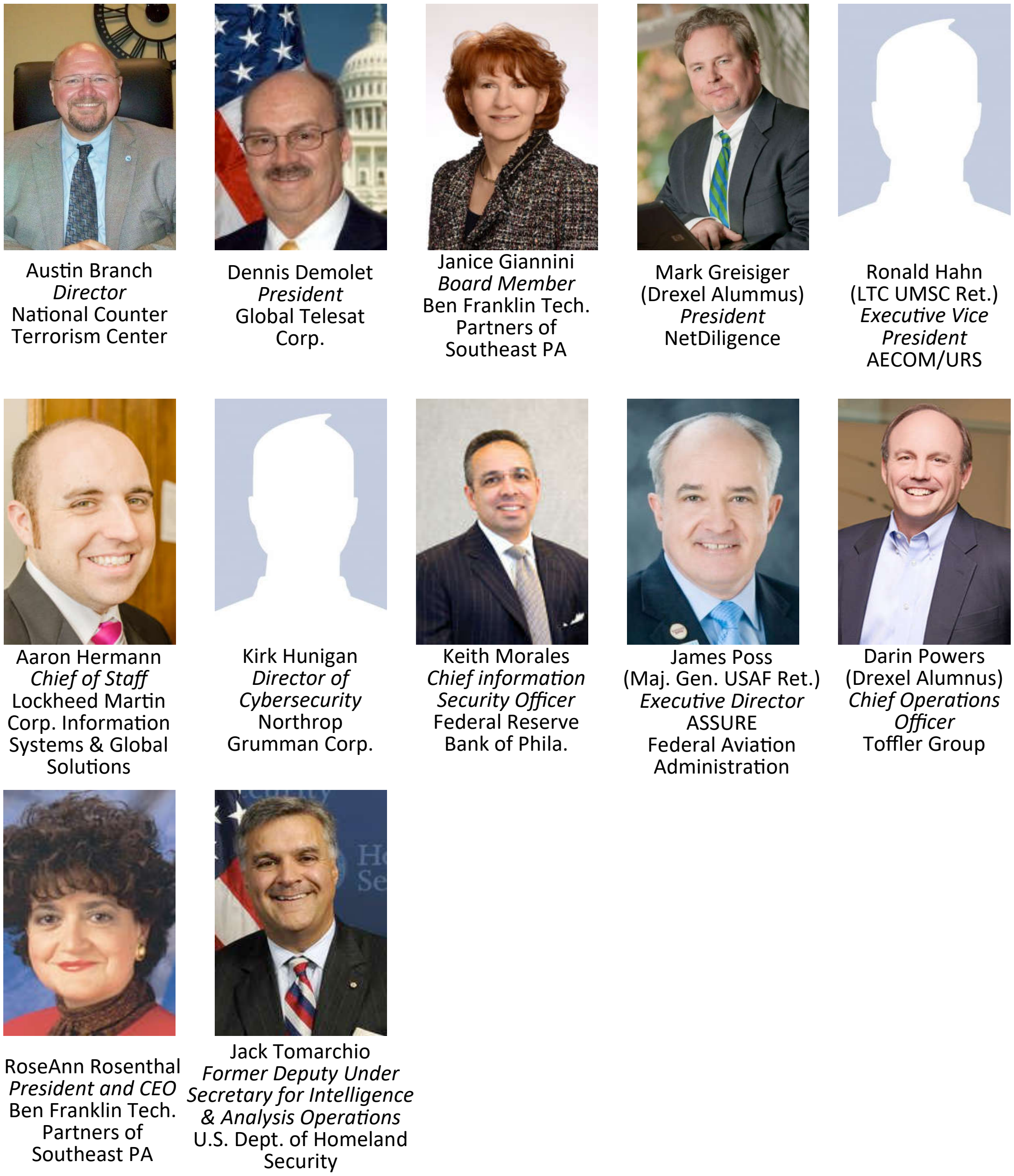


Figure 2: The ILACI Senior Advisory Board (as of July, 2017).

3 Faculty Affiliates

To date nineteen (19) Drexel faculty from across the university have affiliated with the ILACI, representing cybersecurity research and teaching excellence in

1. College of Computing and Informatics (CCI)
2. College of Engineering (CoE)
3. College of Arts and Sciences (CoAS)
4. LeBow College of Business

The faculty are listed with their corresponding cybersecurity keywords in Table 1, their pictures are shown in Fig. 3, and their academic titles, affiliations, and positions are listed in Table 2.

Murugan Anandarajan	*data mining and identity theft; text mining; predictive modeling; cyber deviant behavior*
Kapil Dandekar	*wireless security; reactive jamming; wireless penetration testing; visualization*
Rob D'Ovidio	*intersection of computer technology, crime, and the criminal justice system*
David Gefen	*trust management systems; behavioral effects of fraud; privacy management*
Christopher Geib	*computer network security*
Rachel Greenstadt	*privacy & security of multi-agent systems; economics of electronic privacy & information security*
Nagarajan Kandasamy	*network anomaly detection*
Constantine Katsinis	*computer security; network security; information assurance*
Geoffrey Mainland	*program analysis; anomaly detection*
Spiros Mancoridis	*malware detection, classification, and mitigation; software security; reverse engineering; code analysis*
Gaurav Naik	*mobile network security; computer network security*
Ioannis Savidis	*hardware security; Trojan detection and mitigation; gate level logic encryption; side-channel analysis; circuit-level intellectual property protection; design for trust*
Harish Sethu	*web security and privacy; network anomaly detection*
James Shackleford	*runtime code injection; virtual address space manipulation; transparent library redirection*
Matthew Stamm	*information security; multimedia forensics and anti-forensics; information verification*
Baris Taskin	*hardware security; hardware/software co-design for exascale system performance*
Kristene Unsworth	*surveillance; national security policy*
Steven Weber	*network performance; statistical analysis; anomaly detection; security overhead analysis*
Christopher Yang	*security informatics; information sharing and privacy; sentiment analysis*

Table 1: The ILACI Faculty Affiliates and their cybersecurity keywords.

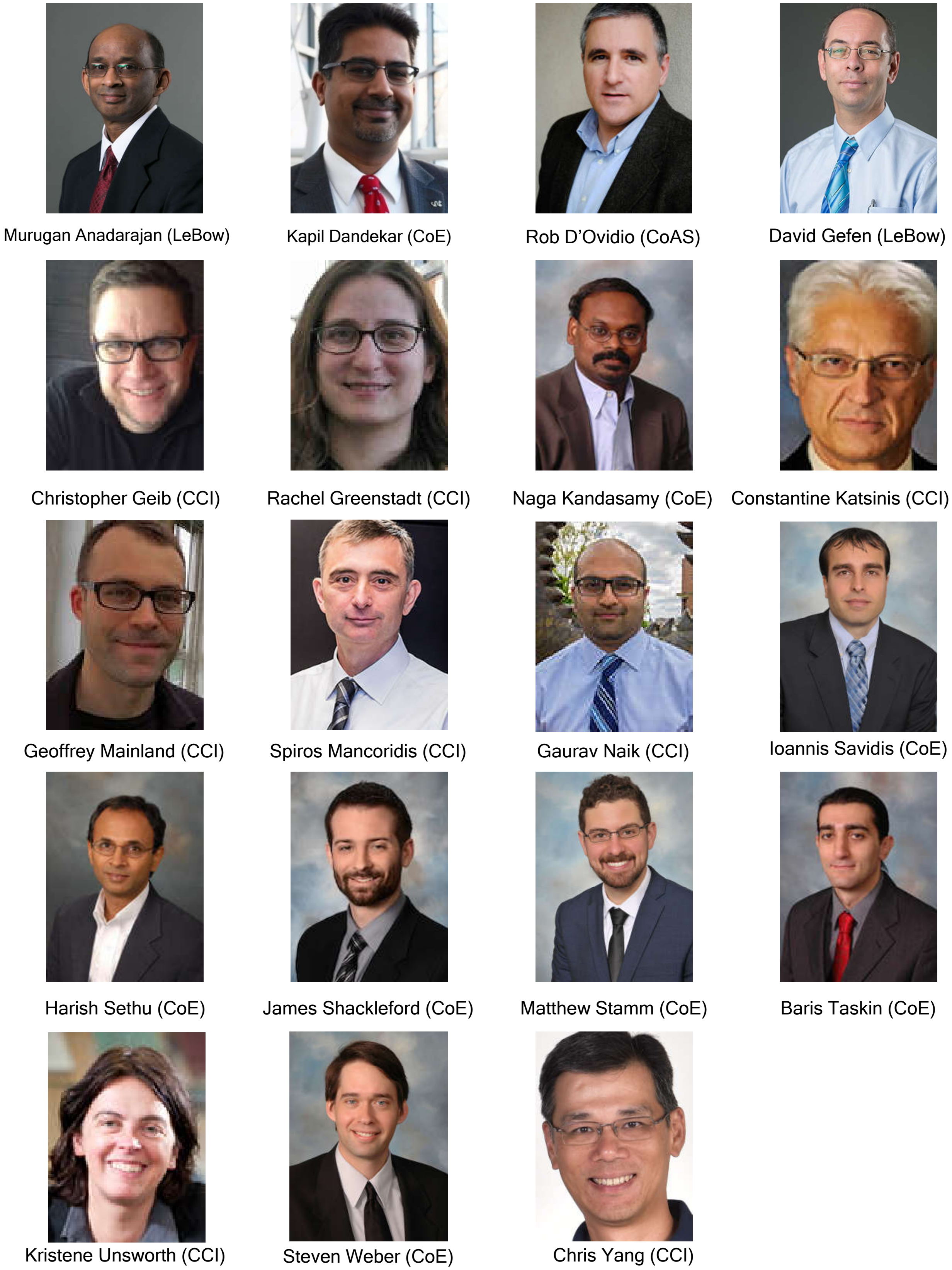


Figure 3: The ILACI Faculty Affiliates.

Murugan Anandarajan	*Professor and Department Head*, Departments of Management, Decision Sciences & MIS, LeBow College of Business
Kapil Dandekar	*Professor*, Department of Electrical and Computer Engineering; *Associate Dean of Research and Graduate Studies*, College of Engineering. *Director*, Drexel Wireless Systems Laboratory (DWSL)
Rob D'Ovidio	*Associate Professor*, Department of Criminology and Justice Studies; *Associate Dean for Humanities and Social Science Research and Graduate Education*, College of Arts and Sciences
David Gefen	*Professor and Provost Distinguished Research Professor*, Department of Decision Sciences and MIS, LeBow College of Business
Christopher Geib	*Associate Professor*, Department of Computer Science, College of Computing and Informatics
Rachel Greenstadt	*Associate Professor*, Department of Computer Science, College of Computing and Informatics. *Director*, Privacy, Security and Automation Lab (PSAL)
Nagarajan Kandasamy	*Profesor and Associate Department Head of Graduate Affairs*, Department of Electrical and Computer Engineering, College of Engineering
Constantine Katsinis	*Associate Teaching Professor*, Department of Computer Science, College of Computing and Informatics
Geoffrey Mainland	*Assistant Professor*, Department of Information Science, College of Computing and Informatics
Spiros Mancoridis	*Isaac L. Auerbach Technical Fellow*, Department of Computer Science; *Interim Dean*, College of Computing and Informatics
Gaurav Naik	*Assistant Research Professor*, Department of Computer Science, College of Computing and Informatics
Ioannis Savidis	*Assistant Professor*, Department of Electrical and Computer Engineering, College of Engineering. *Director*, Integrated Circuits and Electronics (ICE) Design and Analysis Laboratory
Harish Sethu	*Associate Profesor*, Department of Electrical and Computer Engineering, College of Engineering
James Shackleford	*Assistant Professor*, Department of Electrical and Computer Engineering, College of Engineering
Matthew Stamm	*Assistant Professor*, Department of Electrical and Computer Engineering, College of Engineering. *Director*, Multimedia and Information Security Laboratory (MISL)
Baris Taskin	*Profesor*, Department of Electrical and Computer Engineering, College of Engineering. *Director*, Drexel VLSI and Architecture Laboratory
Kristene Unsworth	*Assistant Professor*, Department of Information Science, College of Computing and Informatics
Steven Weber	*Professor*, Department of Electrical and Computer Engineering, College of Engineering; *Director*, Drexel Cybersecurity Institute. *Director*, Drexel Modeling and Analysis of Networks Laboratory (MANLab)
Christopher Yang	*Associate Professor*, Department of Information Science, College of Computing and Informatics

Table 2: The ILACI Faculty Affiliates and their academic titles, affiliations, and positions.

Faculty profile: **Murugan Anandarajan, Ph.D.**

Title	Professor
College	LeBow College of Business
Department	Management, Decision Sciences & MIS
Position	Department Head
Email	ma33@drexel.edu
Phone	(215) 895-6212
University page	http://www.lebow.drexel.edu/people/murugananandarajan

Research/teaching keywords: text analytics; visual analytics; protection motivation theory.

Cybersecurity expertise: data mining and identity theft; text mining; predictive modeling; cyber deviant behavior.

Background: my research focuses on safeguarding consumers and organizations against cyber crime through mechanisms such as behavior modification and policy.

Publications:

[1] Rob D'Ovidio, Murugan Anandarajan, and Irv Schlanger. Patrons Beware: Security Vulnerabilities and Public Access Internet Facilities. *ASIS Security Journal*, (in press) 2015.

[2] Murugan Anandarajan and Irina-Marcela Nedelcu. Self-protecting the smartphone: A motivational model. *Proceedings of the Northeast Decision Sciences Institute Annual Conference (DSI)*, Baltimore, MD, April 2015.

[3] Alexander Jenkins, Murugan Anandarajan, and Rob D'Ovidio. 'All that Glitters is not Gold': The Role of Impression Management in Data Breach Notification. *WSCA Western Journal of Communication*, 78(3):337–357, May 2014.

[4] Murugan Anandarajan, Rob D'Ovidio, and Alexander Jenkins. Safeguarding consumers against identity-related fraud: examining data breach notification legislation through the lens of routine activities theory. *Oxford Journal of International Data Privacy Law*, 3(1):51–60, March 2013.

[5] Murugan Anandarajan, Narasimha Paravasta, Bay Arinze, and Rob D'Ovidio. Online Identity Theft: A Longitudinal Study of Individual Threat-Response and Coping Behaviors. *Journal of Information System Security*, 8(2):43–69, February 2012.

[6] Irv Schlanger, Rob D'Ovidio, and Murugan Anandarajan. Whos watching the net: The risk of victimization with public access wifi. *Department of Defence Cyber Crime Conference*, St. Louis, MO, January 2010.

Research funding:

[1] Murugan Anandarajan and Rob D'Ovidio. Cyber crime and forensics institute expansion of services. *United States Department of Justice, National Institute of Justice*, 2010–. $500,000.

[2] Murugan Anandarajan and Rob D'Ovidio. Cyber crime and computer forensics research. *United States Department of Justice*, 2009–. $500,000.

[3] Murugan Anandarajan and Rob D'Ovidio. Cyber crime and computer forensics research. *National Institute of Justice*, 2008–. $223,250.

Faculty profile: **Kapil R. Dandekar, Ph.D.**

Title	Professor
College	Engineering
Department	Electrical and Computer Engineering
Position	Associate Dean of Research and Graduate Studies – College of Engineering
Research Lab	Drexel Wireless Systems Laboratory (DWSL)
Email	dandekar@coe.drexel.edu
Phone	(215) 895-2228
University page	http://drexel.edu/ece/contact/faculty-directory/DandekarKapil/
Lab page	http://wireless.ece.drexel.edu

Research/teaching keywords: wireless communications; antenna design; software defined radio.

Cybersecurity expertise: wireless security; reactive jamming; wireless penetration testing; visualization.

Background: The central philosophy of the Drexel Wireless Systems Laboratory (DWSL) is to take a systems-centric view of new and emerging wireless technologies using a combination of interdisciplinary research and hardware prototyping. In the context of cybersecurity, DWSL has developed and built systems leveraging new antenna technologies to implement physical layer based encryption key generation, user authentication, and reactive jamming. DWSL is also using techniques from gaming and mobile augmented reality to develop and visualize cybersecurity based educational programs.

Publications:

[1] J. Chacko, K. Juretus, M. Jacovic, C. Sahin, N. Kandasamy, I. Savidis, and K. Dandekar. Securing wireless communication through physical layer key based packet obfuscation. *IEEE Transaction on Computers*, 2017.

[2] Cem Sahin, Brandon Katz, and Kapil Dandekar. Secure and robust symmetric key generation using physical layer techniques under various wireless environments. *2016 IEEE Radio and Wireless Symposium (RWS)*, 2016.

[3] Cem Sahin, Danh Nguyen, James Chacko, and Kapil R. Dandekar. Cybersecurity education: taking research into the classroom. *Frontiers in Education (FIE) Conference*, El Paso, TX, October 2015.

[4] Danh Nguyen, Cem Sahin, Boris Shishkin, Nagarajan Kandasamy, and Kapil R. Dandekar. A real-time and protocol-aware reactive jamming framework built on software-defined radios. *Proceedings of the ACM SIGCOMM Software Radio Implementation Forum (SRIF)*, Chicago, IL, August 2014.

[5] Nikhil Gulati, Rachel Greenstadt, Kapil R. Dandekar, and John M. Walsh. GMM based semi-supervised learning for channel-based authentication scheme. *Proceedings of the 7th IEEE Fall Vehicular Technology Conference (VTC)*, Las Vegas, NV, September 2013.

[6] Prathaban Mookiah and Kapil R. Dandekar. A reconfigurable antenna-based solution for stationary device authentication in wireless networks. *Hindawi International Journal of Antennas and Propagation*, 2012.

Research funding:

[1] Steven Weber (PI), Kapil Dandekar, Ioannis Savidis, and Matthew Stamm. Security by design: Drexel hands-on cybersecurity laboratory curriculum. *NSA-CNAP*, October 1, 2017 – September 30, 2018. $255,359.93.

[2] Kapil Dandekar (PI), Stefan Rank, Pramod Abichandani a nd Nagarajan Kandasamy, and Jennifer S. Standford. Satc: Edu: Software defined radio wars for cybersecurity and information assurance education. *National Science Foundation*, September, 2017 – August 2019. $299,888.

[3] Kapil R. Dandekar (PI), Jaudelice C. de Oliveira, Karen Miu Miller, Chikaodinaka Nwankpa, and Steven Weber. Secure wireless control for future naval smart grids. *Office of Naval Research (ONR)*, N000141612037, November, 2015 – December, 2018. $749,831.

[4] Kapil R. Dandekar (PI), Rachel Greenstadt, Constantine Katsinis, Steven Weber, and Christopher C. Yang. Capacity building: Development and dissemination of the Drexel University cybersecurity program. *National Science Foundation CyberCorps Scholarship for Service Program (NSF-SFS)*, DUE-1241631, November, 2012 – October, 2015. $888,491.

[5] Steven Weber (PI), Kapil R. Dandekar, Spiros Mancoridis, and Harish Sethu. TTP: Medium: Securing the Wireless Philadelphia Network. *National Science Foundation Secure and Trustworthy Cyberspace Program (NSF-SaTC)*, CNS-1228847, September, 2012 – August, 2016. $1,080,800.

[6] Kapil R. Dandekar (PI), Rachel Greenstadt, and John MacLaren Walsh. A framework for wireless network security based on reconfigurable antennas. *National Science Foundation Networking Technology and Systems (NeTS) Program*, CNS-1028608, September, 2010 – August, 2014. $359,506.

[7] Kapil R. Dandekar, Tracy Camp, Zhu Han, and H.V. Poor. NeTS-Medium: Collaborative Research - cooperative beamforming for efficient and secure wireless communications. *National Science Foundation Networking Technology and Systems (NeTS) Program*, CNS-0905425, September, 2009 – August, 2012. $199,999 (Drexel award).

Courses taught:

ECES	306	Analog & Digital Communication	ECET	512	Wireless Systems
ECET	890	Software Defined Radio Security Lab			

DREXEL UNIVERSITY
Isaac L. Auerbach
Cybersecurity Institute

Faculty profile: **Rob D'Ovidio, Ph.D.**

Title	Associate Professor
College	Arts and Sciences
Department	Criminology and Justice Studies
Position	Associate Dean for Humanities and Social Science Research and Graduate Education – College of Arts and Sciences
Email	robert.dovidio@drexel.edu
Phone	(215) 895-1803
University page	http://drexel.edu/coas/faculty-research/faculty-directory/dovidio-robert/
Personal page	http://www.pages.drexel.edu/∼rd64/Home.html

Research/teaching keywords: computer and high technology crime; criminal justice technology; criminological theory.

Cybersecurity expertise: intersection of computer technology, crime, and the criminal justice system.

Background: My research and teaching interests lie at the intersection of computer technology, crime, and the criminal justice system. My most recent work looks at the connection between virtual currencies and electronic fraud and the notification process that follows computer network breaches and data thefts. I have received funding from the National Institute of Justice, the Bureau of Justice Assistance, and the U.S. Department of Education to support my research. I am a member of the American Society of Criminology and the Computer Crime and Digital Evidence Committee of the International Association of Chiefs of Police. I provide regular commentary to media outlets on news stories pertaining to computer crime, Internet safety, identity theft, and electronic surveillance.

Publications:

[1] Rob D'Ovidio, Murugan Anandarajan, and Irv Schlanger. Patrons Beware: Security Vulnerabilities and Public Access Internet Facilities. *ASIS Security Journal*, (in press) 2015.

[2] Alexander Jenkins, Murugan Anandarajan, and Rob D'Ovidio. 'All that Glitters is not Gold': The Role of Impression Management in Data Breach Notification. *WSCA Western Journal of Communication*, 78(3):337–357, May 2014.

[3] Murugan Anandarajan, Rob D'Ovidio, and Alexander Jenkins. Safeguarding consumers against identity-related fraud: examining data breach notification legislation through the lens of routine activities theory. *Oxford Journal of International Data Privacy Law*, 3(1):51–60, March 2013.

[4] Ashley Podhradsky, Rob D'Ovidio, Pat Engebretson, and Cindy Casey. Xbox 360: Mapping Investigative Data. *Proceedings of the 4th International Conference on Digital Forensics and Cyber Crime*, Moscow, Russia, September 2013.

[5] Ashley Podhradsky, Rob D'Ovidio, Pat Engebretson, and Cindy Casey. Xbox 360 Hoaxes, Social Engineering, and Gamertag Exploits. *Proceedings of the 46th IEEE Hawaii International Conference on System Sciences (HICSS)*, pages 3239–3250, Maui, Hawaii, January 2013.

[6] Murugan Anandarajan, Narasimha Paravasta, Bay Arinze, and Rob D'Ovidio. Online Identity Theft: A Longitudinal Study of Individual Threat-Response and Coping Behaviors. *Journal of Information System Security*, 8(2):43–69, February 2012.

Research funding:

[1] Rob D'Ovidio (Co-PI) and NAMES. Research and training program to educate stakeholders on crimes committed using handheld devices. *U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance*, 2011-BE-BX-K001, January, 2012 – December, 2013. $986,976 (collaborative project with Drakontas, LLC and BKForensics).

[2] Rob D'Ovidio (Co-PI) and NAMES. Real crimes in virtual worlds and online video game worlds. *U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance*, 2009-D2-BX-K005, January, 2012 – December, 2013. $500,000 (collaborative project with Drakontas, LLC).

Courses taught:

CJS	274	Sex, Violence, and Crime on the Internet	CJS	273	Surveillance, Technology, and the Law
CJS	276	Computer Crime	CJS	366	Technology and the Justice System
CJ	377	Intellectual Property Theft in the Digital Age			

Professional service:

1. *Member*, International Association of Chiefs of Police, Computer Crime and Digital Evidence Committee

Faculty profile: **David Gefen, Ph.D.**

Title	Professor and Provost Distinguished Research Professor
College	LeBow College of Business
Department	Decision Sciences and MIS
Email	gefend@drexel.edu
Phone	(215) 895-2148
University page	http://www.lebow.drexel.edu/people/davidgefen

Research/teaching keywords: information systems (IS) outsourcing; strategic management of IS; database analysis and design; data analysis; ecommerce; online markets; IS implementation; informatics.

Cybersecurity expertise: trust management systems; behavioral effects of fraud; privacy management.

Background: I teach IS outsourcing, strategic management of information systems, databases, statistical programming, and research methodology. I have published extensively in the top tier journals about IS outsourcing management, online markets, information systems implementation management, and informatics. I was one of the senior editors at MISQ, the leading academic journal in the MIS discipline, and am on the editorial board of JMIS. Before becoming an academic I was a chief programmer and systems analyst, and then senior manager of a large logistics information system.

Publications:

[1] David Gefen and Erran Carmel. Why the first provider takes it all: The consequences of a low trust culture on pricing and ratings in online sourcing markets. *European Journal of Information Systems*, pages 604–618, Winter 2013.

[2] David Gefen and P.A. Pavlou. The boundaries of trust and risk: The quadratic moderating role of institutional structures. *Information Systems Research*, 23:940–959, November 2012.

[3] David Gefen, Simon Wyss, and Yossi Lichtenstein. Business familiarity as risk mitigation in software development outsourcing contracts. *Management Information Systems Quarterly*, 32:531–551, September 2008.

[4] David Gefen and Erran Carmel. Is the world really flat? a look at offshoring in an online programming marketplace. *Management Information Systems Quarterly*, 32:367–384, June 2008.

[5] P.A. Pavlou and David Gefen. Psychological contract violation in online marketplaces: Antecedents, consequences, and moderating role. *Information Systems Research*, 16:372–399, August 2005.

[6] P.A. Pavlou and David Gefen. Building effective online market places with institution based trust. *Information Systems Research*, 15:37–59, September 2004.

[7] David Gefen. What makes ERP implementation relationships worthwhile: Linking trust mechanisms and ERP usefulness. *Journal of Management Information Systems*, 21:275–301, September 2004.

[8] David Gefen and Arik Ragowsky. A multi-level approach to measuring the benefits of an ERP system in manufacturing firms. *Information Systems Management*, 22:18–25, January 2004.

[9] David Gefen, E. Karahanna, and Detmar W. Straub. Trust and TAM in online shopping: An integrated model. *Management Information Systems Quarterly*, 27:51–90, September 2003.

Research funding:

[1] David Gefen (PI), Frances Cornelius, Jennifer Taylor, Noreen Robertson, and Murugan Anadarajan. Applying and improving latent semantic analysis to extract insight from claims and EMR documents. *Drexel University Provost Award*, November 2015. $20,000.

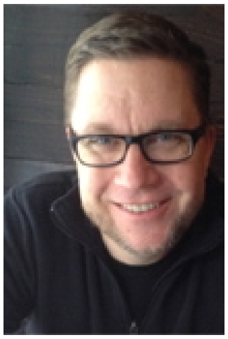
[2] Dominic Gullo (PI), David Gefen, and Michel Miller. Risk, resiliency and protective factors: Building a bioecological model for understanding school readiness and social competence in young children. *Drexel University Social Science Research Fund*, November 2013. $20,000.

Courses taught:

MIS	633	Predictive Business Analytics with Relational Database Data
MIS	634	Advance Programming in SAS
STAT	990	Multivariate II, Covariate based Structured Equation Modeling
MIS	651	IS Outsourcing Management

Faculty profile: **Christopher Geib, Ph.D.**

Title	Associate Professor
College	Computing and Informatics
Department	Computer Science
Email	cwg33@drexel.edu
Phone	(215) 571-4533
University page	http://drexel.edu/cci/contact/Faculty/Geib-Christopher/
Personal page	https://dl.dropboxusercontent.com/u/4326974/Site/Homepage.html



Research/teaching keywords: decision making and reasoning under conditions of uncertainty; planning; scheduling; constraint-based reasoning; human-computer and robot interaction; probabilistic reasoning; process control; user interfaces.

Cybersecurity expertise: computer network security.

Background: My research focuses broadly on decision making and reasoning about actions under conditions of uncertainty. I have worked in planning, scheduling, constraint based reasoning, human computer and robot interaction and probabilistic reasoning. My recent research focus has been on probabilistic intent recognition through weighted model counting and planning based on grammatical formalisms. This has been applied to computer network security, assistive systems and human robot interaction.

Courses taught:

INFO	108	Foundations of Software	INFO	336	Distributed Network Security
CS	380	Artificial Intelligence	CS	510	Introduction to Artificial Intelligence

Faculty profile: **Rachel Greenstadt, Ph.D.**

Title	Associate Professor
College	Computing and Informatics
Department	Computer Science
Research Lab	Privacy, Security and Automation Lab (PSAL)
Email	greenstadt@gmail.com
Phone	(215) 895-2920
University page	http://drexel.edu/cci/contact/Faculty/Greenstadt-Rachel/
Personal page	https://www.cs.drexel.edu/∼greenie/
Lab page	https://psal.cs.drexel.edu/

Research/teaching keywords: artificial intelligence; privacy; security; multi-agent systems.

Cybersecurity expertise: privacy & security of multi-agent systems; economics of electronic privacy & information security.

Background: My lab – the Privacy, Security, and Automation Laboratory (PSAL) – focuses on designing more trustworthy intelligent systems that act autonomously and with integrity, so that they can be trusted with important data and decisions. The lab takes a highly interdisciplinary approach to this research, incorporating ideas from artificial intelligence, psychology, economics, data privacy, and system security. However, a common thread of this work has been studying information flow, trustworthiness, and control. Recently, much of PSAL's work has focused on using machine learning to better understand textual communication.

Publications:

[1] B. Alsulami, E. Dauber, R. Harang, S. Mancoridis, and R. Greenstadt. Source code authorship attribution using long short-term memory based networks. *European Symposium on Research in Computer Security (ESORICS)*, 2017.

[2] E. Dauber, R. Overdorf, and R. Greenstadt. Stylometric authorship attribution of collaborative documents. *International Symposium on Cyber Security, Cryptography, and Machine Learning (CSCML)*, 2017.

[3] A. Forte, N. Andalibi, and R. Greenstadt. Privacy, anonymity and perceived risk in open collaboration: A study of tor users and wikipedians. *Proceedings of Compute-Supported Cooperative Work and Social Computing (CSCW)*, Portland, OR, 2017.

[4] R. Overdorf and R. Greenstadt. Blogs, twitter feeds, and reddit comments: Cross-domain authorship attribution. *Proceedings on Privacny Enhancing Technologies*, Vol 2016(Issue 3), 2016.

[5] Aylin Caliskan-Islam, Richard Harang, Andrew Liu, Arvind Narayanan, Clare Voss, Fabian Yamaguchi, and Rachel Greenstadt. De-anonymizing programmers via code stylometry. *Proceedings of the 24th Usenix Security Symposium*, Washington, D.C., August 2015.

[6] Lex Fridman, Steven Weber, Rachel Greenstadt, and Moshe Kam. Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location. *IEEE Systems Journal*, June 2017.

[7] Vaibhav Garg, Sadia Afroz, Rebekah Overdorf, and Rachel Greenstadt. Computer-supported cooperative crime. *Proceedings of the 19th International Conference on Financial Cryptography and Data Security (FC)*, Puerto Rico, January 2015.

[8] Lex Fridman, Ariel Stolerman, Sayandeep Acharya, Patrick Brennan, Patrick Juola, Rachel Greenstadt, and Moshe Kam. Multimodal decision fusion for continuous authentication. *Elsevier Computers and Electrical Engineering*, 41, January 2015.

[9] Aylin Caliskan-Islam, Jonathan Walsh, and Rachel Greenstadt. Privacy detective: Detecting private information and collective privacy behavior in a large social network. *Workshop on Privacy in the Electronic Society (WPES)*, Scottsdale, AZ, November 2014.

[10] Marc Juarez, Sadia Afroz, Gunes Acar, Claudia Diaz, and Rachel Greenstadt. A critical evaluation of website fingerprinting attacks. *Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS)*, Scottsdale, AZ, November 2014.

[11] Rebekah Overdorf, Travis Dutko, and Rachel Greenstadt. Blogs and twitter feeds: A stylometric environmental impact study. *Proceedings of the 7th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPets)*, Amsterdam, Netherlands, July 2014.

Research funding:

[1] Rachel Greenstadt (PI). Attribution of maliciou binaries. *Defence Advanced Research Project Agency (DARPA)*, 2017 – 2019. $599,729 (share $352,205).

[2] Rachel Greenstadt (PI) and Andrea Forte. EAGER: Cybercrime science. *National Science Foundation Division Of Computer and Network Systems (CNS)*, CNS-1347151, September, 2013 – August, 2016. $188,676.

[3] Rachel Greenstadt (PI). CAREER: Privacy analytics for end-users in a big data world. *NSF Faculty Early Career Development Program (CAREER)*, CNS-1253418, February, 2013 – January, 2018. $418,056.

[4] Rachel Greenstadt (PI), Moshe Kam, and P. Juola. Active authentication via linguistic modalities. *Defense Advanced Research Projects Agency (DARPA) Active Authentication Program*, 2012 – 2013. $699,379.

[5] Kapil R. Dandekar (PI), Rachel Greenstadt, Constantine Katsinis, Steven Weber, and Christopher C. Yang. Capacity building: Development and dissemination of the Drexel University cybersecurity program. *National Science Foundation CyberCorps Scholarship for Service Program (NSF-SFS)*, DUE-1241631, November, 2012 – October, 2015. $888,491.

[6] Rachel Greenstadt. Secure computing research for userś benefit (SCRUB). *Intel Science and Technology Center for Secure Computing*, MONTH, 2011 – MONTH, 2014. $540,000.

[7] Rachel Greenstadt. CSSG Phase II: Adversarial linguistic analysis. *Defense Advanced Research Projects Agency (DARPA) Computer Science Study Group (CSSG) Program*, 2011 – 2013. $393,399.

[8] Rachel Greenstadt. Behavior-based access control. *Air Force Research Laboratory (AFRL) and Raytheon BBN Technologies*, MONTH, 2011 – MONTH, 2014. $292,588.

[9] Kapil R. Dandekar (PI), Rachel Greenstadt, and John MacLaren Walsh. A framework for wireless network security based on reconfigure antennas. *National Science Foundation Networking Technology and Systems (NeTS) Program*, ECCS-1028608, September, 2010 – August, 2013. $359,506.

[10] Rachel Greenstadt. CSSG Phase I: Investigating the limitations and potential of automated linguistic analysis. *Defense Advanced Research Projects Agency (DARPA) Computer Science Study Group (CSSG) Program*, MONTH, 2010 – MONTH, 2011. $99,926.

Courses taught:

CS	613	Machine Learning	CS	475	Computer and Network Security
CS	680	Privacy	CS	645	Network Security
CS	467	Security and Human Behavior			

Professional service:

1. *General chair*, Privacy Enhancing Technologies Symposium (PETS), Philadelphia, PA, June, 2015.
2. *Co-Editor-in-Chief*, Proceedings on Privacy Enhancing Technologies
3. *Program Chair*, Privacy Enhancing Technologies Symposium

Faculty profile: **Nagarajan Kandasamy, Ph.D.**

Title	Professor
College	Engineering
Department	Electrical and Computer Engineering
Position	Associate Department Head for Graduate Affairs
Email	kandasamy@drexel.edu
Phone	(215) 895-1996
University page	http://drexel.edu/ece/contact/faculty-directory/KandasamyNagarajan/
Personal page	http://www.ece.drexel.edu/kandasamy/

Research/teaching keywords: computer performance management; computer architecture; fault-tolerant systems; dependable computing.

Cybersecurity expertise: network anomaly detection.

Background: I am an Associate Professor in the Electrical and Computer Engineering Department at Drexel University where I teach and conduct research in the area of computer engineering, with specific interests in embedded systems, self-managing systems, reliable and fault-tolerant computing, distributed systems, computer architecture, and testing and verification of digital systems. I am a recipient of the 2007 National Science Foundation Early Faculty (CAREER) Award and best student paper awards at the IEEE International Conference on Autonomic Computing in 2006 and 2008, and the IEEE Pacific Rim Dependability Conference in 2012.

Publications:

[1] J. Chacko, K. Juretus, M. Jacovic, C. Sahin, N. Kandasamy, I. Savidis, and K. Dandekar. Securing wireless communication through physical layer key based packet obfuscation. *IEEE Trandsaction on Computer*, 2017.

[2] T. Huang, H. Sethu, and N. Kandasamy. A fast algorithm for detecting anomalous changes in network traffic. *Proceedings of the 11th International Conference on Network and Service Management (CNSM)*, Barcelona, Spain, November 2015.

[3] T. Huang, N. Kandasamy, and H. Sethu. Anomaly detection in computer systems using compressed measurements. *Proceedings of the IEEE International Symposium on Software Reliability Engineering (ISSRE)*, Gaithersburg, MD, November 2015.

[4] Justin Hummel, Andrew McDonald, Vatsal Shah, Riju Singh, Bradford D. Boyle, Tingshan Huang, Nagarajan Kandasamy, Harish Sethu, and Steven Weber. A modular multi-location anonymized traffic monitoring tool for a WiFi network (outstanding poster award). *ACM Conference on Data and Application Security and Privacy (CODASPY)*, San Antonio, TX, March 2014.

[5] T. Huang, N. Kandasamy, and H. Sethu. Evaluating compressive sampling strategies for performance monitoring of data centers. *Proceedings of the IEEE/ACM Conference Autonomic Computing (ICAC)*, San Jose, CA, September 2012.

[6] T. Huang, N. Kandasamy, and H. Sethu. Evaluating compressive sampling strategies for performance monitoring of data centers. *Proceedings of the IEEE/IFIP Network Operations and Management Symposium (NOMS)*, Maui, Hawaii, April 2012.

Research funding:

[1] Kapil Dandekar (PI), Stefan Rank, Pramod Abichandani, Nagarajan Kandasamy, and Jennifer S. Standford. Satc: Edu: Software defined radio wars for cybersecurity and information assurance education. *National Science Foundation*, September, 2017 – August 2019. $299,888.

[2] Matthew C. Stamm (PI) and Nagarajan Kandasamy. High performance techniques to identify the source of digital images using multimedia forensics. *Defense Forensics and Biometrics Agency (DFBA) and the Army Research Office (ARO)*, W911NF-15-2-0013, February, 2015 – July, 2016. $374,971.

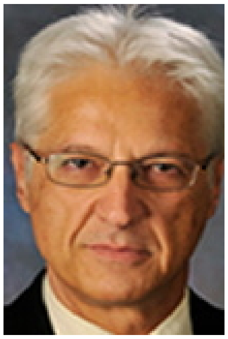
[3] Spiros Mancoridis (PI), Harish Sethu, Naga Kandasamy, and Steven Weber. Machine learning and big data analytics. *Comcast and University of Connecticut Center of Excellence for Security Innovation (CSI)*, January, 2015 – December, 2016. $200,000.

Courses taught:

ENGR	121	Computation Lab I
ECEC	413	Introduction to Parallel Computer Architecture
ECE	200	Digital Logic
ECEC	520	Dependable Computing
ECEC	414	High Performance Computing
ENGR	122	Computation Lab II
ECEC	622	Parallel Computer Architecture
ECEC	353	Introduction to Operating Systems
ECEC	355	Computer Architecture and Organization

Faculty profile: **Constantine Katsinis, Ph.D.**

Title	Associate Teaching Professor
College	Computing and Informatics
Department	Computer Science
Email	katsinis@drexel.edu
Phone	(215) 895-0966
University page	http://drexel.edu/cci/contact/Faculty/Katsinis-Constantine/
Personal page	http://www.pages.drexel.edu/ ck47/



Research/teaching keywords: parallel computer architectures; mobile computing; fault tolerant systems; image processing; pattern recognition.

Cybersecurity expertise: computer security; network security; information assurance.

Background: My research interests include: computer security, computer architecture, parallel processing systems, fault tolerant systems, image processing and pattern recognition. I received my B.S. from the Polytechnic University of Athens, Greece, and my M.S. and Ph.D. from the University of Rhode Island, Kingston, RI, all in Electrical Engineering. I have held positions at the University of Denver and the University of Alabama in Huntsville and have been with Drexel since 1998. I am currently Associate Professor of Computer Security at the College of Computing and Informatics. I have specialized in computer and network security, parallel computer architectures, fault tolerant systems, image processing and performance analysis. I have been the PI or Co-I of several research projects supported by NSF, US ARMY MICOM, DARPA, ONR, NASA, IBM, Motorola, and other companies totaling more than $3,000,000. I have supervised 12 MS Students and 5 Ph.D. students.

Faculty profile: **Geoffrey Mainland, Ph.D.**

Title	Assistant Professor
College	Computing and Informatics
Department	Computer Science
Email	mainland@drexel.edu
Phone	(215) 895-1518
University page	http://drexel.edu/cci/contact/Faculty/Mainland-Geoffrey/
Personal page	https://www.cs.drexel.edu/∼mainland/

Research/teaching keywords: programming languages; functional programming; metaprogramming; type systems; software defined radio.

Cybersecurity expertise: program analysis; anomaly detection.

Background: My research focuses on high-level programming language and runtime support for non-general purpose computation. My work seeks to make it easier to exploit the power of special-purpose devices, like GPUs and FPGAs, that require specialized programming models for optimal efficiency.

Publications:

[1] Gordon Stewart, Mahanth Gowda, Geoffrey Mainland, Bozidar Radunovic, Dimitrios Vytiniotis, and Cristina Luengo Agull. Ziria: An optimizing compiler for wireless PHY programming. *Proceedings of the 20th international conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '15)*, Istanbul, Tukey, 2015.

[2] Geoffrey Mainland, Roman Leshchinskiy, and Simon Peyton Jones. Exploiting vector instructions with generalized stream fusion. *Proceedings of the 18th ACM SIGPLAN International Conference on Functional Programming (ICFP '13)*, pages 37–48, New York, NY, USA, 2013.

[3] Geoffrey Mainland. Explicitly heterogeneous metaprogramming with MetaHaskell. *Proceedings of the 17th ACM SIGPLAN International Conference on Functional Programming (ICFP '12)*, pages 311–322, Copenhagen, Denmark, 2012.

[4] Geoffrey Mainland and Greg Morrisett. Nikola: Embedding compiled GPU functions in Haskell. *Proceedings of the third ACM Symposium on Haskell (Haskell '10)*, pages 67–78, Baltimore, Maryland, USA, 2010.

[5] Geoffrey Mainland, Greg Morrisett, and Matt Welsh. Flask: Staged Functional Programming for Sensor Networks. *Proceeding of the 13th ACM SIGPLAN International Conference on Functional Programming (ICFP '08)*, pages 335–346, Victoria, BC, Canada, 2008.

Faculty profile: **Spiros Mancoridis, Ph.D.**

Title	Isaac L. Auerbach Technical Fellow
College	Computing and Informatics
Department	Computer Science
Position	Interim Dean – College of Computing and Informatics
Research Lab	Software Engineering Research Group (SERG)
Email	spiros@drexel.edu
Phone	(215) 895-6824
University page	http://drexel.edu/cci/contact/Faculty/Mancoridis-Spiros/
Personal page	https://www.cs.drexel.edu/∼spiros/

Research/teaching keywords: security and privacy; software engineering; reverse engineering; software clustering; software visualization; genetic algorithms; software engineering education; evolutionary computation.

Cybersecurity expertise: malware detection, classification, and mitigation; software security; reverse engineering; code analysis.

Background: I serve as interim dean and professor at the College of Computing & Informatics (CCI) at Drexel University. I joined Drexel's faculty in 1996, previously serving as interim department head of the Department of Computer Science, and then as senior associate dean of CCI academic affairs. I have authored or co-authored more than 70 refereed technical publications. In 2008, I was recognized with an Outstanding Researcher Award from the College of Engineering.

Publications:

[1] Ni An, Alexander Duff, Gaurav Naik, Michaelis Faloutsos, Steven Weber, and Spiros Mancoridis. Behavioral anomaly detection of malware on home routers. *12th International Conference on Malicious and Unwanted Software*, Fajardo, Puerto Rico, October 11 – 14 2017.

[2] Bander Alsulami, Spiros Mancoridis, Avinash Srinivasan, and Hunter Dong. Lightweight behavioral malware detection for windows platforms. *12th International Conference on Malicious and Unwanted Software*, Fajardo, Ruerto Rico, October 11 – 14 2017.

[3] A. Darki, A. Duff, Z. Qian, G. Naik, S. Mancoridis, and M. Faloutsos. Don't trust your router: Detecting compromised router. *IEEE Proceedings of the 12th International Conference on Emerging Networking Experiments and Technologies CoNEXT'16 Student Workshop*, Irvine, CA, 2016.

[4] M. Ping, B. Alsulami, and S. Mancoridis. On the effectiveness of application characteristics in the automatic classification of malware smartphones. *Proc. 2016 IEEE International Conference on Malicious and Unwanted Software (MALWARE'16)*, Puerto Rico, October 2016.

[5] Raymond Canzanese, Spiros Mancoridis, and Moshe Kam. Run-time classification of malicious processes using system call analysis. *Proceedings of the 10th International Conference on Malicious and Unwanted Software (MALCON)*, Puerto Rico, USA, October 2015.

[6] Marcello Balduccini and Spiros Mancoridis. Action languages and the mitigation of malware. *Proceedings of the First Workshop on Action Languages, Process Modeling, and Policy Reasoning (ALPP)*, Lexington, KY, September 2015.

[7] Raymond Canzanese, Spiros Mancoridis, and Moshe Kam. System call-based detection of malicious processes. *Proceedings of the IEEE International Conference on Software Security and Reliability (QRS)*, Vancouver, British Columbia, August 2015.

[8] Raymond Canzanese, Moshe Kam, and Spiros Mancoridis. Toward an automatic, online behavioral malware classification system. *Proceedings of the International Conference on Self-Adaptive and Self-Organizing Systems (SASO)*, Philadelphia, PA, September 2013.

Research funding:

[1] Marcello Balduccini and Spiros Mancoridis. Robustness testing of smart grids. *Drexel University Institute for Energy and the Environment (IExE) internal competitive grant*, 2014–2015. $50,000.

[2] Marcello Balduccini and Spiros Mancoridis. Roots of trust in electric energy generation and distribution. *Cyber Security Research Alliance (CSRA)*, 2013–2014. $60,000.

[3] Steven Weber (PI), Kapil R. Dandekar, Spiros Mancoridis, and Harish Sethu. TTP: Medium: Securing the Wireless Philadelphia Network. *National Science Foundation Secure and Trustworthy Cyberspace Program (NSF-SaTC)*, CNS-1228847, September, 2012 – August, 2016. $1,080,800.

[4] Spiros Mancoridis (PI), Harish Sethu, Naga Kandasamy, and Steven Weber. Machine learning and big data analytics. *Comcast and University of Connecticut Center of Excellence for Security Innovation (CSI)*, January, 2015 – December, 2016. $200,000.

Professional service:

1. *Technical Program Committee Member*, Malware Conference, Fajardo, Puerto Rico, 2017.

Faculty profile: **Gaurav Naik**

Title	Assistant Research Professor
College	Computing and Informatics
Department	Computer Science
Email	gn@drexel.edu
Phone	(215) 571-4512
University page	http://drexel.edu/cci/contact/Faculty/Naik-Gaurav/

Research/teaching keywords: architectures and algorithms of computer networks; software defined networks.

Cybersecurity expertise: mobile network security; computer network security.

Background: My current research interests lie in the area of computer networks. In particular, my focus is on next generation Internet architectures and content distribution. My background spans a diverse set of areas in computer science/engineering that also include: mobile ad hoc networks, group key crypto, operating systems, and embedded systems.

Publications:

[1] Ahmad Darki, Alex Duff, Z. Qian, Gaurav Naik, Spiros Mancoridis, and M. Faloutsos. Don't trust your router:detecting compromised router. *The IEEE proceedings of the 12th International Conference on Emerging Networking Experiments and Technologies CoNEXT'16 Student Workshop*, Irvine, CA, 2016.

[2] J. Kopena, E. Sultanik, G. Naik, I. Howley, M. Peysakhov, V.A. Cicirello, M. Kam, and W. Regli. Service-based computing on manets: Enabling dynamic interoperability of first responders. *IEEE Intelligent Systems*, 20(5):17–25, Sep–Oct 2005.

[3] V. Cicirello, M. Peysakhov, G. Anderson, Gaurav Naik, K. Tsang, W. Regli, and M. Kam. Designing dependable agent systems for mobile wireless networks. *IEEE Intelligent Systems*, 19(5):39–45, Sep–Oct 2004.

[4] Gustave Anderson, Andrew Burnheimer, Vincent Cicirello, David Dorsey, Saturnino Garcia, Moshe Kam, Joseph Kopena, Kris Malfettone, Andy Mroczkowski, Gaurav Naik, Max Peysakhov, William Regli, Joshua Shaffer, Evan Sultanik, Kenneth Tsang, Leonardo Urbano, Kyle Usbeck, and Jacob Warren. Intelligent systems demonstration: the secure wireless agent testbed (SWAT). *Proceedings of the 19th National Conference on Artifical Intelligence (AAAI)*, San Jose, CA, July 2004.

[5] Gustave Anderson, Andrew Burnheimer, Vincent Cicirello, David Dorsey, Saturnino Garcia, Moshe Kam, Joseph Kopena, Kris Malfettone, Andy Mroczkowski, Gaurav Naik, Max Peysakhov, William Regli, Joshua Shaffer, Evan Sultanik, Kenneth Tsang, Leonardo Urbano, Kyle Usbeck, and Jacob Warren. Demonstration of the secure wireless agent testbed (swat). *Proceedings of the 3rd International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, New York, NY, July 2004.

[6] Gustave Anderson, Leonardo Urbano, Gaurav Naik, David Dorsey, Andrew Mroczkowski, Donovan Artz, Nicholas Morizio, Andrew Burnheimer, Kris Malfetone, Dan Lapadat, Evan Sultanik, Saturnino Garcia, Max Peysakhov, William Regli, and Moshe Kam. A secure wireless agent-based testbed. *Proceedings of the 2nd IEEE International Information Assurance Workshop (IWIA)*, Charlotte, NC, April 2004.

Research funding:

[1] Ali Shokoufandeh (PI), Gaurav Naik, and Steven Weber. Predicting QoE. *Comcast/Xfinity R&D TechFund*, November, 2015 – July, 2016. $87,547.

[2] Gaurav Naik (PI). Content addressing. *NBC Universal*, November, 2015 – July, 2016.

[3] Gaurav Naik (PI). IPv6 Routing (Phase 2). *Comcast Cable*, June, 2015 – May, 2016.

Courses taught:

CS	675	Reverse Engineering

Faculty profile: **Ioannis Savidis, Ph.D.**

Title	Assistant Professor
College	Engineering
Department	Electrical and Computer Engineering
Research Lab	Integrated Circuits and Electronics (ICE) Design and Analysis Laboratory
Email	isavidis@coe.drexel.edu
Phone	(215) 571-4584
University page	http://drexel.edu/ece/contact/faculty-directory/SavidisIoannis/
Personal page	http://ece.drexel.edu/savidis/
Lab page	http://ice.ece.drexel.edu

Research/teaching keywords: analysis, modeling, and design methodologies for high performance digital and mixed-signal integrated circuits; emerging integrated circuit technologies; electrical and thermal modeling and characterization; signal and power integrity analysis; power and clock analysis and design.

Cybersecurity expertise: hardware security; Trojan detection and mitigation; gate level logic encryption; side-channel analysis; circuit-level intellectual property protection; design for trust.

Background: I am an Assistant Professor in the Electrical and Computer Engineering Department at Drexel University where I direct the ICE Laboratory. My research interests include analysis, modeling, and design methodologies for high performance digital and mixed-signal integrated circuits, emerging integrated circuit technologies, heterogeneous 3-D integrated circuits, and interconnect related issues. In the area of security, my research interests include circuit level techniques and methods to 1) prevent the placement of undesired circuits (such as hardware Trojans) in an IC design, 2) detect and implement countermeasures to respond to the presence of foreign circuits, 3) encrypt the functionality of critical circuit blocks to prevent reverse engineering and circuit manipulation by adversaries, and 4) develop algorithms and methodologies to incorporate security into the integrated circuit design flow.

Publications and patents:

[1] J. Chacko, K. Juretus, M. Jacovic, C. Sahin, N. Kandasamy, I. Savidis, and K. Dandekar. Physical gate based preable obfuscation for securing wireless communication. *IEEE International Conference on Computing, Networking and Communication (ICNC)*, 2017.

[2] K. Juretus and I. Savidis. Reducing logic encryption overhead through gate level key insertion. *submitted for inclusion in the proceedings of the IEEE International Symposium on Circuits and Systems (ISCS)*, Montreal, Quebec, May 2016.

[3] Kyle Juretus and Ioannis Savidis. Reduced overhead gate level logic encryption. Provisional Patent, DRX.P020.US.61, 2016. Filed May 18.

[4] K. Juretus and I. Savidis. Low overhead gate level logic encryption. *Proceedings of the Government Microcircuit Applications & Critical Technology Conference (GOMACTech)*, Orlando, FL, March 2016.

[5] Ioannis Savidis. Ip protection through security-aware integrated circuit design. *Defense Advanced Research Projects Agency (DARPA) IP Theft Workshop*, Arlington, Virginia, February 2016.

[6] Kyle Juretus and Ioannis Savidis. Low overhead gate level logic encryption. U.S. Patent Application No. 62/245,155, 2015. Drexel Technology ID 15-1848.

[7] K. Juretus and I. Savidis. Securing Integrated Circuits Through Gate-Level Logic Encryption. *2015 Defense Innovation Summit*, 2015.

Research funding:

[1] Ioannis Savidis (PI). Secure hardware ip solution low overhead circuit obfuscation primitives. *Drexel Ventures Innovation Fund*, July, 2017 – June 2018. $50k.

[2] Ioannis Savidis (PI). Eager: Securing integrated circuits through realtime hardware trojan detection. *National Science Foundation*, CNS-1648878, September, 2016 – August, 2018. $288,650.

Courses taught:

ECEC	471	Introduction to VLSI Design	ECEC	571	Introduction to VLSI Design
ECEC	472	Custom VLSI Design & Analysis I	ECEC	572	Custom VLSI Design & Analysis I
ECEC	473	Modern VLSI IC Design I	ECEC	573	Custom VLSI Design & Analysis II
ENGR	121	Computation Lab I			

Faculty profile: **Harish Sethu, Ph.D.**

Title	Associate Professor
College	Engineering
Department	Electrical and Computer Engineering
Email	sethu@drexel.edu
Phone	(215) 895-5876
University page	http://drexel.edu/ece/contact/faculty-directory/SethuHarish/
Personal page	http://www.ece.drexel.edu/sethu/

Research/teaching keywords: network science and data mining; social computing; web security and privacy; web performance; design and analysis of protocols, architectures and algorithms in computer networks.

Cybersecurity expertise: web security and privacy; network anomaly detection.

Background: My current research and teaching interests lie in the areas of network science, web performance, web security, computer networks and data science. My background spans a diverse set of areas in computer engineering and computer science that also include: parallel computing, performance analysis and quality-of-service in computer networks, mobile ad hoc networks, and sensor networks.

Publications:

[1] T. Huang, H. Sethu, and N. Kandasamy. A fast algorithm for detecting anomalous changes in network traffic. *Proceedings of the 11th International Conference on Network and Service Management (CNSM)*, Barcelona, Spain, November 2015.

[2] T. Huang, N. Kandasamy, and H. Sethu. Anomaly detection in computer systems using compressed measurements. *Proceedings of the IEEE International Symposium on Software Reliability Engineering (ISSRE)*, Gaithersburg, MD, November 2015.

[3] Justin Hummel, Andrew McDonald, Vatsal Shah, Riju Singh, Bradford D. Boyle, Tingshan Huang, Nagarajan Kandasamy, Harish Sethu, and Steven Weber. A modular multi-location anonymized traffic monitoring tool for a WiFi network (outstanding poster award). *ACM Conference on Data and Application Security and Privacy (CODASPY)*, San Antonio, TX, March 2014.

[4] T. Huang, N. Kandasamy, and H. Sethu. Evaluating compressive sampling strategies for performance monitoring of data centers. *Proceedings of the IEEE/ACM Conference Autonomic Computing (ICAC)*, San Jose, CA, September 2012.

[5] Adam J. O'Donnell and Harish Sethu. On achieving software diversity for improved network security using distributed coloring algorithms. *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pages 121–131, October 2004.

Research funding:

[1] Steven Weber (PI), Kapil R. Dandekar, Spiros Mancoridis, and Harish Sethu. TTP: Medium: Securing the Wireless Philadelphia Network. *National Science Foundation Secure and Trustworthy Cyberspace Program (NSF-SaTC)*, CNS-1228847, September, 2012 – August, 2016. $1,080,800.

[2] Harish Sethu (PI) and Steven Weber. BIGDATA: Small: DA: Mining large graphs through subgraph sampling. *National Science Foundation Critical Techniques and Technologies for Advancing Foundations and Applications of Big Data Science and Engineering Program (NSF-BIGDATA)*, IIS-1250786, October, 2013 – September, 2016. $548,367.

[3] Spiros Mancoridis (PI), Harish Sethu, Naga Kandasamy, and Steven Weber. Machine learning and big data analytics. *Comcast and University of Connecticut Center of Excellence for Security Innovation (CSI)*, January, 2015 – December, 2016. $200,000.

Courses taught:

ECEC	690	Web Security I	ECEC	690	Web Security II
ECEC	631	Principles of Computer Networking	ECEC	632	Performance Analysis of Computer Networks
ECEC	633	Advanced Topics in Computer Networks	ECEC	203	Programming for Engineers
ECEC	301	Advanced Programming for Engineers	ECEC	433	Network Programming

Faculty profile: **James Shackleford, Ph.D.**

Title	Assistant Professor
College	Engineering
Department	Electrical and Computer Engineering
Email	shack@drexel.edu
Phone	(215) 571-4269
University page	http://drexel.edu/ece/contact/faculty-directory/ShacklefordJames/

Research/teaching keywords: medical image processing; high performance computing; embedded systems; computer vision; machine learning.

Cybersecurity expertise: runtime code injection; virtual address space manipulation; transparent library redirection.

Background: I received my Ph.D in 2011 from Drexel University for my work on GPU accelerated deformable three-dimensional medical image registration. The algorithms produced by my thesis form the high performance B-spline based image registration core of the open source medical image processing software Plastimatch. Prior to joining Drexel as an Assistant Professor, I was a post-doctoral researcher in the Radiation Oncology Department at the Massachusetts General Hospital in Boston where I conducted tumor motion management research for photon and proton based radiation therapy.

Publications:

[1] James Shackleford, Nagarajan Kandasamy, and Gregory Sharp. *High Performance Deformable Image Registration Algorithms for Manycore Processors.* Morgan Kaufmann Publishers Inc., San Francisco, CA, 2013.

[2] James Shackleford, Nagarajan Kandasamy, and Gregory Sharp. Analytic regularization of uniform cubic b-spline deformation fields. *Proceedings of the 15th International Conference on Medical Image Computing and Computer-Assisted Intervention (MICCAI)*, Nice, France, October 2012.

[3] James Shackleford, Nagarajan Kandasamy, and Gregory Sharp. Deformable volumetric registration in B-Splines. Wen mei W. Hwu, editor, *GPU Computing Gems Emerald Edition (Applications of GPU Computing Series).* Morgan Kaufmann Publishers Inc., San Francisco, CA, 2011.

[4] James Shackleford, Nagarajan Kandasamy, and Gregory Sharp. On developing B-spline registration algorithms for multi-core processors. *Physics in Medicine and Biology*, 55(21):6329, 2010.

Courses taught:

ECE	200	Digital Logic Design	ECEC	353	Systems Programming
ECEC	631	Principles of Computer Networking	ECEC	632	Performance Analysis of Computer Networks
ECEC	301	Advanced Programming for Engineers			

Faculty profile: **Matthew Stamm, Ph.D.**

Title	Assistant Professor
College	Engineering
Department	Electrical and Computer Engineering
Research Lab	Multimedia and Information Security Laboratory (MISL)
Email	mstamm@coe.drexel.edu
Phone	(215) 895-5894
University page	http://drexel.edu/ece/contact/faculty-directory/StammMatthew/
Personal page	http://www.ece.drexel.edu/stamm/
Lab page	http://misl.ece.drexel.edu

Research/teaching keywords: information security; multimedia forensics and anti-forensics; information verification; adversarial dynamics; signal processing.

Cybersecurity expertise: information security; multimedia forensics and anti-forensics; information verification.

Background: I head the Multimedia and Information Security Laboratory (MISL) where I conduct research on signal processing and information security with a focus on digital multimedia forensics and anti-forensics. Much of my research involves developing techniques to detect information forgeries, such as falsified images and videos, along with understanding what anti-forensic countermeasures an information attacker can use to disguise their forgery. For my dissertation research, I was awarded the Dean's Doctoral Research Award in 2012 from the University of Maryland. Additionally, I was a radar systems engineer at the Johns Hopkins University Applied Physics Laboratory from 2004 until 2006.

Publications:

[1] O. Mayer and M. Stamm. Accurate and efficient image forgery detection using lateral chromatic aberration. *IEEE Transactions on Information Forensics and Security*, 2017.

[2] Xiaoyu Chu, Matthew C. Stamm, and K.J.R. Liu. Compressive sensing forensics. *IEEE Transactions on Information Forensics and Security*, 10(7):1416–1431, July 2015.

[3] Xiaoyu Chu, Matthew C. Stamm, Yan Chen, and K.J.R. Liu. On antiforensic concealability with rate-distortion tradeoff. *IEEE Transactions on Image Processing*, 24(3):1087–1100, March 2015.

[4] Xiaoyu Chu, Yan Chen, Matthew C. Stamm Liu, and K.J.R. Liu. Information theoretical limit of compression forensics. *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Florence, Italy, May 2014.

[5] Matthew C. Stamm, W.S. Lin, and K.J.R. Liu. Temporal forensics and anti-forensics for motion compensated video. *IEEE Transactions on Information Forensics and Security*, 7(4):1315–1329, August 2012.

[6] Matthew C. Stamm and K.J.R. Liu. Anti-forensics of digital image compression. *IEEE Transactions on Information Forensics and Security*, 6(3):1050–1065, September 2011.

[7] Matthew C. Stamm and K.J.R. Liu. Forensic detection of image manipulation using statistical intrinsic fingerprints. *IEEE Transactions on Information Forensics and Security*, 5(3):492–506, September 2010.

[8] Matthew C. Stamm, S.K. Tjoa, W.S. Lin, and K.J.R. Liu. Anti-forensics of JPEG compression. *Proceedings of the IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP)*, Dallas, TX, March 2010.

Research funding:

[1] Matthew C. Stamm (PI) and Nagarajan Kandasamy. High performance techniques to identify the source of digital images using multimedia forensics. *Defense Forensics and Biometrics Agency (DFBA) and the Army Research Office (ARO)*, W911NF-15-2-0013, February, 2015 – July, 2016. $374,971.

[2] Matthew C. Stamm (PI). CAREER: Scaling multimedia forensic algorithms for big data and adversarial environments. *NSF Faculty Early Career Development Program (CAREER)*, March, 2016 – February, 2021 (estimated). $587,000.

Courses taught:

ECES	301	Transform Methods and Filtering	ECES	435	Multimedia Signal Processing and Information Security

Professional service:

1. *Technical Program Committee Member*, IEEE International Workshop on Information Forensics and Security (WIFS), (2014, 2015)
2. *General Chair*, ACM Workshop on Information Hiding and Multimedia Security (2017)

Faculty profile: **Baris Taskin, Ph.D.**

Title	Professor
College	Engineering
Department	Electrical and Computer Engineering
Research Lab	Drexel VLSI and Architecture Laboratory
Email	taskin@coe.drexel.edu
Phone	(215) 895-5972
University page	http://drexel.edu/ece/contact/faculty-directory/TaskinBaris/
Lab page	http://vlsi.ece.drexel.edu

Research/teaching keywords: electronic design automation (EDA) of VLSI circuits; high-performance circuits; resonant clocking; integrated circuit (IC) physical design; networks-on-chip (NoC); hardware/software design for exascale computing.

Cybersecurity expertise: hardware security; hardware/software co-design for exascale system performance.

Background: I joined Drexel University as an assistant professor in 2005. Between 2003-2004, I was a staff engineer at MultiGiG Inc., Scotts Valley, CA, working on electronic design automation of integrated circuit timing and clocking. I am the coauthor of the book entitled Timing Optimization Through Clock Skew Scheduling (Springer, 2009). I am an "A. Richard Newton Award" winner from the ACM SIGDA in 2007 (for junior faculty starting new programs in EDA); a recipient of the Faculty Early Career Development Award (CAREER) from the National Science Foundation (NSF) in 2009; and the Distinguished Service Award from ACM SIGDA in 2012.

Publications:

[1] Weicheng Liu, Emre Salman, Can Sitik, Baris Taskin, Savithri Sundareswaran, and Benjamin Huang. Circuits and algorithms to facilitate low swing clocking in nanoscale technologies. *Proceedings of Semiconductor Research Corporation (SRC) TechCon*, Santa Clara, CA, November 2015.

[2] Karthik Sangaiah, Mark Hempstead, and Baris Taskin. Uncore RPD: Rapid design space exploration of the uncore via regression modeling. *Proceedings of IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, Austin, TX, November 2015.

[3] Leo Filippini, Emre Salman, and Baris Taskin. A wirelessly powered system with charge recovery logic. *Proceedings of the IEEE International Conference on Computer Design (ICCD)*, New York, NY, October 2015.

[4] Mallika Rathore, Emre Salman, Can Sitik, and Baris Taskin. A novel static D flip-flop topology for low swing clocking. *Proceedings of ACM Great Lakes Symposium on VLSI (GLSVLSI)*, Pittsburgh, PA, May 2015.

[5] Weicheng Liu, Emre Salman, Can Sitik, and Baris Taskin. Clock skew scheduling in the presence of heavily gated clock networks. *Proceedings of ACM Great Lakes Symposium on VLSI (GLSVLSI)*, Pittsburgh, PA, May 2015.

[6] Weicheng Liu, Emre Salman, Can Sitik, and Baris Taskin. Enhanced level shifter for multi-voltage operation. *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS)*, Lisbon, Portugal, May 2015.

Research funding:

[1] Baris Taskin (PI) and Kapil R. Dandekar. Wireless on-chip interconnects. *National Science Foundation (NSF)*, ECCS-1232164, September, 2012 – August, 2016. $416,000.

[2] Mark Hempstead and Baris Taskin (Co-PI). Fast and Efficient Hardware Design Exploration through Memory-NoC Analysis for Multi-Core SoCs. *Samsung Global Research Organization*, #003897-002, September, 2014 – August, 2015. $100,000.

[3] Baris Taskin (PI), Bahram Nabet, Mark Hempstead, Nagarajan Kandasamy, and Timothy Kurzweg. II-NEW: Testbed for High Speed Interconnects. *National Science Foundation (NSF)*, CNS-1305350, September, 2013 – August, 2016. $700,000.

[4] Baris Taskin (PI) and Emre Salman. Design and automation of low swing clocking. *Semiconductor Research Corporation (SRC)*, Innovative and Intelligent Internet of Things (I3T)- Task.2451, July, 2013 – September, 2016. $225,000.

[5] Baris Taskin (PI). Resonant clocking technologies. *National Science Foundation (NSF)*, CCF-0845270, June, 2009 – May, 2014. $400,000.

Courses taught:

ECEC	671	Electronic Design Automation for VLSI Circuits I	ECEC	672	Electronic Design Automation for VLSI Circuits II
ENGR	121	Computation Lab I	ENGR	122	Computation Lab II

Faculty profile: **Kristene Unsworth, Ph.D.**

Title	Assistant Professor
College	Computing and Informatics
Department	Information Science
Email	unsworth@drexel.edu
Phone	(215) 895-6016
University page	http://drexel.edu/cci/contact/Faculty/Unsworth-Kristene/
Personal page	http://cci.drexel.edu/faculty/kunsworth/

Research/teaching keywords: information policy; ethics; government information.

Cybersecurity expertise: surveillance; national security policy.

Background: My research interests are in the areas of information policy, ethics, government information and surveillance studies. I have conducted research on the use of social categorization in national security policy in historical, international and contemporary contexts. My work examines the ethical issues behind social categorization, information use and retrieval in government contexts. Current projects include examining the role of citizen participation in government See something, Say something campaigns and the ethical implications of and such participation. My teaching interests focus on issues of access to and critique of government information, information policy and ethics.

Faculty profile: **Steven Weber, Ph.D.**

Title	Professor
College	Engineering
Department	Electrical and Computer Engineering
Position	Director of the Drexel Cybersecurity Institute
Research Lab	Drexel Modeling and Analysis of Networks Lab (MANLab)
Email	sweber@coe.drexel.edu
Phone	(215) 895-0254
University page	http://drexel.edu/ece/contact/faculty-directory/WeberSteven/
Personal page	http://www.ece.drexel.edu/weber/
Lab page	http://network.ece.drexel.edu

Research/teaching keywords: computer networks; wireless networks; resource allocation; network performance analysis; probability; stochastic processes; statistics; information theory; optimization; network economics; network simulation.

Cybersecurity expertise: network performance; statistical analysis; anomaly detection; security overhead analysis.

Background: my research focuses on the mathematical modeling and performance analysis of wireless and wired computer and communication networks. Using probability, stochastic processes, optimization, and information theory, I seek to capture performance bounds and performance tradeoffs, leading to optimized network designs. My security interests are in network anomaly detection, network security-overhead tradeoffs, and user authentication.

Publications:

[1] Ni An, Alexander Duff, Gaurav Naik, Michaelis Faloutsos, Steven Weber, and Spiros Mancoridis. Behavioral anomaly detection of malware on home routers. *12th International Conference on Malicious and Unwanted Software*, Fajardo, Puerto Rico, October 11 – 14 2017.

[2] Ni An, Vinod Mishra, and Steven Weber. Pca-based statistical anomaly detection of stealthy reactive jamming in wifi networks. *IEEE Conference on Communications and Network Security (CNS)*, Las Vegas, NV, October 2017.

[3] Steven Weber. A slotted aloha message concentration protocol for wireless sensor network. *IEEE Wireless Communications and Networking Conference (WCNC)*, San Francisco, CA, March 20 2017.

[4] Ni An and Steven Weber. On the sample size of pca-based anomaly detection. *Proceedings of the 51st Annual Conference on Information Sciences and Systems (CISS)*, Baltimore, MD, March 2017.

[5] Ni An and Steven Weber. On the performance overhead tradeoff of distributed principal component analysis via data partitioning. *Proceedings of the 50th Annual Conference on Information Sciences and Systems (CISS)*, Princeton, NJ, March 2016.

[6] Lex Fridman, Steven Weber, Rachel Greenstadt, and Moshe Kam. Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location. *IEEE Systems Journal*, accepted August 2015.

[7] Justin Hummel, Andrew McDonald, Vatsal Shah, Riju Singh, Bradford D. Boyle, Tingshan Huang, Nagarajan Kandasamy, Harish Sethu, and Steven Weber. A modular multi-location anonymized traffic monitoring tool for a WiFi network (outstanding poster award). *ACM Conference on Data and Application Security and Privacy (CODASPY)*, San Antonio, TX, March 2014.

Research funding:

[1] Steven Weber (PI), Kapil Dandekar, Ioannis Savidis, and Matthew Stamm. Security by design: Drexel hands-on cybersecurity laboratory curriculum. *NSA-CNAP*, October 1, 2017 – September 30, 2018. $255,359.93.

[2] Steven Weber (PI). Cyber risk management: Identification and quantification of unreported health care data breaches. *Casualty Actuarial Society (CAS) Cyber Risk Task Force*, January, 2016 – December, 2016. $30,000.

[3] Steven Weber (PI), Kapil R. Dandekar, Spiros Mancoridis, and Harish Sethu. TTP: Medium: Securing the Wireless Philadelphia Network. *National Science Foundation Secure and Trustworthy Computing Program (NSF-SaTC)*, CNS-1228847, September, 2012 – August, 2016. $1,080,800.

[4] Spiros Mancoridis (PI), Harish Sethu, Naga Kandasamy, and Steven Weber. Machine learning and big data analytics. *Comcast and University of Connecticut Center of Excellence for Security Innovation (CSI)*, January, 2015 – December, 2016. $200,000.

[5] Kapil R. Dandekar (PI), Jaudelice C. de Oliveira, Karen Miu Miller, Chikaodinaka Nwankpa, and Steven Weber. Secure wireless control for future naval smart grids. *Office of Naval Research (ONR)*, N000141612037, November, 2015 – December, 2018. $749,831.

[6] Ali Shokoufandeh (PI), Gaurav Naik, and Steven Weber. Predicting qoe. *Comcast and University of Conneticut Center of Excellence for Security Innovation (CSI)*, January, 2016 – December, 2017. $137,010.79.

[7] Steven Weber (PI) and Christopher Carroll. The drexel cybersecurity for soldiers program (dcsp). *National Security Agency (NSA)*, September, 2016 – August, 2017. $206,165.

Courses taught:

ECE	361	Probability for engineers	ECES	523	Detection and estimation theory
ECES	302	Transform methods and filtering	ECEC	631	Principles of computer networking
ECES	521	Probability and random variables	ECEC	632	Performance analysis of comp. networks
ECES	522	Random proc. & spectral analysis	ECEC	633	Advanced topics in comp. networking

Faculty profile: **Christopher Yang, Ph.D.**

Title	Associate Professor
College	Computing and Informatics
Department	Information Science
Email	chris.yang@drexel.edu
Phone	(215) 895-1631
University page	http://drexel.edu/cci/contact/Faculty/Yang-Christopher/
Personal page	https://cci.drexel.edu/faculty/cyang/

Research/teaching keywords: web search and mining; knowledge management; cross-lingual information retrieval; text summarization; multimedia retrieval; information visualization; digital library; electronic commerce.

Cybersecurity expertise: security informatics; information sharing and privacy; sentiment analysis.

Background: In my recent work on healthcare informatics and security informatics, I am closely collaborating with USC Keck School of Medicine, UCSF School of Medicine, Marshfield Clinic Research Institute, Children's Hospital of Philadelphia, UPenn Medical School, and Johnson & Johnson. I serve as associate editor-in-chief of Security Informatics (Springer) and co-editor of Electronic Commerce Research and Applications (Elsevier). I have edited special issues on social media, healthcare informatics, security informatics, Web mining, multilingual information systems, knowledge management, and electronic commerce in IEEE Transactions, ACM Transactions, IEEE Intelligent Systems, JASIST, DSS, IPM.

Publications:

[1] Zhen Hai, Kuiyu Chang, Jung-Jae Kim, and Christopher C. Yang. Identifying opinion features in sentiment analysis via domain-specific and generic topical relevance. *IEEE Transactions on Knowledge and Data Engineering*, 26(3):623–634, March 2014.

[2] Xuning Tang and Christopher C. Yang. Social network integration and analysis using a generalization and probabilistic approach for privacy preservation. *SpringerOpen Security Informatics Journal*, 1(7), December 2012.

[3] Christopher C. Yang, Xuning Tang, and Xiajing Gong. Identifying clusters from dark web with temporal coherence analysis. *Proceedings of IEEE International Conference on Intelligence and Security Informatics (ISI)*, Beijing, China, July 2011.

[4] Christopher C. Yang and Bhavani Thuraisingham. Privacy-preserved social network integration and analysis for security informatics. *IEEE Intelligent Systems Magazine*, 25(3):88–90, September–October 2010.

[5] Christopher C. Yang and Xuning Tang. Information integration for terrorist or criminal social networks. *Annals of Information Systems*, 9:41–58, 2010.

[6] Christopher C. Yang and Marc Sageman. Analysis of terrorist social networks with fractal views. *Sage Journal of Information Science*, 35(3):299–320, March 2009.

Research funding:

[1] Hsinchun Chen (PI), Catherine Larson, Mark Patton, and Chris Yang. CIF21 DIBBs: DIBBs for intelligence and security informatics research community. *National Science Foundation (NSF) Division Of Advanced Cyber Infrastructure (ACI)*, ACI-1443019, October, 2014 – September, 2017. $1,499,531 total, $150,000 to Drexel.

[2] Kapil R. Dandekar (PI), Rachel Greenstadt, Constantine Katsinis, Steven Weber, and Christopher C. Yang. Capacity building: Development and dissemination of the Drexel University cybersecurity program. *National Science Foundation CyberCorps Scholarship for Service Program (NSF-SFS)*, DUE-1241631, November, 2012 – October, 2015. $888,491.

Courses taught:

INFO	101	Introduction to Information Technology	INFO	300	Information Retrieval Systems
INFO	812	Research Statistics I			

Professional service:

1. *Chair*, IEEE ICDM Workshop on Intelligence and Security Informatics 2015, Atlantic City, November, 2015
2. *Chair*, ACM SIGKDD Workshop on Intelligence and Security Informatics 2012, Beijing, China, August, 2012
3. *Associate Editor-in-Chief*, SpringerOpen Security Informatics Journal

4 Research

The research section of this overview is broken down as follows:

- §4.1 Research projects
- §4.2 Research funding
- §4.3 Research articles
- §4.4 Graduate students
- §4.5 Research community engagement
- §4.6 Technology commercialization

4.1 Research projects

On the following pages we present brief summaries of a select set of current cybersecurity research topics:

1. Active authentication on mobile devices – *Lex Fridman, Steven Weber, Rachel Greenstadt, Moshe Kam*

2. Malware detection, classification, and mitigation – *Bander Alsulamy, Raymond Canzanese, Marcello Balduccini, Spiros Mancoridis, Moshe Kam*

3. Network anomaly detection – *Tingshan Huang, Ni An, Harish Sethu, Naga Kandasamy, Matthew C. Stamm, Steven Weber*

4. Secure wireless symmetric key generation and protocol-aware reactive jamming of wireless signals – *Danh Nguyen, Cem Sahin, Boris Shishkin, Naga Kandasamy, Kapil Dandekar*

Research project profile: **active authentication on mobile devices**

Investigators	Lex Fridman	Post-doc	AgeLab	M.I.T.
	Steven Weber	Professor	Dept. of ECE	Drexel University
	Rachel Greenstadt	Associate Profesor	CS Dept.	Drexel University
	Moshe Kam	Professor	Dept. of ECE	NJIT

L. Fridman

S. Weber

R. Greenstadt

M. Kam

Research summary: Active authentication is the problem of continuously verifying the identity of a person based on behavioral aspects of their interaction with a computing device. In this study, we collect and analyze behavioral biometrics data from 200 subjects, each using their personal Android mobile device for a period of at least 30 days. This dataset is novel in the context of active authentication due to its size, duration, number of modalities, and absence of restrictions on tracked activity. The geographical colocation of the subjects in the study is representative of a large closed-world environment such as an organization where the unauthorized user of a device is likely to be an insider threat: coming from within the organization. We consider four biometric modalities: (1) text entered via soft keyboard, (2) applications used, (3) websites visited, and (4) physical location of the device as determined from GPS (when outdoors) or WiFi (when indoors). We implement and test a classifier for each modality and organize the classifiers as a parallel binary decision fusion architecture. We characterize performance with respect to intruder detection time, and quantify how each modality affects overall performance.

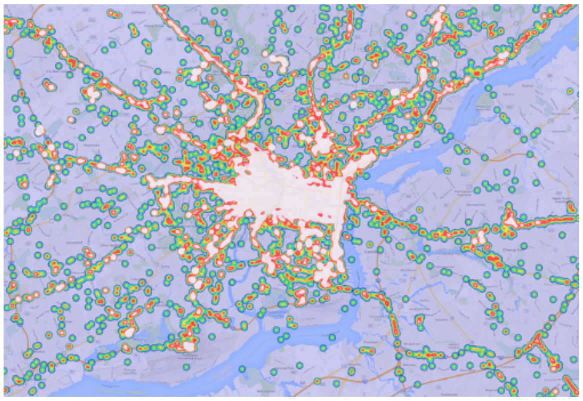


Figure 4: An aggregate heatmap showing a selection from the dataset of GPS locations in the Philadelphia area.

Publications related to this research project include:

[1] Lex Fridman, Steven Weber, Rachel Greenstadt, and Moshe Kam. Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location. *IEEE Systems Journal*, June 2017.

This research is partially supported by the following grants:

[1] Rachel Greenstadt (PI), Moshe Kam, and P. Juola. Active authentication via linguistic modalities. *Defense Advanced Research Projects Agency (DARPA) Active Authentication Program*, MONTH, 2012 – MONTH, 2013. $699,379.

Research project profile: **malware detection, classification, and mitigation**

Investigators	Bander Alsulamy	Ph.D. student	CS Dept.	Drexel University
	Raymond Canzanese	Ph.D.		Sift Security
	Marcello Balduccini	Assistant Research Professor	CS Dept.	Drexel University
	Spiros Mancoridis	Isaac L. Auerbach Professor	CS Dept.	Drexel University
	Moshe Kam	Professor	Dept. of ECE	NJIT

B. Alsulamy

R. Canzanese

M. Balduccini

S. Mancoridis

M. Kam

Research summary: Despite efforts to mitigate the malware threat, the proliferation of malware continues, with record-setting numbers of malware samples being discovered each quarter. Malware are any intentionally malicious software, including software designed for extortion, sabotage, and espionage. Traditional malware defenses are primarily signature-based and heuristic-based, and include firewalls, intrusion detection systems, and antivirus software. Such defenses are reactive, performing well against known threats but struggling against new malware variants and zero-day threats. Together, the reactive nature of traditional defenses and the continuing spread of malware motivate the development of new techniques to detect such threats. One set of techniques uses features from system call traces to infer malicious behaviors.

This research studies detecting and classifying malicious processes using system call trace analysis. The goal is to identify techniques that are 'lightweight' enough and exhibit a low enough false positive rate to be deployed in production environments. Contributions are: (1) a study of the effects of feature extraction strategy on malware detection performance; (2) the comparison of signature-based and statistical detection techniques for malware detection and classification; (3) the application of sequential detection techniques for malware detection, with the goal of identifying malicious behaviors as quickly as possible; (4) a study of malware detection performance at very low false positive rates; and (5) an extensive empirical evaluation, wherein the performance of the malware detection and classification systems are evaluated against data collected from production hosts and from the execution of recently discovered malware samples. The outcome is a proof-of-concept system that detects the execution of malicious processes in production environments and classifies them using known malware.

Publications related to this research project include:

[1] Raymond Canzanese, Spiros Mancoridis, and Moshe Kam. Run-time classification of malicious processes using system call analysis. *Proceedings of the 10th International Conference on Malicious and Unwanted Software (MALCON)*, Puerto Rico, USA, October 2015.

[2] Marcello Balduccini and Spiros Mancoridis. Action languages and the mitigation of malware. *Proceedings of the First Workshop on Action Languages, Process Modeling, and Policy Reasoning (ALPP)*, Lexington, KY, September 2015.

[3] Raymond Canzanese, Spiros Mancoridis, and Moshe Kam. System call-based detection of malicious processes. *Proceedings of the IEEE International Conference on Software Security and Reliability (QRS)*, Vancouver, British Columbia, August 2015.

[4] Raymond Canzanese, Moshe Kam, and Spiros Mancoridis. Toward an automatic, online behavioral malware classification system. *Proceedings of the International Conference on Self-Adaptive and Self-Organizing Systems (SASO)*, Philadelphia, PA, September 2013.

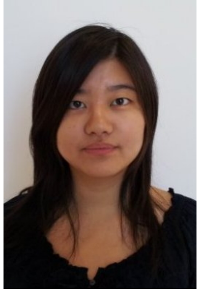
[5] Raymond Canzanese, Moshe Kam, and Spiros Mancoridis. Multi-channel change-point malware detection. *Proceedings of the 7th IEEE International Conference on Software Security and Reliability (SERE)*, Washington, D.C., June 2013.

This research is partially supported by the following grants:

[1] Spiros Mancoridis (PI), Harish Sethu, Naga Kandasamy, and Steven Weber. Machine learning and big data analytics. *Comcast and University of Connecticut Center of Excellence for Security Innovation (CSI)*, January, 2015 – December, 2016. $200,000.

Research project profile: **network anomaly detection**

Investigators	Tingshan Huang	Ph.D.		Akamai
	Ni An	Ph.D. student	Dept. of ECE	Drexel University
	Harish Sethu	Associate Professor	Dept. of ECE	Drexel University
	Naga Kandasamy	Associate Professor	Dept. of ECE	Drexel University
	Matthew C. Stamm	Assistant Professor	Dept. of ECE	Drexel University
	Steven Weber	Professor	Dept. of ECE	Drexel University


T. Huang

N. An

H. Sethu

N. Kandasamy

M. Stamm

S. Weber

Research summary: The goal of this research project is to better understand the fundamental issues in detecting anomalies in a network, and to apply that understanding to the design of improved network anomaly detection mechanisms, algorithms, and protocols.

The work of Tingshan Huang, Harish Sethu, Naga Kandasamy, and Matthew Stamm is on dimensionality reduction techniques for low-cost online performance monitoring and anomaly detection.

The work of Ni An and Steven Weber is on the performance overhead tradeoff of distributed principal component analysis via data partitioning. Data partitioning is desirable or even necessary when the network data used to infer the presence or absence of anomalies cannot be gathered into a single location. Performing network anomaly detection on partitioned data involves first compressing the information stored at each local site (e.g., using principal component analysis), and then sending the compressed signatures to a central data fusion center. The focus of this work is to analytically characterize the relationship between the controls (including the number of sites and the level of compression) and the resulting performance (including the quality of the reconstructed data and the amount of network bandwidth consumed).

Publications related to this research project include:

[1] Ni An, Alexander Duff, Gaurav Naik, Michaelis Faloutsos, Steven Weber, and Spiros Mancoridis. Behavioral anomaly detection of malware on home routers. *12th International Conference on Malicious and Unwanted Software*, Fajardo, Puerto Rico, October 11 – 14 2017.

[2] Ni An and Steven Weber. On the sample size of PCA-based anomaly detection. *Proceedings of the 50th Conference on Information Sciences and Systems (CISS)*, Baltimore, MD, March 2017.

[3] Ni An and Steven Weber. On the performance overhead tradeoff of distributed principal component analysis via data partitioning. *submitted for inclusion in the proceedings of the 50th Conference on Information Sciences and Systems (CISS)*, Princeton, NJ, March 2016.

[4] T. Huang, H. Sethu, and N. Kandasamy. A fast algorithm for detecting anomalous changes in network traffic. *Proceedings of the 11th International Conference on Network and Service Management (CNSM)*, Barcelona, Spain, November 2015.

[5] T. Huang, N. Kandasamy, and H. Sethu. Anomaly detection in computer systems using compressed measurements. *Proceedings of the IEEE International Symposium on Software Reliability Engineering (ISSRE)*, Gaithersburg, MD, November 2015.

This research is partially supported by the following grants:

[1] Steven Weber (PI), Kapil R. Dandekar, Spiros Mancoridis, and Harish Sethu. TTP: Medium: Securing the Wireless Philadelphia Network. *National Science Foundation Secure and Trustworthy Computing Program (NSF-SaTC)*, CNS-1228847, September, 2012 – August, 2018. $1,080,800.

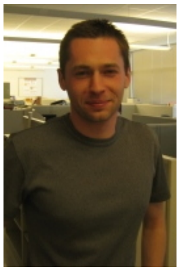
[2] Spiros Mancoridis (PI), Harish Sethu, Naga Kandasamy, and Steven Weber. Machine learning and big data analytics. *Comcast and University of Connecticut Center of Excellence for Security Innovation (CSI)*, January, 2015 – December, 2016. $200,000.

Research project profile: **secure wireless symmetric key generation** and **protocol-aware reactive jamming of wireless signals**

Investigators	Danh Nguyen	Ph.D. student	Dept. of ECE	Drexel University
	Cem Sahin	Ph.D. student	Dept. of ECE	Drexel University
	Boris Shishkin			LMCO-ATL
	Naga Kandasamy	Associate Professor	Dept. of ECE	Drexel University
	Kapil Dandekar	Professor	Dept. of ECE	Drexel University

D. Nguyen

C. Sahin


B. Shishkin

N. Kandasamy

K.R. Dandekar

Research summary – secure wireless symmetric key generation: Our algorithm, which is designed for orthogonal frequency-division multiplexing (OFDM) systems, collects channel state information (CSI) data to extract randomness from the wireless channel. We start by sending packets that contain dummy or non-confidential data back and forth between two legitimate users. For each received packet, the nodes extract CSI and store them inside a matrix. Within the matrix, each column corresponds to the subcarrier index and the rows indicate the packet number. We call this collection of individual CSI measurements the channel trend information (CTI). CTI is used to determine the overall fading trend of each data subcarrier. The confidence constant, N, is set by the user and indicates the number of agreeing ones or zeroes required before a secret bit can be locked. These secret bits are then concatenated to form a secret key. The value of N also determines the number of dummy packets that needs to be transmitted before the key generation takes place. Apart from transmitting packets with dummy data, our algorithm provides secrecy as it does not leak any sensitive information.

Research summary – protocol-aware reactive jamming of wireless signals: We develop a software-defined radio (SDR) framework for real-time reactive adversarial jamming in wireless networks. The system consists of detection and RF response infrastructure, implemented in the FPGA of a USRP N210 and designed to function with the open source GNU Radio SDR library. The framework can be used to implement a fast turnaround reactive jamming system capable of timely RF response within *80ns* of signal detection. Our framework also allows for full control and feedback from the FPGA hardware to the GNU Radio-based cognitive radio backend, making it applicable to a wide range of preamble-based wireless communication schemes. Using this platform, we demonstrate real-time reactive jamming capabilities in both WiFi (802.11g) and mobile WiMAX (802.16e) networks and quantify jamming performances by measuring the network throughput using the iperf software tool. The results indicate that our system works reliably in real time as a reactive jammer.

Publications related to this research project include:

[1] Danh Nguyen, Cem Sahin, Boris Shishkin, Nagarajan Kandasamy, and Kapil R. Dandekar. A real-time and protocol-aware reactive jamming framework built on software-defined radios. *Proceedings of the ACM SIGCOMM Software Radio Implementation Forum (SRIF)*, Chicago, IL, August 2014.

[2] Nikhil Gulati, Rachel Greenstadt, Kapil R. Dandekar, and John M. Walsh. GMM based semi-supervised learning for channel-based authentication scheme. *Proceedings of the 7th IEEE Fall Vehicular Technology Conference (VTC)*, Las Vegas, NV, September 2013.

[3] Prathaban Mookiah and Kapil R. Dandekar. A reconfigurable antenna-based solution for stationary device authentication in wireless networks. *Hindawi International Journal of Antennas and Propagation*, 2012.

This research is partially supported by the following grants:

[1] Steven Weber (PI), Kapil R. Dandekar, Spiros Mancoridis, and Harish Sethu. TTP: Medium: Securing the Wireless Philadelphia Network. *National Science Foundation Secure and Trustworthy Cyberspace Program (NSF-SaTC)*, CNS-1228847, September, 2012 – August, 2016. $1,080,800.

[2] Kapil R. Dandekar (PI), Rachel Greenstadt, and John MacLaren Walsh. A framework for wireless network security based on reconfigurable antennas. *National Science Foundation Networking Technology and Systems (NeTS) Program*, CNS-1028608, September, 2010 – August, 2014. $359,506.

4.2 Research funding

Recent government funding sources are listed in Table 3. Recent corporate funding sources include Intel, Google, Comcast, the Cyber Security Research Alliance (CSRA), and the Casualty Actuarial Society (CAS).

Army Reseearch Office	Rapid Innovation Fund	2017–2019
National Security Agency (NSA)	Cybersecurity National Action Plan (CNAP)	2017–2018
National Science Foundation	Computer and Network System (CNS)	2016–2018
National Science Foundation	Secure and Trustworthy Computing (SaTC)	2012–2017
National Science Foundation	Division of Advanced Cyber Infrastructure (ACI)	2014–2017
National Science Foundation	Cybercorps Scholarships for Service (SFS)	2012–2015
National Science Foundation	Faculty Early Career Development Program (CAREER)	2013–2018, 2016–2021
Defense Forensics and Biometrics Agency (DFBA) and Army Research Office (ARO)		2015–2016
Defense Advanced Research Projects Agency (DARPA)	Active Authentication Program	2012–2013
Defense Advanced Research Projects Agency (DARPA)	Integrated Cyber Analysis System (ICAS) Program	2013–2014
Office of Naval Research (ONR)		2015–2018
Air Force Research Labs (AFRL)		2011–2014
National Security Agency (NSA)		2013–2015
Department of Justice (DoJ)	Office of Justice Programs, Bureau of Justice Assistance	2012–2013
Department of Justice (DoJ) / National Institute of Justice (NIJ)		2009–2011

Table 3: Recent government agencies funding Drexel cybersecurity research and education programs.

The amount of money (in thousands of dollars) in federal and corporate support for Drexel cybersecurity research and education programs is broken down by agency and year in Table 4. The table shows more than $11.4M in cybersecurity research over past nine years, from 7+ agencies, 4+ companies, for 25+ projects, supporting 15+ faculty.

Agency	2009	2010	2011	2012	2013	2014	2015	2016	2017	Total
NSF	200	360		1081	607	150		876	300	4,462
DoJ/NIJ	489			1,487						2,199
DARPA		100	393	699	230				600	2,022
ONR							750			750
DFBA/ARO							375		648	1,023
AFRL			293							293
Intel			540							540
Comcast							288			288
CSRA					60					60
CAS								30		30
Total	689	460	1,225	4,155	897	150	1,413	906	1,548	11,433

Table 4: Federal and corporate support for Drexel cybersecurity research and education programs, by agency and year.

The following is a list of cybersecurity research grants active over the past five years, listed in reverse chronological order:

[1] Steven Weber (PI), Kapil Dandekar, Ioannis Savidis, and Matthew Stamm. Security by design: Drexel hands-on cybersecurity laboratory curriculum. *NSA-Cybersecurity Workforce Education*, October 1, 2017 – September 30, 2018. $255,359.93.

[2] Kapil Dandekar (PI), Stefan Rank, Pramod Abichandani, Nagarajan Kandasamy, and Jennifer S. Standford. Satc: Edu: Software defined radio wars for cybersecurity and information assurance education. *National Science Foundation*, September, 2017 – August 2019. $299,888.

[3] Matthew C. Stamm (PI). High performance techniques to identify the source and authenticity of digital videos using multimedia forensics. *the Army Research Office Rapid Innovation Fund*, July, 2017 – June 2019. $648,572.

[4] Ioannis Savidis (PI). Secure hardware ip solution low overhead circuit obfuscation primitives. *Drexel Ventures Innovation Fund*, July, 2017 – June 2018. $50k.

[5] Rachel Greenstadt (PI). Attribution of malicious binaries. *Defence Advanced Research Project Agency (DARPA)*, 2017 – 2019. $599,729 (share $352,205).

[6] Ioannis Savidis (PI). Eager: Securing integrated circuits through realtime hardware trojan detection. *NSF Computer and Network System (CNS)*, September, 2016 – August, 2018. $288,650.

[7] Matthew C. Stamm (PI). CAREER: Scaling multimedia forensic algorithms for big data and adversarial environments. *NSF Faculty Early Career Development Program (CAREER)*, March, 2016 – February, 2021 (estimated). $587,000.

[8] Steven Weber (PI). Cyber risk management: Identification and quantification of unreported health care data breaches. *Casualty Actuarial Society (CAS) Cyber Risk Task Force*, January, 2016 – December, 2016. $30,000.

[9] Ali Shokoufandeh (PI), Gaurav Naik, and Steven Weber. Predicting QoE. *Comcast/Xfinity R & D TechFund*, November, 2015 – July, 2016. $87,547.

[10] Baris Taskin (PI). Subtask 3.4.1 HPC prototype/component support. *Subcontract to Pro2Serve, in response to Homeland Defense and Security Technical Area Tasks (HDTAT) Project HT-15-1158, for the National Security Agency (NSA) Laboratory for Physical Systems (LPS)*, November, 2015 –. (under contract negotiation).

[11] Kapil R. Dandekar (PI), Jaudelice C. de Oliveira, Karen Miu Miller, Chikaodinaka Nwankpa, and Steven Weber. Secure wireless control for future naval smart grids. *Office of Naval Research (ONR)*, N000141612037, November, 2015 – December, 2018. $749,831.

[12] Matthew C. Stamm (PI) and Nagarajan Kandasamy. High performance techniques to identify the source of digital images using multimedia forensics. *Defense Forensics and Biometrics Agency (DFBA) and the Army Research Office (ARO)*, W911NF-15-2-0013, February, 2015 – July, 2016. $374,971.

[13] Spiros Mancoridis (PI), Harish Sethu, Naga Kandasamy, and Steven Weber. Machine learning and big data analytics. *Comcast and University of Connecticut Center of Excellence for Security Innovation (CSI)*, January, 2015 – December, 2016. $200,000.

[14] Hsinchun Chen (PI), Catherine Larson, Mark Patton, and Chris Yang. CIF21 DIBBs: DIBBs for intelligence and security informatics research community. *National Science Foundation (NSF) Division Of Advanced Cyber Infrastructure (ACI)*, ACI-1443019, October, 2014 – September, 2017. $1,499,531 total, $150,000 to Drexel.

[15] Marcello Balduccini and Spiros Mancoridis. Roots of trust in electric energy generation and distribution. *Cyber Security Research Alliance (CSRA)*, November 2013– May 2014. $60,000.

[16] Marcello Balduccini. FUSION: Federated understanding of security information over networks. *Defense Advanced Research Projects Agency (DARPA) Integrated Cyber Analysis System (ICAS)*, 2013–2014. $230,000 (subcontract).

[17] Rachel Greenstadt (PI) and Andrea Forte. EAGER: Cybercrime science. *National Science Foundation Division Of Computer and Network Systems (CNS)*, CNS-1347151, September, 2013 – August, 2016. $188,676.

[18] Rachel Greenstadt (PI). CAREER: Privacy analytics for end-users in a big data world. *NSF Faculty Early Career Development Program (CAREER)*, CNS-1253418, February, 2013 – January, 2018. $418,056.

[19] Kapil R. Dandekar (PI), Rachel Greenstadt, Constantine Katsinis, Steven Weber, and Christopher C. Yang. Capacity building: Development and dissemination of the Drexel University cybersecurity program. *National Science Foundation CyberCorps Scholarship for Service Program (NSF-SFS)*, DUE-1241631, November, 2012 – October, 2015. $888,491.

[20] Steven Weber (PI), Kapil R. Dandekar, Spiros Mancoridis, and Harish Sethu. TTP: Medium: Securing the Wireless Philadelphia Network. *National Science Foundation Secure and Trustworthy Computing Program (NSF-SaTC)*, CNS-1228847, September, 2012 – August, 2018. $1,080,800.

[21] Rachel Greenstadt (PI), Moshe Kam, and P. Juola. Active authentication via linguistic modalities. *Defense Advanced Research Projects Agency (DARPA) Active Authentication Program*, MONTH, 2012 – MONTH, 2013. $699,379.

[22] Rob D'Ovidio (Co-PI) and NAMES. Research and training program to educate stakeholders on crimes committed using handheld devices. *U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance*, 2011-BE-BX-K001, January, 2012 – December, 2013. $986,976 (collaborative project with Drakontas, LLC and BKForensics).

[23] Rob D'Ovidio (Co-PI) and NAMES. Real crimes in virtual worlds and online video game worlds. *U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance*, 2009-D2-BX-K005, January, 2012 – December, 2013. $500,000 (collaborative project with Drakontas, LLC).

[24] Rachel Greenstadt. CSSG Phase II: Adversarial linguistic analysis. *Defense Advanced Research Projects Agency (DARPA) Computer Science Study Group (CSSG) Program*, MONTH, 2011 – MONTH, 2013. $393,399.

[25] Rachel Greenstadt. Secure computing research for userś benefit (SCRUB). *Intel Science and Technology Center for Secure Computing*, MONTH, 2011 – MONTH, 2014. $540,000.

[26] Rachel Greenstadt. Behavior-based access control. *Air Force Research Laboratory (AFRL) and Raytheon BBN Technologies*, MONTH, 2011 – MONTH, 2014. $292,588.

[27] Kapil R. Dandekar (PI), Rachel Greenstadt, and John MacLaren Walsh. A framework for wireless network security based on reconfigurable antennas. *National Science Foundation Networking Technology and Systems (NeTS) Program*, CNS-1028608, September, 2010 – August, 2014. $359,506.

The following pages give overviews of several ongoing funded cybersecurity research projects.

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
Isaac L. Auerbach
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.

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

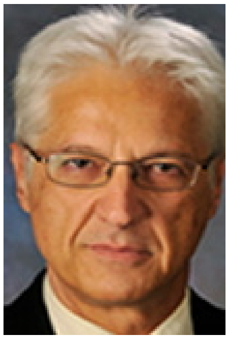
K.R. Dandekar

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.

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.

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.

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.

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.

4.3 Research articles

Recent cybersecurity publications by Drexel faculty have appeared in a variety of top conference venues, including

- 2017 IEEE Wireless Communications and Networking Conference (WCNC)
- 2016,2017 Conference on Information Sciences and Systems (CISS)
- 2017 IEEE Transactions on Information Forensics and Security
- 2017 IEEE Transaction on Computer
- 2016 IEEE International Symposium on Circuits and Systems (ISCAS)
- 2016 *IEEE Systems Journal*
- 2016 IEEE/ACM Great Lake Symposium on VLSI (GLSVLSI)
- 2015 *ASIS Security Journal*
- 2015 *IEEE Transactions on Information Forensics and Security*
- 2015 IEEE International Workshop on Information Forensics and Security (WIFS)
- 2015 Usenix Security Symposium
- 2015 Information Security Solutions Europe (ISSE)
- 2015,2017 International Conference on Malicious and Unwanted Software (MALCON)
- 2015 International Conference on Quality, Reliability, and Security (QRS)
- 2015 IEEE International Symposium on Software Reliability Engineering (ISSRE)
- 2014 ACM SIGCOMM Software Radio Implementation Forum (SRIF)
- 2014 ACM Conference on Data and Application Security and Privacy (CODASPY)

Recent journal publications include the *IEEE Systems Journal*, the *ASIS Security Journal*, and the *IEEE Transactions on Information Forensics and Security.*

The following is a list of cybersecurity research articles published in 2014–2017, listed in reverse chronological order:

[1] Ni An, Alexander Duff, Gaurav Naik, Michaelis Faloutsos, Steven Weber, and Spiros Mancoridis. Behavioral anomaly detection of malware on home routers. *12th International Conference on Malicious and Unwanted Software*, Fajardo, Puerto Rico, October 11 – 14 2017.

[2] Bander Alsulami, Spiros Mancoridis, Avinash Srinivasan, and Hunter Dong. Lightweight behavioral malware detection for windows platforms. *12th International Conference on Malicious and Unwanted Software*, Fajardo, Ruerto Rico, October 11 – 14 2017.

[3] Steven Weber. A slotted aloha message concentration protocol for wireless sensor network. *IEEE Wireless Communications and Networking Conference (WCNC)*, San Francisco, CA, March 20 2017.

[4] Ni An and Steven Weber. On the sample size of PCA-based anomaly detection. *Proceedings of the 50th Conference on Information Sciences and Systems (CISS)*, Baltimore, MD, March 2017.

[5] O. Mayer and Matthew Stamm. Acuurate and efficient image forgery detection using lateral chromatic abberration. *IEEE Transactions on Information Forensics and Security*, 2017.

[6] J. Chacko, K. Juretus, M. Jacovic, C. Sahin, N. Kandasamy, I. Savidis, and K. Dandekar. Securing wireless communication through physical layer key based packet obfuscation. *IEEE Trandsaction on Computer*, 2017.

[7] Belhassen Bayar and Matthew Stamm. A deep learning approach to universal image manipulation detection using a new convolutional layer. *ACM Workshop on Information Hiding and Multimedia Security (IH & MMSec)*, Vigo Galicia, Spain, 2016.

[8] M. Ping, Bander Alsulami, and Spiros Mancoridis. On the effectiveness of application characteristics in the automatic classification of malware smartphones. *the IEEE International Conference on Malicious and Unwanted Software (MALWARE'16)*, Puerto Rico, October 2016.

[9] Ahmad Darki, Alex Duff, Z. Qian, Gaurav Naik, Spiros Mancoridis, and M. Faloutsos. Don't trust your router:detecting compromised router. *The IEEE proceedings of the 12th International Conference on Emerging Networking Experiments and Technologies CoNEXT'16 Student Workshop*, Irvine, CA, 2016.

[10] Kyle Juretus and Ioannis Savidis. Reducing logic encryption overhead through gate level key insertion. *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS)*, Montreal, Canada, May 2016.

[11] Kyle Juretus and Ioannis Savidis. Reduced overhead gate level logic encryption. *IEEE/ACM Great Lake Symposium on VLSI (GLSVLSI)*, Boston, MA, May 2016.

[12] Kyle Juretus and Ioannis Savidis. Low overhead gate level logic encryption. *the Government Microcircuit Applications & Critical Technology Conference*, Orlando, FL, March 2016.

[13] Ni An and Steven Weber. On the performance overhead tradeoff of distributed principal component analysis via data partitioning. *submitted for inclusion in the proceedings of the 50th Conference on Information Sciences and Systems (CISS)*, Princeton, NJ, March 2016.

[14] Rob D'Ovidio, Murugan Anandarajan, and Irv Schlanger. Patrons Beware: Security Vulnerabilities and Public Access Internet Facilities. *ASIS Security Journal*, (in press) 2015.

[15] Claire Vishik and Marcello Balduccini. Making sense of future cybersecurity technologies: Using ontologies for multidisciplinary domain analysis. *Information Security Solutions Europe Conference (ISSE)*, Berlin, Germany, November 2015.

[16] T. Huang, H. Sethu, and N. Kandasamy. A fast algorithm for detecting anomalous changes in network traffic. *Proceedings of the 11th International Conference on Network and Service Management (CNSM)*, Barcelona, Spain, November 2015.

[17] T. Huang, N. Kandasamy, and H. Sethu. Anomaly detection in computer systems using compressed measurements. *Proceedings of the IEEE International Symposium on Software Reliability Engineering (ISSRE)*, Gaithersburg, MD, November 2015.

[18] Raymond Canzanese, Spiros Mancoridis, and Moshe Kam. Run-time classification of malicious processes using system call analysis. *Proceedings of the 10th International Conference on Malicious and Unwanted Software (MALCON)*, Puerto Rico, USA, October 2015.

[19] C. Sahin, D. Nguyen, J. Chacko, and K. R. Dandekar. Cybersecurity education: taking research into the classroom. *Frontiers in Education (FIE) Conference*, El Paso, TX, October 2015.

[20] Marcello Balduccini and Spiros Mancoridis. Action languages and the mitigation of malware. *Proceedings of the First Workshop on Action Languages, Process Modeling, and Policy Reasoning (ALPP)*, Lexington, KY, September 2015.

[21] Lex Fridman, Steven Weber, Rachel Greenstadt, and Moshe Kam. Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location. *IEEE Systems Journal*, June 2017.

[22] Raymond Canzanese, Spiros Mancoridis, and Moshe Kam. System call-based detection of malicious processes. *Proceedings of the IEEE International Conference on Software Security and Reliability (QRS)*, Vancouver, British Columbia, August 2015.

[23] Aylin Caliskan-Islam, Richard Harang, Andrew Liu, Arvind Narayanan, Clare Voss, Fabian Yamaguchi, and Rachel Greenstadt. De-anonymizing programmers via code stylometry. *Proceedings of the 24th Usenix Security Symposium*, Washington, D.C., August 2015.

[24] Xiaoyu Chu, Matthew C. Stamm, and K.J.R. Liu. Compressive sensing forensics. *IEEE Transactions on Information Forensics and Security*, 10(7):1416–1431, July 2015.

[25] Marcello Balduccini, Sarah Kushner, and Jacquelin Speck. Ontology-driven data semantics discovery for cyber-security. *Practical Aspects of Declarative Languages (PADL)*, Portland, OR, June 2015.

[26] Murugan Anandarajan and Irina-Marcela Nedelcu. Self-protecting the smartphone: A motivational model. *Proceedings of the Northeast Decision Sciences Institute Annual Conference (DSI)*, Baltimore, MD, April 2015.

[27] Thomas Shortell and Ali Shokoufandeh. Secure brightness/contrast filter using fully homomorphic encryption. *Proceedings of the 14th International Conference on Information Processing in Sensor Networks (IPSN)*, Seattle, WA, April 2015.

[28] Xiaoyu Chu, Matthew C. Stamm, Yan Chen, and K.J.R. Liu. On antiforensic concealability with rate-distortion tradeoff. *IEEE Transactions on Image Processing*, 24(3):1087–1100, March 2015.

[29] Lex Fridman, Ariel Stolerman, Sayandeep Acharya, Patrick Brennan, Patrick Juola, Rachel Greenstadt, and Moshe Kam. Multi-modal decision fusion for continuous authentication. *Elsevier Computers and Electrical Engineering*, 41, January 2015.

[30] Vaibhav Garg, Sadia Afroz, Rebekah Overdorf, and Rachel Greenstadt. Computer-supported cooperative crime. *Proceedings of the 19th International Conference on Financial Cryptography and Data Security (FC)*, Puerto Rico, January 2015.

[31] Aylin Caliskan-Islam, Jonathan Walsh, and Rachel Greenstadt. Privacy detective: Detecting private information and collective privacy behavior in a large social network. *Workshop on Privacy in the Electronic Society (WPES)*, Scottsdale, AZ, November 2014.

[32] Marc Juarez, Sadia Afroz, Gunes Acar, Claudia Diaz, and Rachel Greenstadt. A critical evaluation of website fingerprinting attacks. *Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS)*, Scottsdale, AZ, November 2014.

[33] D. Nguyen, C. Sahin, B. Shishkin, N. Kandasamy, and K. R. Dandekar. A real-time and protocol-aware reactive jamming framework built on software-defined radios. *Proceedings of the ACM SIGCOMM Software Radio Implementation Forum (SRIF)*, Chicago, IL, August 2014.

[34] Rebekah Overdorf, Travis Dutko, and Rachel Greenstadt. Blogs and twitter feeds: A stylometric environmental impact study. *Proceedings of the 7th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPets)*, Amsterdam, Netherlands, July 2014.

[35] Alexander Jenkins, Murugan Anandarajan, and Rob D'Ovidio. 'All that Glitters is not Gold': The Role of Impression Management in Data Breach Notification. *WSCA Western Journal of Communication*, 78(3):337–357, May 2014.

[36] Sadia Afroz, Aylin Caliskan-Islam, Ariel Stolerman, Rachel Greenstadt, and Damon McCoy. Doppelganger finder: Taking stylometry to the underground. *Proceedings of the 35th IEEE Symposium on Security & Privacy (Oakland)*, San Jose, CA, May 2014.

[37] Xiaoyu Chu, Yan Chen, Matthew C. Stamm Liu, and K.J.R. Liu. Information theoretical limit of compression forensics. *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Florence, Italy, May 2014.

[38] Ni An and Steven Weber. Selective overview of network anomaly detection in cybersecurity (poster). *Women in Cybersecurity (WiCY)*, Nashville, TN, April 2014.

[39] Justin Hummel, Andrew McDonald, Vatsal Shah, Riju Singh, Bradford D. Boyle, Tingshan Huang, Nagarajan Kandasamy, Harish Sethu, and Steven Weber. A modular multi-location anonymized traffic monitoring tool for a WiFi network (outstanding poster award). *ACM Conference on Data and Application Security and Privacy (CODASPY)*, San Antonio, TX, March 2014.

[40] Zhen Hai, Kuiyu Chang, Jung-Jae Kim, and Christopher C. Yang. Identifying opinion features in sentiment analysis via domain-specific and generic topical relevance. *IEEE Transactions on Knowledge and Data Engineering*, 26(3):623–634, March 2014.

[41] M. Atighetchi, M. Mayhew, R. Greenstadt, and A. Adler. Problems and mitigation strategies for developing and validating statistical cyber defenses. *CrossTalk – The Journal of Defense Software Engineering*, 27(2), March–April 2014.

[42] A. Stolerman, R. Overdorf, S. Afroz, and R. Greenstadt. Classify, but verify: Breaking the closed-world assumption in stylometric authorship attribution. *Proceedings of the 10th Annual IFIP WG 11.9 International Conference on Digital Forensics*, Vienna, Austria, January 2014.

[43] A. Stolerman, A. Fridman, R. Greenstadt, P. Brennan, and P. Juola. Active linguistic authentication revisited: Real-time stylometric evaluation towards multi-modal decision fusion. *Proceedings of the 10th Annual IFIP WG 11.9 International Conference on Digital Forensics*, Vienna, Austria, January 2014.

4.4 Graduate students

Fig. 5 shows pictures of current Drexel Ph.D. students performing cybersecurity research, along with the name of their faculty advisor. Fig. 6 shows pictures of recent Drexel Ph.D. graduates with cybersecurity-related theses.

Bander Alsulamy
Ph.D. student
Advisor: S. Mancoridis

Ni An
Ph.D. student
Advisor: S. Weber

Belhassen Bayar
Ph.D. student
Advisor: M.C. Stamm

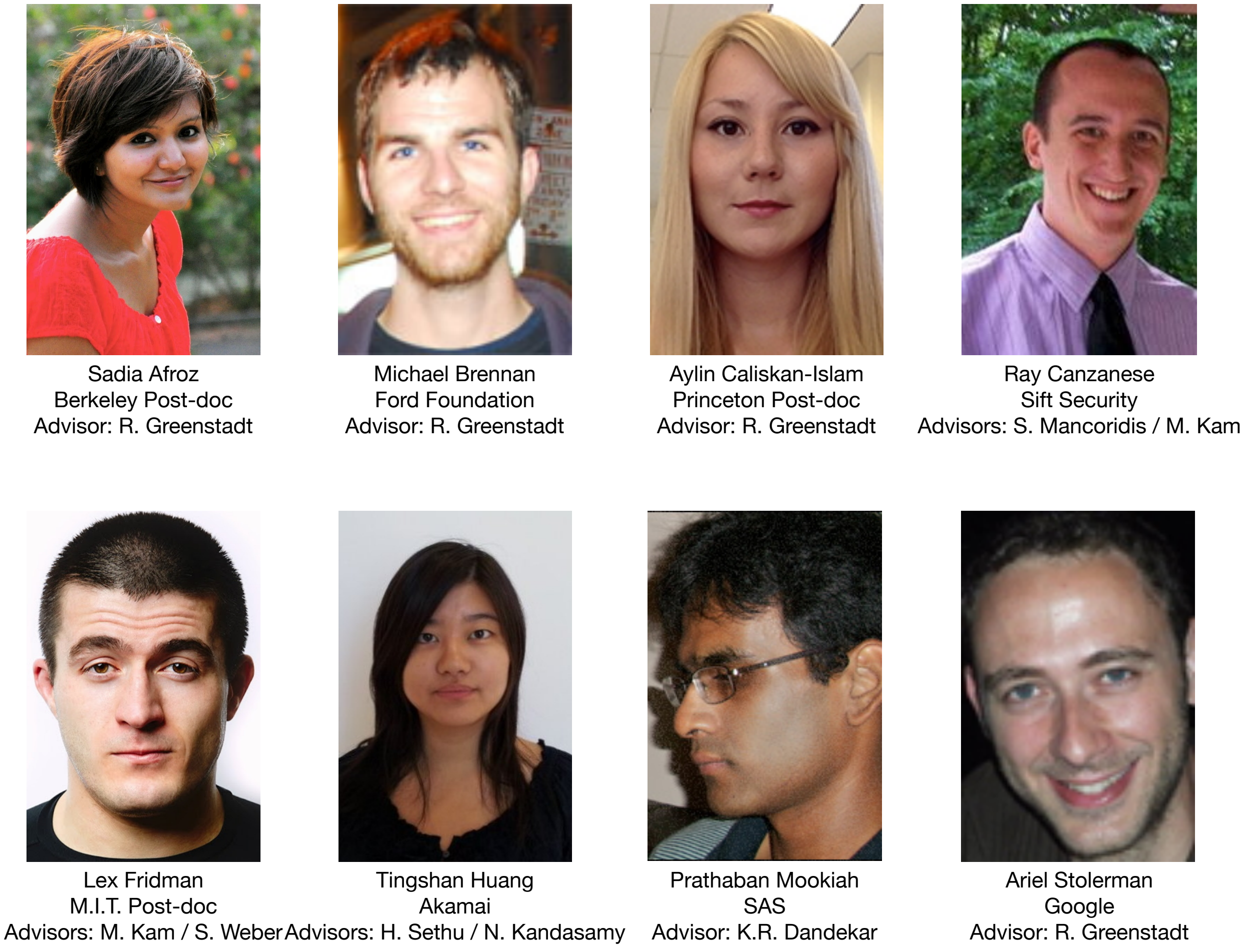
Chen Chen
Ph.D. student
Advisor: M.C. Stacmm

Owen Mayer
Ph.D. student
Advisor: M.C. Stamm

Cem Sahin
Ph.D. student
Advisor: K.R. Dandekar

Xinwei Zhao
Ph.D. student
Advisor: M.C. Stamm

Figure 5: Current Drexel Ph.D. students performing cybersecurity research.



Sadia Afroz
Berkeley Post-doc
Advisor: R. Greenstadt

Michael Brennan
Ford Foundation
Advisor: R. Greenstadt

Aylin Caliskan-Islam
Princeton Post-doc
Advisor: R. Greenstadt

Ray Canzanese
Sift Security
Advisors: S. Mancoridis / M. Kam

Lex Fridman
M.I.T. Post-doc
Advisors: M. Kam / S. Weber

Tingshan Huang
Akamai
Advisors: H. Sethu / N. Kandasamy

Prathaban Mookiah
SAS
Advisor: K.R. Dandekar

Ariel Stolerman
Google
Advisor: R. Greenstadt

Figure 6: Drexel Ph.D. graduates with cybersecurity-related theses.

The following is a list of recent cybersecurity-related M.S. and Ph.D. student candidacy exams, thesis proposals, and thesis defenses, listed in reverse chronological order:

[1] Brandon Katz. Enabling real-time wireless channel based encryption key generation (MS thesis defense). *Advised by Kapil Dandekar*, May 2016.

[2] Tingshan Huang. Adaptive sampling and statistical inference for anomaly detection (Ph.D. thesis defense). *Advised by Harish Sethu and Naga Kandasamy*, November 2015.

[3] Tingshan Huang. Adaptive sampling and statistical inference for anomaly detection (Ph.D. thesis proposal). *Advised by Harish Sethu and Naga Kandasamy*, June 2015.

[4] Aylin Caliskan-Islam. Stylometric fingerprints and privacy behavior in textual data (Ph.D. thesis defense). *Advised by Rachel Greenstadt*, June 2015.

[5] Ray Canzanese. Detection and classification of malicious processes using system call analysis (Ph.D. thesis defense). *Advised by Moshe Kam and Spiros Mancoridis*, May 2015.

[6] Ariel Stolerman. Authorship verification (Ph.D. thesis defense). *Advised by Rachel Greenstadt*, April 2015.

[7] Lex Fridman. Learning of identity from behavioral biometrics for active authentication on desktop computers and mobile devices (Ph.D. thesis defense). *Advised by Moshe Kam and Steven Weber*, December 2014.

[8] Ni An. Network anomaly detection using PCA subspace method (Ph.D. candidacy exam). *Advised by Steven Weber*, September 2014.

[9] Lex Fridman. Learning of identity from behavioral biometrics foractive authentication ondesktop computers and mobile devices (Ph.D. thesis proposal). *Advised by Moshe Kam and Steven Weber*, September 2014.

[10] Sadia Afroz. Deception in authorship attribution (Ph.D. thesis defense). *Advised by Rachel Greenstadt*, June 2014.

[11] Ray Canzanese. Host-based online behavior malware detection and classification (Ph.D. thesis proposal). *Advised by Moshe Kam and Spiros Mancoridis*, April 2014.

[12] Michael Brennan. Managing quality, identity and adversaries in public discourse with machine learning (Ph.D. thesis defense). *Advised by Rachel Greenstadt*, December 2012.

[13] Prathaban Mookiah. Reconfigurable antennas for wireless network security (Ph.D. thesis defense). *Advised by Kapil R. Dandekar*, September 2011.

4.5 Research community engagement

The following is a select list of Drexel faculty leadership in the cybersecurity research community:

[1] Spiros Mancoridis. Technical Program Committee Member. *Malware Conference*, Fajardo, Puerto Rico, October 2017.

[2] Steven Weber. Academia Sector Chierf. *Philadelphia Cyber Education Alliance*, Philadelphia, PA, February 2017.

[3] Matthew Stamm. General Chair. *ACM Workshop on Information Hiding and Multimedia Security*, Philadelphia, PA, June 2017.

[4] Rachel Greenstadt. Co-Editor in Chief. *Proceedings on Privacy Enhancing Technologies*, 2017 – 2018.

[5] Christopher C. Yang. General Chair. *IEEE ICDM Workshop on Intelligence and Security Informatics*, Atlantic City, NJ, November 2015.

[6] Rachel Greenstadt. General Chair. *Privacy Enhancing Technologies Symposium*, Philadelphia, PA, June 2015.

[7] Rachel Greenstadt. Technical Program Committee Member. *IEEE Conference on Social Computing (SocialCom)*, Sydney Australia, December 2014.

[8] Rachel Greenstadt. Technical Program Committee Member. *Workshop on Privacy and the Electronic Society (WPES)*, Scottsdale, AZ, November 2014.

[9] Rachel Greenstadt. Technical program committee member. *ACM Workshop on Artificial Intelligence and Security (AISec)*, Scottsdale, AZ, November 2014.

[10] Rachel Greenstadt. Technical Program Committee Member. *Usenix Security Symposium*, San Diego, CA, August 2014.

[11] Rachel Greenstadt. Co-chair. *Privacy Enhancing Technologies Award Committee*, Amsterdam, Netherlands, July 2014.

[12] Rachel Greenstadt. Member. *Privacy Enhancing Technologies Advisory Board*, Amsterdam, Netherlands, July 2014.

[13] Rachel Greenstadt. Technical Program Committee Member. *Privacy Enhancing Technologies Symposium*, Amsterdam, Netherlands, July 2014.

[14] Marcello Balduccini. Member. *NIST Cyber-Physical Systems Public Working Group*, 2014–present.

[15] Chris Yang. General Chair. *ACM SIGKDD Workshop on Intelligence and Security Informatics*, Beijing, China, August 2012.

[16] Chris Yang. Associate Editor-In-Chief. *Springer Security Informatics*, 2010–present.

[17] Rob D'Ovidio. Member. *International Association of Chiefs of Police, Computer Crime and Digital Evidence Committee*, 2010–present.

4.6 Technology commercialization

The following is a list of cybersecurity patents developed by the Drexel research community and marketed by the Drexel Office of Technology Commercialization:

[1] Prathaban Mookiah, Kapil R. Dandekar, John MacLaren Walsh, and Rachel Greenstadt. A reconfigurable antenna based solution for device authentication in wireless networks. Granted Patent: US 9560073 B2, 2017. Drexel University.

[2] Boris Shishkin, Kpil Dandekar, Danh Nguyen, Cem Sahin, Nagarajan Kandasamy, and David Dorsey. Real-time and protocol-aware reactive jamming in wireless networks. Granted Patent US 9531497 B2, 2016. Drexel University.

[3] Kyle Juretus and Ioannis Savidis. Reduced overhead gate level logic encryption. Provisional US Patent Application Pending, 2016. DRX.P020.US.61.

[4] Cem Sahin and Kapil Dandekar. Symmetric encryption key generation using wireless physical layer information without sharing any information paertinent to the key. Provisional Patent Application 62/261,761, 2016. Drexel University.

[5] Spiros Mancoridis, Raymond Canzanese, and Moshe Kam. Behavioral change-point malware detection system, 2016. Patent Pending.

[6] Kyle Juretus and Ioannis Savidis. Low overhead gate level logic encryption. U.S. Patent Application No. 62/245,155, 2015. Drexel Technology ID 15-1848.

[7] Raymond Canzanese Jr., Spiros Mancoridis, and Moshe Kam. Behavioral change-point malware detection system. Provisional US Patent Application 61/979,259 Pending, 2011. Drexel Technology ID 14-1651D.

[8] Prathaban Mookiah, Kapil R. Dandekar, John MacLaren Walsh, and Rachel Greenstadt. A reconfigurable antenna based solution for device authentication in wireless networks. International Application Pending: PCT/US2012/054205, 2011. Drexel Technology ID 11-1327D.

[9] Spiros Mancoridis, Chris Rorres, Maxim Shevertalov, Edward Stehle, and Kevin Lynch. Zero-day malware and software fault detection and mitigation for enterprise, cloud, and ecommerce servers. US and Intentional patents pending - PCT/US2011/022846, US-2013-0198565-A1, 2009. Drexel Technology ID 09-1111D.

5 Business Development

Drexel University had cybersecurity-oriented business development interactions with the following industry and government entities:

1. BHP Enterprises, LLC (January, 2017)
2. U.S. House of Representative (February, 2017)
3. CenTrak (February, 2017)
4. SAP (March, 2017 – present)
5. Australian Trade Delegation (March, 2017)
6. Department of Homeland Security (DHS) (March, 2017 – present)
7. NSA National Cryptologic School (NCS) (November 2016 – present)
8. Aspen Insurance (October, 2016)
9. NSA Center of Academic Excellence (CAE) program (September 2016 – present)
10. Navigant (August, 2016)
11. 4A Security and Compliance (August, 2016 – present)
12. NetDiligence (June, 2016)
13. Alion Science and Technology (June, 2016 – present)
14. National Institute of Standards and Technology (NIST) (May, 2016)
15. Ben Franklin Technology Parteners of Southeastern PA (April, 2016)
16. National Academies Government-University-Industry Research Roundtable (GUIRR) (March, 2016)
17. Sabre Systems (March, 2016)
18. U.S Army Reserve (persistent relationship)
19. Foreign Policy Research Institute (FPRI) (January, 2016)
20. Office of Governement Relations (OGR) (January, 2016 – present)
21. Susquehanna International Group (SIG) (January, 2016 – present)
22. Huawei North America Network Division (December, 2015)
23. Bowhead IT Group (November, 2015)
24. Federal Reserve Bank of Philadelphia (October, 2015 – present)
25. FAA ASSURE Center of Excellence in Unmanned Aerial Systems Research (October, 2015 – present)
26. Pro2Serve (September, 2015 – present)
27. Praxis Engineering (August, 2015)
28. Innovative Defense Technologies (IDT) (August, 2015 – present)
29. Cybersecurity Analysis, Ltd. (August, 2015)
30. U.S. Army CERDEC and ARDEC (persistent relationship)
31. The Judge Group (July, 2015 – present)
32. Areva Nuclear (June, 2015)
33. Exelon/PECO (June, 2015)
34. Turkish Air Force Academy (April, 2015)
35. Jardine Lloyd Thompson (JLT) (April – May, 2015)
36. National White Collar Crime Center (NWC3) (March, 2015)
37. DSA, Inc. (March, 2015)
38. Northrup Grumman (Mach, 2015)
39. Comcast (March, 2015 – present)

40. Casualty Actuarial Society (March, 2015 – present)
41. Fitlinxx Inc. (March, 2015)
42. Toffler Associates (March, 2015 – June, 2015)
43. Lockheed Martin Corporation Information Systems and Global Solutions (LMCO-ISGS) (March, 2015 – May, 2015)
44. National Security Agency (persistent relationship)
45. Gnostech (February, 2015)
46. L3 Communications (January, 2015)
47. Office of the Mayor of Seoul City, Korea (December, 2014)
48. Unisys Stealth Platform Team (December, 2014 – May, 2015)
49. URS/AECOM (December, 2014 – May, 2015)
50. Federal Bureau of Investigation (FBI) (December, 2014 – present)
51. Vanguard (October, 2014 – present)
52. Merck Pharmaceutical (October, 2014 – January, 2015)
53. Momentum Aviation Group (MAG-DS) (October, 2014)
54. Probaris (October, 2014 – present)
55. F-Secure (Helsinki, Finland) (September – October, 2014)
56. Digile (Helsinki, Finland) (September, 2014 – May, 2015)
57. Boscov's Department Store and the Merchant Advisory Group (MAG) (August – November, 2014)
58. U.S. Bank (August, 2014)
59. Melamedia (August, 2014)
60. Electric Power Research Institute (EPRI) (July, 2014)
61. Computer Sciences Corporation (CSC) (July, 2014)
62. Armed Forces Communications and Electronics Association (AFCEA) Educational Foundation (June, 2014)

Many of these interactions were in coordination with Debbie Buchwald, Office of Corporate Relations.

6 Education

Drexel has established its presence in cybersecurity education through a suite of cybersecurity degrees and certificates. This section breaks down our cybersecurity educational activities into the following categories:

1. Courses, Degrees, Certificates (§6.1)
2. NSA/DHS CAE-CDE recertification (§6.2)
3. NSA Cybersecurity Workforce Education Grant (§6.3)
4. U.S. Army Reserve Private Public Partnership (USAR-P3i) (§6.4)
5. Peace engineering and cybersecurity (§6.5)
6. CyberDragons (§6.6)
7. NSA-NCS Articulation Agreement (§6.7)
8. Other educational development activities (§6.8)

6.1 Courses, Degrees, Certificates

Academic degree programs and certificates. Drexel cybersecurity-related academic degree programs and certificates include:

1. Masters of Science in Cybersecurity (CYBR)
2. Bachelor of Science in Computing and Security Technology (CST)
3. Bachelor of Science in Computer Science – Computer Security Concentration.
4. Certificate in Computing and Security Technology
5. Undergraduate Minor in Computer Crime

We briefly comment on the CYBR degrees.

Master of Science in Cybersecurity (CYBR):

- The motivation behind this degree program stem from conversations between Drexel University and the National Security Agency about the need for more *deeply technical* graduate programs in cybersecurity.
- The key novelty of the Drexel cybersecurity degree is its interdisciplinary structure, achieved by integrating coursework from both the Department of Electrical and Computer Engineering (ECE) in the College of Engineering (CoE) and the College of Computing and Informatics (CCI).
- From the degree description, "The program is designed for students with backgrounds in computer engineering, computer science, electrical engineering, telecommunications engineering or other related technical fields and aims to provide deeply technical and specialized training to develop professionals that are able to understand, adapt, and develop new techniques to confront emerging threats in cybersecurity."
- Launched as an on-campus program in Fall 2013, and was approved as an online program in Spring 2014.
- Development of the CYBR program was funded by a three-year "capacity building" grant awarded to Drexel in 2012 from the National Science Foundation (NSF) Cybercorps Scholarships for Service (SFS) program (PI: Kapil Dandekar (CoE), Co-I: Steven Weber (CoE), Constantine Katsinis (CCI), and Rachel Greenstadt (CCI)).

Cybersecurity-related courses offered. Drexel offers a solid array of both undergraduate and graduate level cybersecurity courses. We briefly highlight three of these:

- Web Security I & II (H. Sethu). A list of topics covered in this two-quarter sequence is given on the left, with the list of subtopics covered in the "symmetric and public key encryption" topic on the right:

A security-conscious intro. to web protocols
Symmetric and public key encryption
Digital certificates and authentication
A security-conscious intro. to HTML & CSS
A security-conscious intro. to JavaScript
Origin-based isolation of content
Encrypted web communications (HTTPS)
Attacks on Domain Name System (DNS)
DNS Security Extensions (DNSSEC)
Security and AJAX
Web privacy
Anonymous web browsing
Illegal hosting and anonymous publishing
Internet censorship and surveillance
Elliptic curve cryptography (ECC)
Web-based malware

Symmetric key cryptography; Data Encryption Standard (DES) and the Advanced Encryption Standard (AES); triple DES; cipher block chaining; attacks on cryptographic protocols.
Secret key exchange protocols; the Diffie-Hellman Exchange (DHE); attacks on DHE and countermeasures.
Fundamentals of number theory; modular arithmetic; Fermat's and Euler's theorems; primality testing; the Chinese Remainder Theorem.
Principles of public key cryptography; the RSA algorithm and practical implementation details; the choice of public and private keys; strategies for attacking RSA; how secure is RSA?
Cryptography in practice on the web; limitations of cryptography.

- Media Forensics & Security (M. Stamm). Learning outcomes are on the left, and the list of topics are on the right:

Image representation, processing, storage.
Information hiding in digital signals.
Information for watermarking or authentication.
Forensic detection of image compression
Forensic detection of contrast enhancement.
Reliable source determination of digital images.

Introduction to image processing
Coding & compression
Information hiding & digital watermarking
Decision theory & machine learning
Steganography & steganalysis
Multimedia forensics - Manipulation detection
Multimedia forensics - Device identification

The following is a select list of cybersecurity-related course offerings over the past three academic years:

Table 5: AY 2016-2017

Term	Course	Title	Instructor	#
Spr 2017	ECEC 680	Hardware Security and Trust	I. Savidis	6
	ECEC 643	Web Security III	H. Sethu	12
	ECES 523	Detection & Estimation Theory	F. Cohen	5
	CS 475	Computer and Network Security	G. Naik	31
	CS 645	Network Security	B. Stuart	13
	CT 222	Security and Information Warfare	J. McGarvey	28
	INFO 333	Intro. to Information Security	J. McGarvey	19
	INFO 517	Principles of Cybersecurity	P. Grillo	22
	INFO 710	Information Forensics	T. Heverin	16
Win 2017	ECEC 642	Web Security II	H. Sethu	28
	ECES 522	Random Processes & Spectral Analysis	J. Walsh	19
	CS 543	Operating Systems	M. Kain	15
	CT 382	Applied Cryptography	W. Pehrsson	16
	CT 325	Operating system Security Architecture I	D. Comroe	18
	CT 422	Incident Presponse Best Practices	D. Whipple	17
	CT 472	Security Defense Countermeasures	D. Comroe	14
	INFO 712	Information Assurance	C. Mascaro	11
	INFO 719	Intro. to National Security Enterprise	E. Garber	8
	HSM 544	Intro. to Homeland Security	R. Macreight	4
	HSM 604	Technology for Homeland Security	M. Aspland	8
Fall 2016	ECET 511	Physical Foundations of Telecoms.	A. Daryoush	14
	CS 303	Algorithmic Number Theory and Cryptography	J. Johnson	26
	CST 609	National Security Intelligence	R. McCreight	12
	INFO 333	Intro. to Information Security	D. Comroe	21
	INFO 375	Intro. to Information Systems Assurance	C. Mascaro	14
	INFO 517	Principles of Cybersecurity	D. Whipple	29
	INFO 710	Information Forensics	C. McClain	16

Table 6: AY 2015-2016

Term	Course	Title	Instructor	#
Spr 2016	CS 475	Computer and Network Security	G. Naik	27
	CS 680	Special Topics: Topics in Crytography	O. Pandey	30
	CT 393	Information Technology Security Rist Assessment	A. Podhrodsky	25
	CT 402	Network Security II	B. Green, C	20
	CT 420	Information Technology Security II	D. Comroe	21
	CT 222	Security and Information Warfare	W. Pehrsson	27
	CT 312	Access Control and Intrusion Detection Technology	A. Podhrodsky	22
	CT 315	Security Management Practice	L. Galloway	16
	CT 300	Security Technology Models and Architecture I	W. Pehrsson	10
	INFO 333	Introduction to Information Security	C. Carroll	26
	INFO 375	Introduction to Information Systems Assurance	C. Mascaro	16
	INFO 517	Principles of Cybersecurity	S. White	24
	INFO 710	Information Forensics	C. McClain	12
	INFO 719	Introduction to National Security Enterprise	S. White	7
Win 2016	ECES T680	ST: Media Forensics and Security	M. Stamm	43
	CS 303	Algorithmic Number Theory and Cryptography	J. Johnson	25
	INFO 333	Introduction to Information Security	C. McCain	40
	INFO 712	Information Assurance	P. Grillo	28
	CST 614	Counterintelligence	S. White	9
	HSM 549	Terrorism and Homeland Security	S. White	7
Fall 2015	ECEC 457	Security in Computing	L. Trachtenberg	35
	INFO 375	Introduction to Information Systems Assurance	C. Mascaro	13
	INFO 517	Principles of Cybersecurity	S. White	23
	CST 609	National Security Intelligence	S. White	10
	HSM 544	Introduction to Homeland Security	S. White	13

Table 7: AY 2014-2015

Term	Course	Title	Instructor	#
Spr 2015	CS 303	Algorithmic Number Theory and Cryptography	B. Char	21
	CS 475	Computer and Network Security	R. Greenstadt	24
	HSM 554	Critical Infrastructure Protection	S. White	5
	INFO 333	Introduction to Information Security	C. Carroll	25
	INFO 375	Introduction to Information Systems Assurance	C. Mascaro	23
	INFO 517	Principles of Cybersecurity	S. White	16
	INFO 710	Information Forensics	S. Brown	11
	INFO 718	Cybersecurity, Law and Policy	J. Walters	9
Win 2015	ECEC 690	ST:Web Security II	H. Sethu	25
	ECES 690	ST: Forensic Signal Processing	M. Stamm	27
	CST 614	Counterintelligence	S. White	7
	HSM 549	Terrorism and Homeland Security	S. White	12
	INFO 333	Introduction to Information Security	P. Grillo	25
	INFO 712	Information Assurance	P. Grillo	21
Fall 2014	ECEC 690	ST: Web Security I	H. Sethu	39
	CST 609	National Security Intelligence	S. White	4
	HSM 544	Introduction to Homeland Security	S. White	6
	INFO 333	Introduction to Information Security	C. Carroll	25
	INFO 375	Introduction to Information System Assurance	C. Mascaro	10
	INFO 517	Principles of Cybersecurity	S. White	25
	INFO 710	Information Forensics	S. Brown	19

6.2 NSA/DHS CAE-CDE recertification

- Drexel University has held the designation as a National Security Agency (NSA) / Department of Homeland Security (DHS) Center of Academic Excellence (CAE) in Information Assurance Education for over ten years. The certification is valid up to five years.
- Throughout 2016, the Institute worked on the applicantion to be recertified as an NSA-CAE Cyber Defense Education (CDE). The application was submitted in January 2017.
- Drexel was recertified as an NSA-CAE Cyber Defense Education (CDE) and it was announced at 9th Annual National Cyber Summit in June 2017. The certification is valid through academic year 2022.
- Recertification required establishing coverage of each of twenty-two (22) knowledge units (KUs):

  Basic data analysis
  Basic scripting
  Cyber defense
  Cyber threats
  Databases
  Fundamental security design principles
  IA Fundamentals
  Intro to cryptography
  IT system components
  Network defense
  Network technology and protocols
  Networking concepts
  Operating systems concepts
  Policy, legal, ethics, compliance
  Probability and statistics
  Programming
  Systems administration
  Advanced network technology and protocols
  Database management systems
  Low level programming
  Operating systems theory
  Security risk analysis

  and demonstration of:

  Program outreach and collaboration
  Center for CD education
  A robust and active CD academic program
  CD multidisciplinary efforts
  Practice of CD at the institution level
  Student and faculty CD efforts

6.3 NSA Cybersecurity Workforce Education Grant

This grant will fund the development and offering of several new cybersecurity laboratory courses aimed at senior undergraduate students in Drexel's Department of Electrical and Computer Engineering (ECE), including:

1. Security Offensive and Defensive Topics
2. Blockchain and Cryptocurrency Laboratory
3. Wireless Security Laboratory
4. Image and Video Forensics Laboratory

[1] Steven Weber (PI), Kapil Dandekar, Ioannis Savidis, and Matthew Stamm. Security by design: Drexel hands-on cybersecurity laboratory curriculum. *NSA-Cybersecurity Workforce Education*, October 1, 2017 – September 30, 2018. $255,359.93.

6.4 U.S. Army Reserve Private Public Partnership (USAR-P3i)

ILACI was notified on August 30th 2016 that the Drexel Cybersecurity for Soldiers Program (DCSP), a proposal written by Drexel, was recommended for funding by the NSA and U.S. Army Reserve.

- Use. The funds will be used to develope new cybersecurity courses and laboratories in CCI and in CoE over the next twelve months.

- Seminar series. Besides the courses, the DCSP Seminar Series, consisting of six cybersecurity seminars, will also be developed. Several talks were given in 2016, see (§7.2).
- Thanks to all the people at Drexel who helped with the process, including:

  Ellen Bass
  Colleen Cannon
  Chris Carroll
  Sean Clark
  Kapil Dandekar
  Marie Fazio
  Wayne Hill
  Greg Hislop
  Naga Kandasamy
  Kimberly Logan
  ChiKa Nwankpa
  Aleister Saunders
  Ioannis Savidis
  Matthew Stamm

[1] Steven Weber (PI). The Drexel Cybersecurity for Soldiers Program (DCSP). *National Security Agency (NSA)*, August 30. $206,165.

6.5 Peace engineering and cybersecurity

College of Engineering Dean Joe Hughes has initiated partnerships with Bernard Amadei (founder of Engineers without Borders) and the PeaceTechLab (a non-profit organization spun out of the U.S. Institute for Peace in Washington, D.C.), with the goal of establishing Drexel as an academic leader in the field of peace engineering. The Drexel Cybersecurity Institute has been involved in these discussions, and will continue to play an active role moving foward.

6.6 CyberDragons

In August 2016, the Drexel CyberDragons, a student group was officially formed. The club focuses on general education in cybersecurity and the trainning students for the Collegiate Cyber Defense Competition (CCDC).

- Initial Officers. Colbert Zhu (President), Jennifer Bondarchuk (Vice President), Maksim Bazhydlouski (Treasurer), and Chuck Clift (System Administrator).
- Mentorship. Mr. Chuck Ludwig, head of security at Susquehanna International Group (SIG).
- Outreach. Colbert made presentations at both CCI and ECE new student orientations.
- Structure. Any student with an interest in cybersecurity can join the CyberDragons and participate in the trainnings.
- Equipment. SIG has donated equipment for use by the Drexel CyberDragons; the equipment is housed in the ECE Department.

[1] CyberDragons. *CyberDragons competed Regional Finals for Mid-Atlantic Collegiate Cyber Defense Competition and placed top 4th*, Johns Hopkins Applied Physics Laboratory, MD, March 30 - April 1 2017.

[2] CyberDragons. *CyberDragons attended their First Virtual Qualifier for Mid-Atlantic Collegiate Cyber Defense Competition and placed to 8th*, Drexel University, February 24 2017.

[3] Debbie Buchwald Chris Carroll Chuck Cliff and Steven Weber. *Visited Susquehanna International Group (SIG). Discussion on SIG's mentorship and coaching of the CCDC team.*, Susquehanna International Group Bala Cynwyd PA, June 10 2016.

[4] Steven Weber and Debbie Buchwald (coordinator). Drexel Cybersecurity Institute and Susquehanna International Group (SIG). *CCDC introductory meeting*, Mitchell auditorium Drexel University Edmund D. Bossone Research Enterprise Center Philadelphia PA, April 4 2016.

Figure 7: Drexel CyberDragons logo

6.7 NSA-NCS Articulation Agreement

Since 2016, ILACI has put an effort on the agreement between Drexel University and National Crytologic School (NCS) of the National Security Agency (NSA). The purpose of this agreement is to address the individual needs of the students of the NCS, to recognize the complementary nature of the NSA and Drexel University programs and to provide students who have completed certain NSA-sponsored coursework an oppotunity to more efficiently earn the Drexel University Master of Science degree in Cybersecurity.
ILACI and NCS agreed to confer with each other on a yearly basis regarding changed in curricula involved in this articulation agreement. The agreement was shared with NCS in June, 2017, and has been under review.

6.8 Other educational development activities

Besides the above initiatives, ILACI has also been engaged with several other parties regarding cybersecurity education, including:

- Formation of the organization called Philadelphia Cybersecurity Education Alliance in 2017
- Accommodation of Philly BSide Conference
- Accommodation of Philadelphia Security Shell regular meeting
- Hiring Benjamin Justus as a post-doctoral scientist
- Formation of CyberDragons, student group for Collegiate Cyber Defense Competition trainning and education in cybersecurity
- Extensive interactions with Susan Aldridge and Drexel University Online (DUO) on marketing Drexel cybersecurity education degrees
- Extensive interactions with Debbie Buchwald (Office of Corporate Relations) and Anna Koulas / Patricia Connelly in LeBow Corporate and Executive Education on corporate cybersecurity education
- Involvement in CoE Dean Joe Hughes's effort to build Drexel Peace Engineering, through engagement with Bernard Amadei (Engineers Without Borders) and the Peace Tech Lab (Sheldon Himelfarb)
- Joined the National Cyberwatch Center (cybersecurity education resource clearinghouse), executive director Casey O'Brien
- Participated in 2015 Comcast / U. Conn. CyberSEED hackathon (Mancoridis and Kandasamy)
- Presented at the 2015 Drexel University Computing Academy (DUCA) (M. Stamm)
- Discussions about joint degree and certification initiative with ISACA

- Discussions with Philadelphia String Theory charter school (Balchunas)
- Discussions with Valley Forge Military College (Wayne, PA) (Balchunas)
- Creation of first student chapter of National Military Intelligence Association (NMIA) (Balchunas)

7 Community Engagement

Invited talks given in 2016 by Drexel faculty are listed in §7.1. Events, symposia, invited speakers, and panels organized or co-organized by the Drexel and the Isaac L. Auerbach Cybersecurity Institute are listed in §7.2. Security Community events attended by the ILACI are listed in §7.3. Drexel ILACI has been hosting meetups for the cybersecurity communities like §7.4BSides Philly and §7.5Philly Security Shell. The Drexel ILACI newsletters are listed in §7.6 at the end.

7.1 Invited talks by Drexel faculty

Drexel faculty have given the following invited presentations:

[1] Steven Weber. The value of observations in predicting transmission success in wireless networks under slotted Aloha. *MIT Lincoln Labs*, Boston, MA, August 18 2017.

[2] Rachel Greenstadt. Using Stylometry to Attribute Programmers and Writers. *ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec)*, Philadelphia, PA, June, 20 2017.

[3] Rachel Greenstadt. Privacy, Anonymity, and Perceived Risk in Open Collaboration. *Workshop on Security and Human Behavior*, Cambridge, UK, May 26 2017.

[4] Matthew Stamm. Multimedia Forensics: Using Mathematics and Machine Learning to Detect Image Forgeries. *Rowan University*, NJ, April 2017.

[5] Steven Weber. Facilitating adoption of services with externalities via cost subsidization. *Temple University*, Philadelphia, PA, March 8 2017.

[6] Steven Weber. Block delay under random linear combinations on a random access erasure collision channel. *Information Theory and its Application (ITA)*, San Diego, CA, February 13 2017.

[7] Steven Weber. The value of observations in predicting transmission success in wireless networks under slotted Aloha. *U.S Army Research Labs*, Aberdeen Proving Grounds (APG), VA, January 18 2017.

[8] Matthew Stamm. Multimedia Forensics: Using Mathematics and Machine Learning to Determine an Image's Source and Authenticity. *NSA Center of Academic Exellence Tech Talk*, October 2016.

[9] Steven Weber. Cyber Insurance Modeling: Recent Advances and Challenges. *4A Security Healthcare Data Privacy Symposium*, Drexel Gerri C. LeBow Building, October 4 2016.

[10] Rachel Greenstadt. Implications of Adversarial Learning for Security and Privacy. *2016 USENIX Summit on Hot Topics in Security (HotSEC)*, Austin, TX, August 9 2016.

[11] Matthew Stamm. High Performance Techniques to Identify the Source of Digital Images Using Multimedia Forensics. *Defense Forensics and Biometrics Agency (DFBA)*, August 2016.

[12] Rachel Greenstadt. Erosion of Privacy: Hacking and Privacy Enhancing Technologies. *Pennsylvania Conference of State Trial Judges*, July 28 2016.

[13] Rachel Greenstadt. PoPETs Townhall Meeting Panel. *Privacy Enhancing Technologies Symposium*, Darmdtadt, Germany, July 2016.

[14] Rachel Greenstadt. Attributing Identities Online with Stylometry. *TU Delft Seminar*, Delft Netherlands, June 2016.

[15] Rachel Greenstadt. Deanonymizing programmers. *Crypto Summer School*, Croatia, June 2016.

[16] Kyle Juretus. Hardware Security for the Internet of Things. *IEEE Council on Electronic Design Automation (CEDA)*, May 9 2016.

[17] Rachel Greenstadt. Deanonymizing programmers. *Crypto Working Group*, Utrecht, Netherlands, May 2016.

[18] Rachel Greenstadt. Attrobuting Identities Online with Stylometry. *Security in Times of Surveillance*, TU Eindhoven, Netherlands, May 2016.

[19] Kapil Dandekar. Does the future of wireless network security lie at the physical layer? *Center of Academic Excellence in Information Education Tech Talk*, April 2016.

[20] Rachel Greenstadt. Enhanced attribution teaming brief. *Defense Advanced Research Projects Agency (DARPA)*, Arlington, VA, April 2016.

[21] Matthew Stamm. High performance techniques to identify the source of digital images using multimedia forensics. *Defense Forensics and Biometrics Agency (DFBA)*, March 2016.

[22] Rachel Greenstadt. Stylometry of Source Code and Binaries. *KU Leuven Privacy Seminar*, Leuven, Belgium, February 2016.

[23] Rachel Greenstadt. Doppelganger finder: Taking stylometry to the underground. *City University of New York (CUNY) Graduate Center*, New York, NY, April, 2015.

[24] Steven Weber (panel moderator). Data Overload: Best practices for managing and harnessing data overload. *Comcast Ventures Cybersecurity Practitioner Symposium*, 30 Rockefeller Center, New York, NY, February 19, 2015.

[25] Spiros Mancoridis. TITLE. *U.S. Army 7th Signal Command, Fort Gordon*, Fort Gordon, GA, February 19, 2015.

[26] Norm Balchunas. Drexel Cybersecurity Institute overview. *Abu Dhabi International Offset Conference (ADIOC)*, Ritz-Carlton Abu Dhabi, Grand Canal, United Arab Emirates, February 17–19, 2015.

[27] Aaron Mansheim. Five-year IT Roadmap: A Practitioner's View. *U.S. Army 7th Signal Command, Fort Gordon*, Fort Gordon, GA, November 18, 2014.

[28] Spiros Mancoridis. Panelist. *Comcast CyberSEED Conference*, Storrs, CT, October 29, 2014.

[29] Rachel Greenstadt. Doppelganger finder: Taking stylometry to the underground. *Intel Labs*, June, 2014.

[30] Scott White. Guest speaker. *Israeli Technology: Meeting Todayś Cyber & Homeland Security Challenges*, Fox Rothschild LLP, Philadelphia, PA, June 24, 2014.

[31] Rachel Greenstadt. Doppelganger finder: Taking stylometry to the underground. *University of Michigan*, Ann Arbor, MI, May, 2014.

[32] Spiros Mancoridis. Host-based online behavioral malware detection and classification. *Harvard University Institute for Applied Computational Science IACS Seminar*, Cambridge, MA, April 25, 2014.

[33] Rachel Greenstadt. Doppelganger finder: Taking stylometry to the underground. *Lockheed Martin*, April 23, 2014.

[34] Rachel Greenstadt. Doppelganger finder: Taking stylometry to the underground. *University of California, Berkeley*, Berkeley, CA, April 3, 2014.

[35] Rachel Greenstadt. Analyzing cybercrime forums using stylometry. *Army Research Labs*, Adelphi, MD, February 28, 2014.

7.2 Events organized by the Drexel Isaac L. Auerbach Cybersecurity Institute

The twenty nine (29) events, guest lectures, symposia organized or co-organized by ILACI to date are listed below.

[1] Drexel University. Alion Science. *Drexel hosted visitors from Alion Science*, Drexel Wireless Systems Laboratory (DWSL), 3101 Market St, January 31 2017.

[2] Drexel University. Delaware Valley Chapter of the Information Systems Security Association (ISSA). *The quarterly meeting of the Delaware Valley Chapter of the ISSA*, Behrakis Grand Hall of the Creese Student Center, December 16 2016.

[3] Drexel University. Steven Weber and Ed Croot. *Cybersecurity military/industry/academia thought leadership meeting*, Auerbach and Berger Cybersecurity Lab in 3401 Market St, December 9 2016.

[4] BSides. Brad Bowers. *Philly BSides Conference*, Behrakis Grand Hall in the Creese Student Center, December 2 - 3 2016.

[5] Seminar by Dr. Avinash Srinivasan. Avinash Srinivasan. *Research and Education in Cybersecurity and Forensics: Quo Vadis?”*, November 30 2016.

[6] Drexel Cybersecurity Fall Symposium. Drexel University. *Recognition and celebration of the endowment of the Institute from the Isaac and Carol Auerbach Family Foundation*, Paul Peck Alumni Center, November 14 2016.

[7] When Power Meets Multimedia. IEEE Signal Processing Society Distinguished Lecturer Program Drexel ECE Seminar Series and Institute’s Drexel Cybersecurity for Soldiers Program (DCSP) Seminar Series. *Seminar by Professor Min Wu (U. Maryland)*, October 18 2016.

[8] 4A Security Healthcare Data Privacy Symposium. Drexel University. *Drexel hosted the second annual 4A Security Healthcare Data Privacy Symposium*, Gerri C. LeBow Building, October 4 - 5 2016.

[9] Philadelphia Security Shell. Drexel Cybersecurity Institute. *DCI hosted the Philadelphia Security Shell month meeting first time (continued)*, Auerbach and Berger Cybersecurity Lab Philadelphia PA, June 16 2016.

[10] Drexel University. Drexel University College of Computing and Informatics and Graduate Student Association and Drexel NMIA. *Drexel Cybersecurity Conference*, 3rd floor Atrium, Edmund D. Bossone Research Center, Drexel University, Philadelphia PA, 19104, April 2 2016.

[11] Department of Electrical and Computer Engineering (coordinator). Steven Weber. *The Department of Electrical and Computer and Computer Engineering held the first ”ECE Day”*, Drexel University Edmund D. Bossone Research Enterprise Center Philadelphia PA, February 23 2016.

[12] Drexel University. Philly Code Fest. *Philly CodeFest was held at Drexel University*, Drexel University, February 20 - 21 2016.

[13] Marty Schratz (Judge Group). *Judge Group seminar on job search skills for ECE graduate students*, Drexel University Edmund D. Bossone Research Enterprise Center Philadelphia PA, January 28 2016.

[14] Ben Goodman (President of 4A Security), Lisa Clark (Partner at Duane Morris), Tom Hagy (HB Litigation Conferences), Anna Koulas (LeBow College of Business), and Steven Weber (Drexel Cybersecurity Institute). . *4A Healthcare Data Security and Privacy Symposium*, Gerri C. LeBow Building, Philadelphia, PA, October 22, 2015.

[15] Steven Weber (coordinator). Presenter: David Whipple, Exelon. *Drexel Cybersecurity Institute Symposium: Innovating Securely*, Drexel University Cybersecurity Institute, Philadelphia, PA, June 24, 2015.

[16] Norm Balchunas (coordinator). Presenter: Rob Johnson, Unisys. *Drexel Cybersecurity Institute Symposium: Public and Private Cloud Network Security: Mitigating Virtual Machine Vulnerabilities*, Rush Building, Philadelphia, PA, May 13, 2015.

[17] Norm Balchunas, Steven Weber, David Breen, and Tony Hu (coordinators). Speakers and panelists: Keith Morales (Assistant Vice-President and Information Security Officer at the Federal Reserve Bank of Philadelphia), Ben Goodman (President of 4A Security), Rachel Greenstadt (Associate Professor in CCI), Arun Lakhotia (Professor at U. Louisiana Lafayette), Patrick Lardieri (Lockheed Martin), and Pauli Kuosmanen (Digile). *Drexel Center for Visual and Decision Informatics and Drexel Cybersecurity*

Institute Symposium: Balancing Act: Big Data, Cybersecurity, and Privacy, Paul Peck Alumni Center, Philadelphia, PA, April 13, 2015.

[18] Norm Balchunas (coordinator). Presenter: Hal Berghel (Professor of computer science at the University of Nevada, Las Vegas). *Drexel Cybersecurity Institute Invited Lecture: The Future of Digital Money Laundering*, Paul Peck Alumni Center, Philadelphia, PA, March 31, 2015.

[19] Norm Balchunas (coordinator). Presenters: Darin Bielby and Stephen Ramey from Navigant. *Drexel Cybersecurity Institute Symposium: Data Privacy Challenges in 2015*, Rush Building, Philadelphia, PA, March 26, 2015.

[20] Norm Balchunas (coordinator) and Ben Goodman (President of 4A Security) (moderator). Panelists: Lisa Clark (Partner at Duane Morris, LLP), and Angel Rivera (Developer at Point.io). *Drexel Cybersecurity Institute Symposium: Healthcare Data Security Part II — Life threatening hacks: mobile health and medical device data security*, Rush Building, Philadelphia, PA, February 25, 2015.

[21] Norm Balchunas (coordinator, moderator), and Steven Weber (presenter). Presenters: David Fenske, Susan Aldridge, Scott White, and Rob D'Ovidio. *Drexel Cybersecurity Education Summit. Attendees: Ronald Hahn (URS/AECOM), Theodore Dryer (Dyncorp), Stuart Dyer (Pro2Serv), Kirk Hunigan (Northrup Grumman), Stuart Taylor (Sabre Systems)*, Lafayette Tower, Washington, DC, February 10, 2015.

[22] Norm Balchunas (coordinator) and Ben Goodman (President of 4A Security) (moderator). Panelists: Lisa Clark (Partner, Duane Morris LLP), Elgan Jones (Director of Forensics, Kivu Consulting), Joshua Ladeau (Practice Lead – Privacy and Network Security, Allied World Insurance Company), Charles Mann (Regional Manager, Healthcare, Trend Micro), Jay Orler (Vice President, Security and Infrastructure, Lightbeam Health Solutions), and Paul Rosovsky (Vice President, Healthcare Compliance, 4A Security). *Drexel Cybersecurity Institute Symposium: The Anatomy of a Healthcare Data Breach: Protecting Patient Data Before and After a Breach*, Drexel University Paul Peck Alumni Center, Philadelphia, PA, October 16, 2014.

[23] Norm Balchunas, Debbie Buchwald, and Steven Weber (Drexel coordinators). Opening remarks (Balchunas), panel moderator (Balchunas), panel moderator (Weber). *Delaware Valley Chapter Meeting of the National Defense Industrial Association (NDIA)*, Drexel University College of Business, Philadelphia, PA, September 9, 2014.

[24] Norm Balchunas (coordinator) and Rachel Greenstadt (moderator). Panelists Roger Dingledine (Director, Tor Project) and Nadia Heninger (Magerman Term Assistant Professor, Computer and Information Science, University of Pennsylvania). *Drexel Cybersecurity Institute Symposium: Electronic Privacy*, Drexel University Cybersecurity Institute, Philadelphia, PA, August 6, 2014.

[25] Norm Balchunas (coordinator) and Austin Morris (Managing Partner at SunGard Consulting) (moderator). Panelists Holly Meyers (Senior Vice President, Quality and Risk Management for St. Joseph Health System) and Nick Economidis (Cyber insurance underwriter and expert, Beazley Group). *Drexel Cybersecurity Institute Symposium: Professional Development on Cyber Insurance*, Drexel University Cybersecurity Institute, Philadelphia, PA, June 25, 2014.

[26] Norm Balchunas (coordinator) and Mark Greisiger (President of NetDiligence) (moderator). In partnership with Point.io and LiquidHub; Panelists: Vinny Sakor (ICSA Labs and Verizon), Brian Schaeffer, and Jorge Nieves (Senior Director, Comcast Security Response Center). *Drexel Cybersecurity Institute Symposium: Locking Down Your Company's Data: What Keeps You Awake as CIO?*, Drexel University Cybersecurity Institute, Philadelphia, PA, May 8, 2014.

[27] Norm Balchunas (coordinator). Panelists Scott White and Harvey Rishikof. *Drexel Cybersecurity Institute Symposium: Evidence and Perspectives: Viewing a Cyber Event from the C-Suite*, Drexel University Cybersecurity Institute, Philadelphia, PA, March 25, 2014.

[28] Norm Balchunas (coordinator). Panelists Spiros Mancoridis, Angel Rivera (Senior Developer, Point.io), and Frank Domizio (Computer Forensic Examiner at Federal Bureau of Investigation's Philadelphia

Regional Computer Forensics Lab). *Drexel Cybersecurity Institute Symposium: Cybersecurity Training / Educating the next cybersecurity leaders*, Drexel University Cybersecurity Institute, Philadelphia, PA, March 24, 2014.

[29] Norm Balchunas (coordinator). In partnership with Point.io and LiquidHub. *Drexel Cybersecurity Institute Symposium: CIO Roundtable*, Wells Fargo Center, Philadelphia, PA, March 24, 2014.

7.3 Cybersecurity Community Events attended by the Drexel Isaac L. Auerbach Cybersecurity Institute

The events listed are attended by the Institute.

[1] Steven Weber. NCS 9th Annual National Cyber Summit. , Huntsville, AL, June 6th - 8th 2017.

[2] Steven Weber (co host). Philadelphia Cybersecurity Educaton Alliance (PCEA). *Steven Weber co-hosted the inaugural meeting of PCEA at the headquarters of Susquehanna International Group (SIG)*, Bala Cynwyd, PA, March 27 2017.

[3] Technical Program Committee (TPC). ACM MobiHoc 2017 conference. *Steven Weber atteneded the Technical Program Committee meeting for ACM MobiHoc 2017 conference*, Los Angeles, CA, March 24 2017.

[4] Steven Weber. National Science Foundation. *Dr. Weber attended the National Science Foundation Secure and Trustworthy Computing (NSF-SaTC) principle investigator (PI) meeting*, Washington, DC, January 9 2017.

[5] Steven Weber. *NSA Center of Academic Excellence Program Community Annual Meeting*, Kansas City MO, November 3 2016.

[6] NIST National Initiative on Cybersecurity Education (NICE) Annual Conference. NIST. Kansas City MO, November 1 -2 2016.

[7] CISSE/ISEW. Steven Weber. *2016 Colloquium for Information Systems Security Education (CISSE) And International Security Education Workshop (ISEW)*, Sheraton Society Hill Hotel Philadelphia PA, June 13 -15 2016.

[8] NetDiligence. Steven Weber and Mark Greisiger. *NetDiligence annual Conference*, Hyatt Bellevue hotel downtown, June 7 - 8 2016.

[9] National Security Agency. Steven Weber. *First NSA Signal Information Directorate Senior Executive Academic Liaison (SID SEAL) Day*, Ft. Meade, June 1 2016.

[10] Steven Weber. *Attended the fourth annual "day with the U.S. Army Reserve." Discussion about developments in the USAR-P3i-Cyber program*, U.S. Chamber of Commerce in Washington D.C., May 5 2016.

7.4 Bsides Philly

The first annual BSides Philadelphia Security Conference was held on December 2-3, 2016 on the Drexel campus. The BSides conferences are held in major cities across the nation, and are designed to provide an opportunity for the security community in the city to meet and exchange knowledge. BSides Philadelphia was organized by Mr. Brad Bowers. More information about Philly BSides Conference can be found here:https://www.bsidesphilly.org/.

Figure 8: BSides Philly Conference logo

7.5 Philadelphia Security Shell

Philly Security Shell is intended to be a meetup focused on hands-on learning and networking for those interested in information security. The community meets monthly on the third Thursday of the month. Other than their regular meetups, they organize or announce events related to cybersecurity in the Philadelphia area. Since June 2016, the Institute has hosted the monthly meetup at the Auerbach and Berger Cybersecurity Lab. The main organizers for this community are Leonardo Serrano and Chris Rossi. The meetings are open to everyone with an interest in cybersecurity. More information about this community can be found on their website here:https://www.meetup.com/Philly-Shell-info-sec-meetup/.

7.6 Newsletter

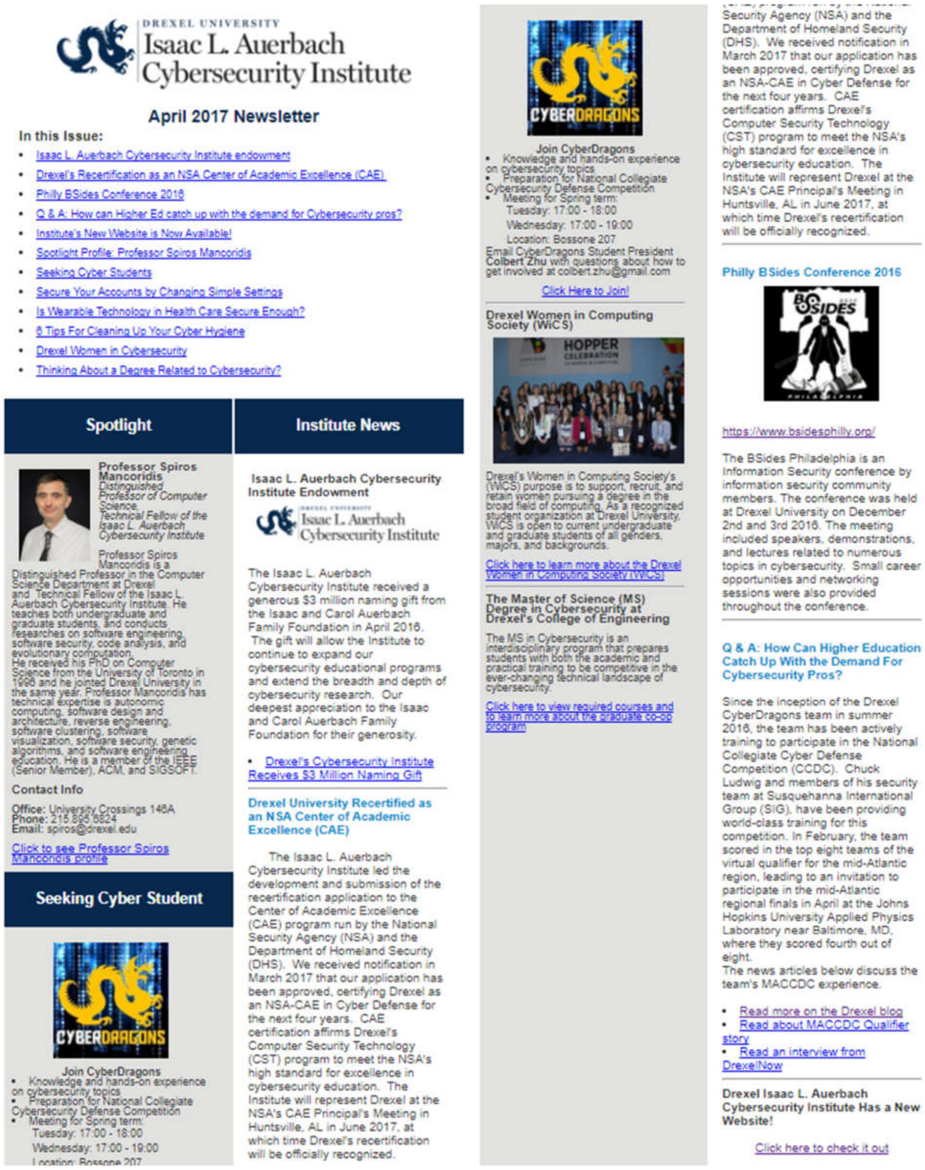
The ILACI had produced a “near-monthly” newsletter, which is distributed to the ILACI “community”. The newsletters have been developed by Norm Balchunas, Dionne Queen, Brenda Sheridan, and Kerry Boland until 2015. Since the beginning of the year 2017, the ”near-quarterly” newsletters have been produced by Institute’s student coordinator coop.

December, 2014
November, 2014
October, 2014
August, 2014
July, 2014
June, 2014
May, 2014
March, 2014
February, 2014

December, 2015
November, 2015
October, 2015
September, 2015
June, 2015
May, 2015
April, 2015
March, 2015
February, 2015
January, 2015

April, 2017

A snapshot of a portion of the April, 2017 newsletter is shown in Fig. 9.



DREXEL UNIVERSITY
Isaac L. Auerbach
Cybersecurity Institute

April 2017 Newsletter

In this Issue:

- Isaac L. Auerbach Cybersecurity Institute endowment
- Drexel's Recertification as an NSA Center of Academic Excellence (CAE)
- Philly BSides Conference 2016
- Q & A: How can Higher Ed catch up with the demand for Cybersecurity pros?
- Institute's New Website is Now Available!
- Spotlight Profile: Professor Spiros Mancoridis
- Seeking Cyber Students
- Secure Your Accounts by Changing Simple Settings
- Is Wearable Technology in Health Care Secure Enough?
- 6 Tips For Cleaning Up Your Cyber Hygiene
- Drexel Women in Cybersecurity
- Thinking About a Degree Related to Cybersecurity?

Spotlight

Professor Spiros Mancoridis
Distinguished Professor of Computer Science,
Technical Fellow of the Isaac L. Auerbach Cybersecurity Institute

Professor Spiros Mancoridis is a Distinguished Professor in the Computer Science Department at Drexel and Technical Fellow of the Isaac L. Auerbach Cybersecurity Institute. He teaches both undergraduate and graduate students, and conducts researches on software engineering, software security, code analysis, and evolutionary computation.
He received his PhD on Computer Science from the University of Toronto in 1996 and he jointed Drexel University in the same year. Professor Mancoridis has technical expertise is autonomic computing, software design and architecture, reverse engineering, software clustering, software visualization, software security, genetic algorithms, and software engineering education. He is a member of the IEEE (Senior Member), ACM, and SIGSOFT.

Contact Info

Office: University Crossings 146A
Phone: 215.895.6824
Email: spiros@drexel.edu

Click to see Professor Spiros Mancoridis profile

Seeking Cyber Student

Join CyberDragons
- Knowledge and hands-on experience on cybersecurity topics
- Preparation for National Collegiate Cybersecurity Defense Competition
- Meeting for Spring term:
  Tuesday: 17:00 - 18:00
  Wednesday: 17:00 - 19:00
  Location: Bossone 207

Institute News

Isaac L. Auerbach Cybersecurity Institute Endowment

DREXEL UNIVERSITY
Isaac L. Auerbach
Cybersecurity Institute

The Isaac L. Auerbach Cybersecurity Institute received a generous $3 million naming gift from the Isaac and Carol Auerbach Family Foundation in April 2016. The gift will allow the Institute to continue to expand our cybersecurity educational programs and extend the breadth and depth of cybersecurity research. Our deepest appreciation to the Isaac and Carol Auerbach Family Foundation for their generosity.

- Drexel's Cybersecurity Institute Receives $3 Million Naming Gift

Drexel University Recertified as an NSA Center of Academic Excellence (CAE)

The Isaac L. Auerbach Cybersecurity Institute led the development and submission of the recertification application to the Center of Academic Excellence (CAE) program run by the National Security Agency (NSA) and the Department of Homeland Security (DHS). We received notification in March 2017 that our application has been approved, certifying Drexel as an NSA-CAE in Cyber Defense for the next four years. CAE certification affirms Drexel's Computer Security Technology (CST) program to meet the NSA's high standard for excellence in cybersecurity education. The Institute will represent Drexel at the NSA's CAE Principal's Meeting in Huntsville, AL in June 2017, at which time Drexel's recertification will be officially recognized.

CYBERDRAGONS

Join CyberDragons
- Knowledge and hands-on experience on cybersecurity topics
- Preparation for National Collegiate Cybersecurity Defense Competition
- Meeting for Spring term:
  Tuesday: 17:00 - 18:00
  Wednesday: 17:00 - 19:00
  Location: Bossone 207

Email CyberDragons Student President **Colbert Zhu** with questions about how to get involved at colbert.zhu@gmail.com

Click Here to Join!

Drexel Women in Computing Society (WiCS)

Drexel's Women in Computing Society's (WiCS) purpose is to support, recruit, and retain women pursuing a degree in the broad field of computing. As a recognized student organization at Drexel University, WiCS is open to current undergraduate and graduate students of all genders, majors, and backgrounds.

Click here to learn more about the Drexel Women in Computing Society (WiCS)

The Master of Science (MS) Degree in Cybersecurity at Drexel's College of Engineering

The MS in Cybersecurity is an interdisciplinary program that prepares students with both the academic and practical training to be competitive in the ever-changing technical landscape of cybersecurity.

Click here to view required courses and to learn more about the graduate co-op program

Security Agency (NSA) and the Department of Homeland Security (DHS). We received notification in March 2017 that our application has been approved, certifying Drexel as an NSA-CAE in Cyber Defense for the next four years. CAE certification affirms Drexel's Computer Security Technology (CST) program to meet the NSA's high standard for excellence in cybersecurity education. The Institute will represent Drexel at the NSA's CAE Principal's Meeting in Huntsville, AL in June 2017, at which time Drexel's recertification will be officially recognized.

Philly BSides Conference 2016

https://www.bsidesphilly.org/

The BSides Philadelphia is an Information Security conference by information security community members. The conference was held at Drexel University on December 2nd and 3rd 2016. The meeting included speakers, demonstrations, and lectures related to numerous topics in cybersecurity. Small career opportunities and networking sessions were also provided throughout the conference.

Q & A: How Can Higher Education Catch Up With the Demand For Cybersecurity Pros?

Since the inception of the Drexel CyberDragons team in summer 2016, the team has been actively training to participate in the National Collegiate Cyber Defense Competition (CCDC). Chuck Ludwig and members of his security team at Susquehanna International Group (SIG), have been providing world-class training for this competition. In February, the team scored in the top eight teams of the virtual qualifier for the mid-Atlantic region, leading to an invitation to participate in the mid-Atlantic regional finals in April at the Johns Hopkins University Applied Physics Laboratory near Baltimore, MD, where they scored fourth out of eight.
The news articles below discuss the team's MACCDC experience.

- Read more on the Drexel blog
- Read about MACCDC Qualifier story
- Read an interview from DrexelNow

Drexel Isaac L. Auerbach Cybersecurity Institute Has a New Website!

Click here to check it out

Figure 9: Snapshot of the April, 2017 newsletter.

8 In The News

Three Drexel faculty regularly interviewed by the media are *i*) Steven Weber (CoE), *ii*) Rob D'Ovidio (CoAS), and *iii*) Rachel Greenstadt (CCI) *iv*) Kapil Dandekar (CoE).

Steven Weber
Interim Dept. Head
Professor, CoE
Mathematical Modeling of
Computer

Rob D'Ovidio
Associate Professor, CoAS
Digital forensics and Cyber crime

Rachel Greenstadt
Associate Professor, CCI
Privacy and security

Kapil Dandekar
Professor, CoE
Wireless physical layer security

Figure 10: Three Drexel faculty regularly interviewed by the media.

Drexel cybersecurity-related activities mentioned in the news include:

[1] Britt Faulstick. Drexel named center of academic excellence for cybersecurity education. *Drexel Now*, June 28, 2017.

[2] Lauren Mayk. Global Cyberattack Concerns Go Local. *NBC 10*, May 15, 2017.

[3] Ben Seal. Drexel Cybersecurity Team's first season marked by 'Amazing' growth. *Drexel Now*, April 13, 2017.

[4] Natalie Gross. 10 schools top new ranking of best cybersecurity programs. *Military Times*, April 3, 2017.

[5] Britt Faulstick. How can higher ed catch up with the demand for cybersecurity pros? *Drexel University Drexel News Blog*, March 20, 2017.

[6] Drexel student team qualifies for Mid-Atlantic Collegiate Cyber Defense Competition. *College of Computing and informatics*, March 13, 2017.

[7] Ian Bush. Team of drexel students compete against the best in computer programming and defense. *CBS Philly News*, January 28, 2017.

[8] Melony Roy. Hacker has message for President Trump: Change your security settings. *CBS News*, January 27, 2017.

[9] Harold Brubaker. Wearable tech gaining in healthcare, but privacy is a concern. *Philly Inquirer*, January 20, 2017.

[10] Britt Faulstick. Drexel Team Eyes Collegiate Cyber Defense Competition. *DrexelNow*, January 11, 2017.

[11] Britt Faulstick. Were You Part of a Cyberattack? *Drexel News Blog*, October 27, 2016. Quotes Gaurav Naik.

[12] Steven Weber and David Whipple. ”6 tips for cleaning up your cyber hygiene”. *Drexel University Online (DUO) blog post The Digital Dragon*, October 18, 2016.

[13] Darlene Storm. Attackers hacked Department of Energy 159 times in 4 years. *ComputerWorld*, September 14, 2015. Quotes Scott White.

[14] Andrew Blake. Energy Dept. computers breached 159 times since 2010: Report. *The Washington Times*, September 10, 2015. Quotes Scott White.

[15] Steve Reilly. Records: Energy Department struck by cyber attacks. *CNBC*, September 10, 2015. Quotes Scott White.

[16] Britt Faulstick. Staying Ahead of the Hackers. *Drexel News Blog*, August 20, 2015. Profiles the DCI, Drexel cybersecurity education, and Drexel cybersecurity research, quotes Kapil Dandekar.

[17] Joel Wee. Demand for jobs high in cyber security. *Philadelphia Inquirer*, August 16, 2015. Quotes Steven Weber and Kapil Dandekar.

[18] Juliana Reyes. Why Drexel’s Rachel Greenstadt is a big deal in the privacy technology scene. *Technical.ly Philly*, July 28, 2015. Interview with Rachel Greenstadt about the Drexel PSAL.

[19] Juliana Reyes. Inside Philadelphias growing internet privacy community. *Technical.ly Philly*, July 8, 2015. Interview with Rachel Greenstadt about PETS 2015 and the Drexel PSAL.

[20] Amber Corrin. Army Reserves train the next generation’s cyber force. *Federal Times*, June 23, 2015. Interview with Erin Thede of USAR Private Public Partnership Office.

[21] SmartBrief Editor. How strong is your IT security desk? *CompTIA SmartBlog on Education*, June 5, 2015. Interview with Steven Weber about cybersecurity.

[22] Michael Keating. Hunting cybersecurity talent. *American City and County*, April 20, 2015. Quotes Steven Weber.

[23] Nicolena Stiles. U.S. Army Reserve partners with universities to create cyber security program. *The Drexel Triangle*, February 22, 2015. Interview with Steven Weber.

[24] Frank Otto. Drexel Cybersecurity Institute Director Receives Veteran Award. *Drexel NOW*, February 13, 2015. Interviews Norm Balchunas, a Philadelphia Business Journal 2015 Veteran of Influence.

[25] Juliana Reyes. Drexel is now one of 6 cybersecurity training centers for the US Army Reserve. *Technical.ly Philly*, February 11, 2015. Discusses USAR P3i program and quotes Norm Balchunas.

[26] Lauren Hertzler. Drexel, U.S. Army Reserve team up to train cyber soldiers. *Philadelphia Business Journal*, February 10, 2015. Discusses USAR P3i program and quotes Norm Balchunas.

[27] Staff writer. Drexel Cybersecurity Institute And U.S. Army Reserve to Train Next Generation of Cyber Soldiers. *Drexel NOW*, February 10, 2015. Discusses USAR P3i program and quotes Norm Balchunas.

[28] Todd Bookman. After Anthem data breach, area insurers vigilant against evolving threat. *NewsWorks*, February 9, 2015. Quotes Rob D’Ovidio.

[29] Lane Blackmer. Drexel partners with U.S. Army on cybersecurity. *Philly Voice*, February 6, 2015. Discusses USAR P3i program and quotes Norm Balchunas.

[30] Britt Faulstick. Online Shopping Safety Tips From The Drexel Cybersecurity Institute. *Drexel News Blog*, November 25, 2014.

[31] Lauren Hertzler. A cyber breach: more likely than a fire. *Philadelphia Business Journal*, June 13, 2014. Quotes Norm Balchunas and Rob D’Ovidio.

[32] Dustin Slaughter. Military and Intelligence Interests Grow at Drexel University. *The Philly Declaration*, June 6, 2014. Discusses launch of DCI, quotes Norm Balchunas.

[33] Staff writer. Drexel opens Auerbach and Berger Families Cybersecurity Laboratory. *Drexel CCI Press Release*, June 2, 2014. Mentions John Fry, David Fenske, Carol Auerbach, Albert Berger, Walter Straub, and Harvey Rishikof.

[34] Lauren Hertzler. Scams expected to hit customers hard after eBay data breach. *Philadelphia Business Journal*, May 25, 2014. Quotes Norm Balchunas.

[35] Tim Jimenez. Drexel U. Cybersecurity Expert Says Chinese Hackers Used Some Simple Tricks. *CBS Philly*, May 19, 2014. Quotes Rob DÓvidio.

[36] Evan Halper. Security holes in power grid have federal officials scrambling. *Los Angeles Times*, April 7, 2014. Quotes Scott White.

[37] Ryan Zimmerman. Cyber Security Research Alliance Initiates First Research and Development Projects with Drexel University and George Mason University. *Cyber Security Research Alliance (CSRA) Press Release*, March 24, 2014. Interviews Spiros Mancoridis about CSRA grant.

[38] Ian Bush. Drexel University Opens Its New Cybersecurity Institute. *CBS Philly*, February 24, 2014. Quotes Norm Balchunas and John Fry.

[39] Staff writer. Drexel Opens Cybersecurity Institute. *Drexel NOW*, February 24, 2014. Quotes David Fenske, Norm Balchunas, John Fry.

[40] Geoff Williams. 5 Things You Probably Didn't Know About Identity Theft. *U.S. News and World Report*, December 18, 2013. Quotes Rob DÓvidio.

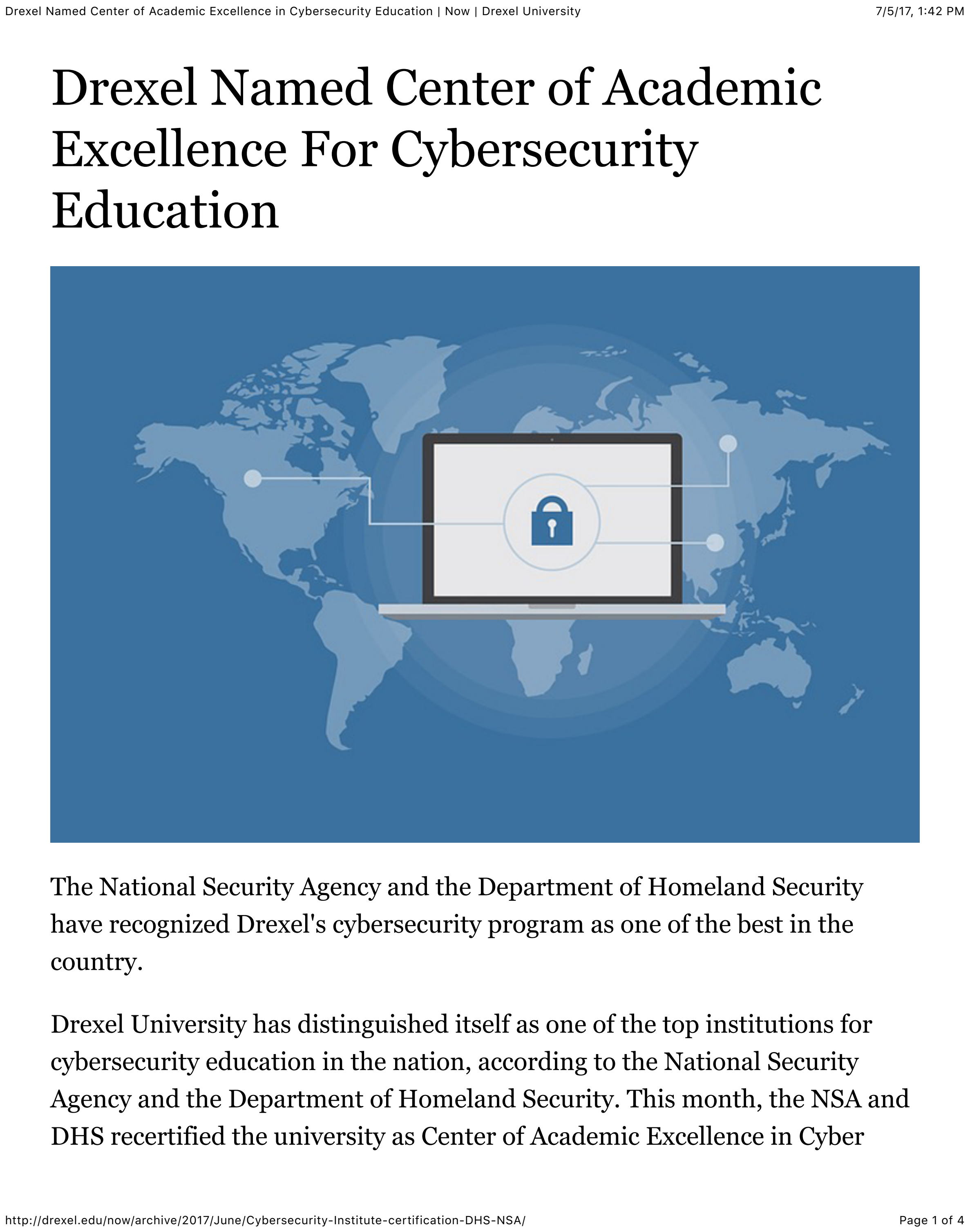
[41] Laura Bennett. This Computer Program Turns Famous Writers Into Anonymous Hacks. *The New Republic*, July 31, 2013. Features Rachel Greenstadt and her Anonymouth software.

[42] Sue Gee. Anonymouth Hides Identity. *I Programmer*, August 4, 2013. Features Rachel Greenstadt and her Anonymouth software.

[43] Pierluigi Paganini. Stylometric analysis to track anonymous users in the underground. *Security Affairs*, January 10, 2013. Features Rachel Greenstadt and her Anonymouth software.

[44] Nicole Perlroth. Software Helps Identify Anonymous Writers or Helps Them Stay That Way. *New York Times Bits Blog*, January 3, 2012. Features Rachel Greenstadt and her Anonymouth software.

Snapshots of some of these articles are shown on the following pages.



Drexel Named Center of Academic Excellence in Cybersecurity Education | Now | Drexel University 7/5/17, 1:42 PM

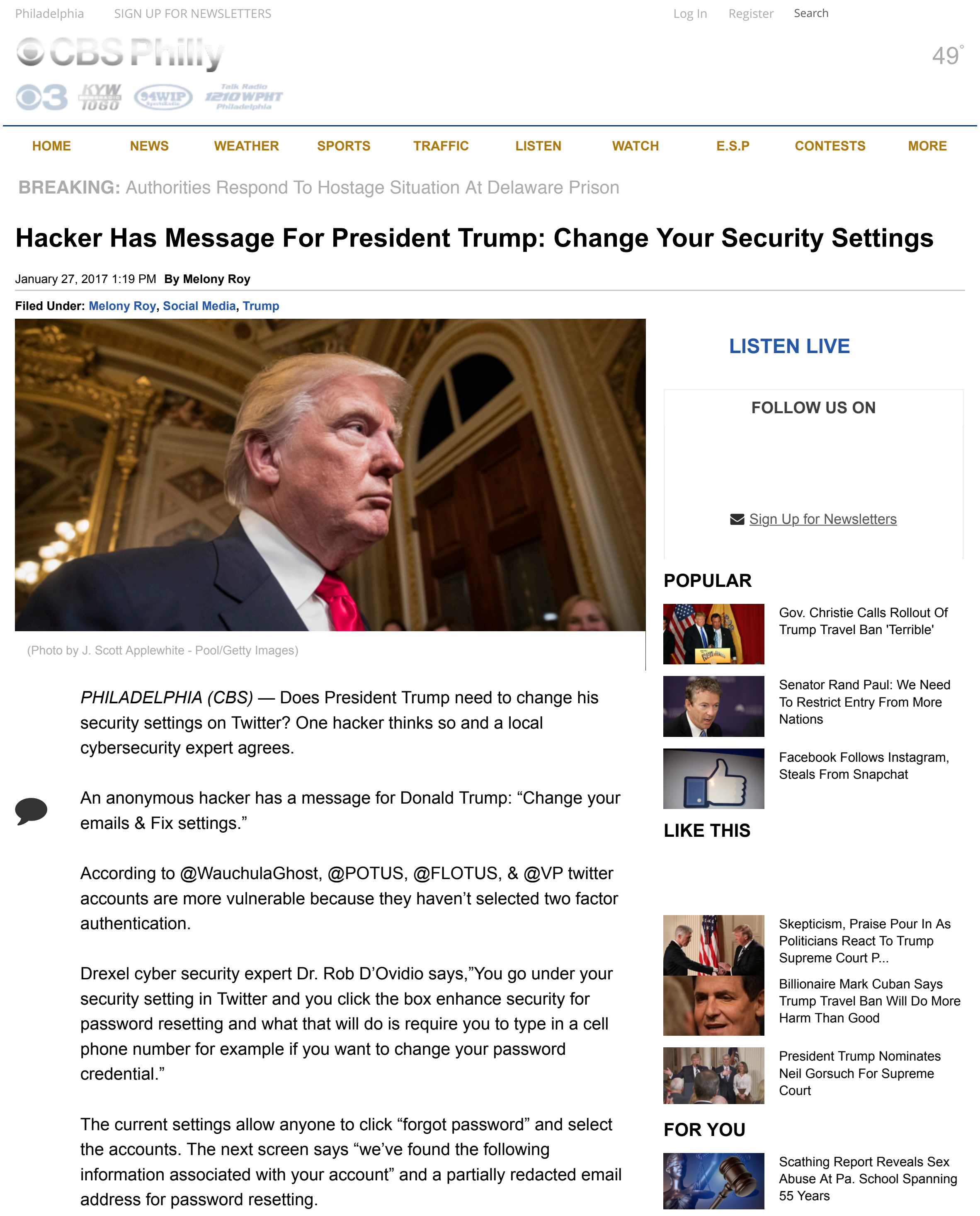
Drexel Named Center of Academic Excellence For Cybersecurity Education

The National Security Agency and the Department of Homeland Security have recognized Drexel's cybersecurity program as one of the best in the country.

Drexel University has distinguished itself as one of the top institutions for cybersecurity education in the nation, according to the National Security Agency and the Department of Homeland Security. This month, the NSA and DHS recertified the university as Center of Academic Excellence in Cyber

http://drexel.edu/now/archive/2017/June/Cybersecurity-Institute-certification-DHS-NSA/ Page 1 of 4

Figure 11: Drexel Now – June 28, 2017.



BREAKING: Authorities Respond To Hostage Situation At Delaware Prison

Hacker Has Message For President Trump: Change Your Security Settings

January 27, 2017 1:19 PM **By Melony Roy**

Filed Under: Melony Roy, Social Media, Trump

(Photo by J. Scott Applewhite - Pool/Getty Images)

PHILADELPHIA (CBS) — Does President Trump need to change his security settings on Twitter? One hacker thinks so and a local cybersecurity expert agrees.

An anonymous hacker has a message for Donald Trump: "Change your emails & Fix settings."

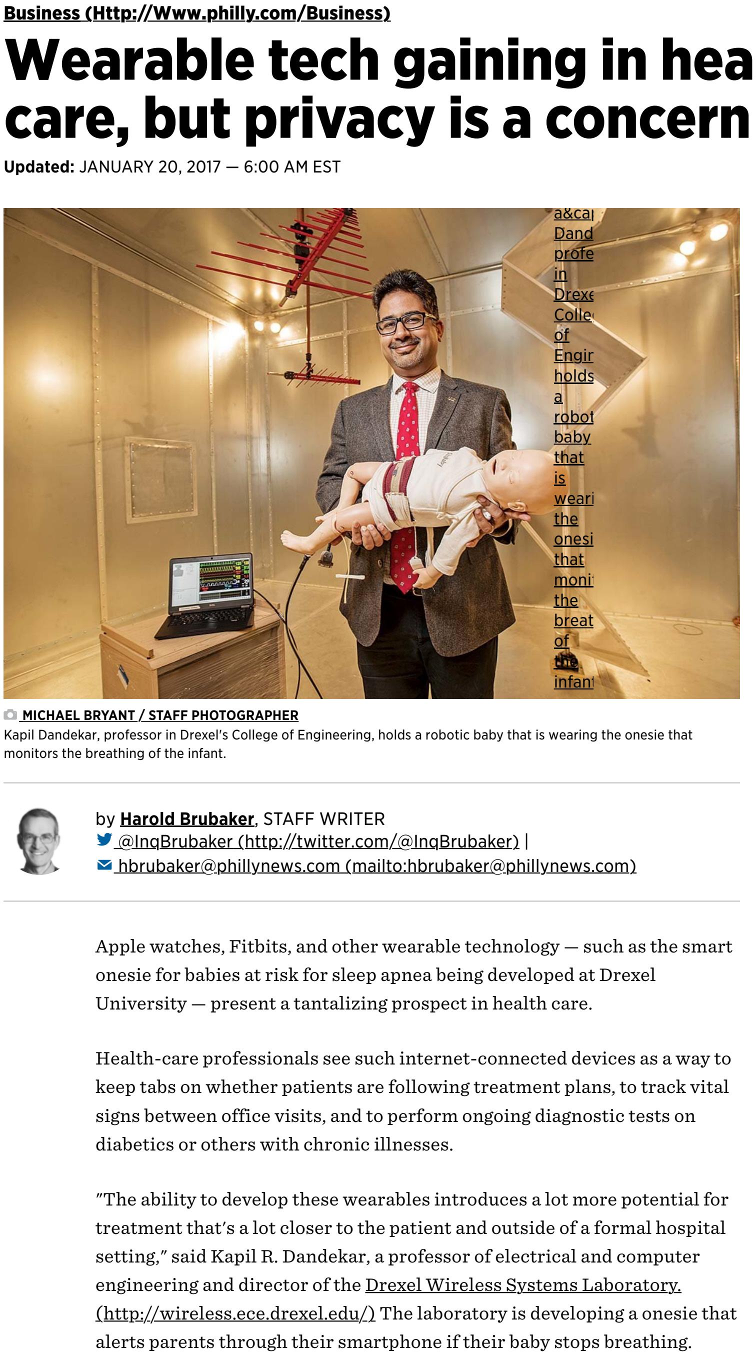
According to @WauchulaGhost, @POTUS, @FLOTUS, & @VP twitter accounts are more vulnerable because they haven't selected two factor authentication.

Drexel cyber security expert Dr. Rob D'Ovidio says,"You go under your security setting in Twitter and you click the box enhance security for password resetting and what that will do is require you to type in a cell phone number for example if you want to change your password credential."

The current settings allow anyone to click "forgot password" and select the accounts. The next screen says "we've found the following information associated with your account" and a partially redacted email address for password resetting.

LISTEN LIVE
FOLLOW US ON
Sign Up for Newsletters
POPULAR
Gov. Christie Calls Rollout Of Trump Travel Ban 'Terrible'
Senator Rand Paul: We Need To Restrict Entry From More Nations
Facebook Follows Instagram, Steals From Snapchat
LIKE THIS
Skepticism, Praise Pour In As Politicians React To Trump Supreme Court P...
Billionaire Mark Cuban Says Trump Travel Ban Will Do More Harm Than Good
President Trump Nominates Neil Gorsuch For Supreme Court
FOR YOU
Scathing Report Reveals Sex Abuse At Pa. School Spanning 55 Years

Figure 12: CBS News – January 27, 2017.



Business (Http://Www.philly.com/Business)

Wearable tech gaining in health care, but privacy is a concern

Updated: JANUARY 20, 2017 — 6:00 AM EST

MICHAEL BRYANT / STAFF PHOTOGRAPHER

Kapil Dandekar, professor in Drexel's College of Engineering, holds a robotic baby that is wearing the onesie that monitors the breathing of the infant.

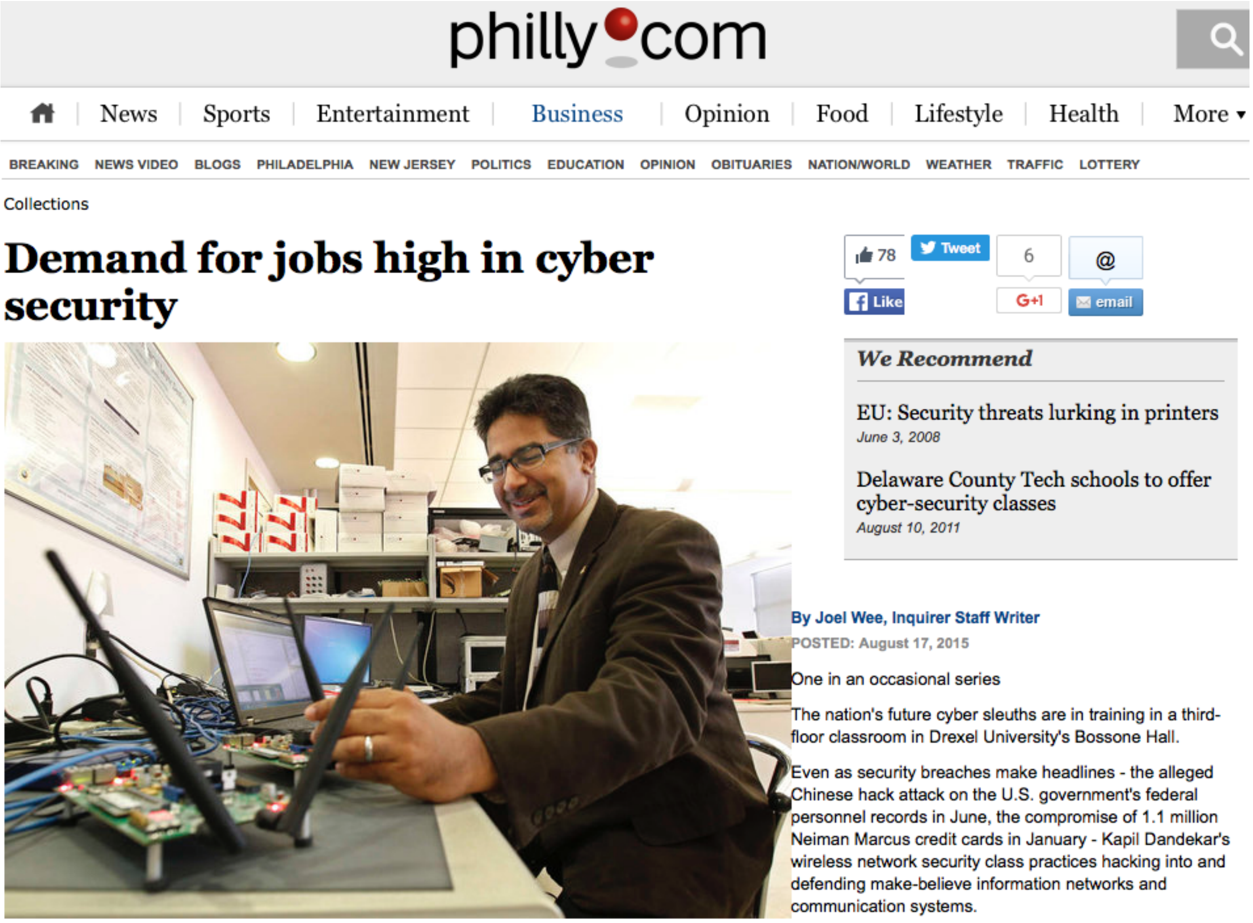
by **Harold Brubaker**, STAFF WRITER
@InqBrubaker (http://twitter.com/@InqBrubaker) |
hbrubaker@phillynews.com (mailto:hbrubaker@phillynews.com)

Apple watches, Fitbits, and other wearable technology — such as the smart onesie for babies at risk for sleep apnea being developed at Drexel University — present a tantalizing prospect in health care.

Health-care professionals see such internet-connected devices as a way to keep tabs on whether patients are following treatment plans, to track vital signs between office visits, and to perform ongoing diagnostic tests on diabetics or others with chronic illnesses.

"The ability to develop these wearables introduces a lot more potential for treatment that's a lot closer to the patient and outside of a formal hospital setting," said Kapil R. Dandekar, a professor of electrical and computer engineering and director of the Drexel Wireless Systems Laboratory. (http://wireless.ece.drexel.edu/) The laboratory is developing a onesie that alerts parents through their smartphone if their baby stops breathing.

Figure 13: Technical.ly Philly – January 20, 2017.


philly.com
News | Sports | Entertainment | Business | Opinion | Food | Lifestyle | Health | More ▾
BREAKING NEWS VIDEO BLOGS PHILADELPHIA NEW JERSEY POLITICS EDUCATION OPINION OBITUARIES NATION/WORLD WEATHER TRAFFIC LOTTERY
Collections
78
Like
Tweet
6
G+1
@
email

Demand for jobs high in cyber security

We Recommend

EU: Security threats lurking in printers
June 3, 2008

Delaware County Tech schools to offer cyber-security classes
August 10, 2011

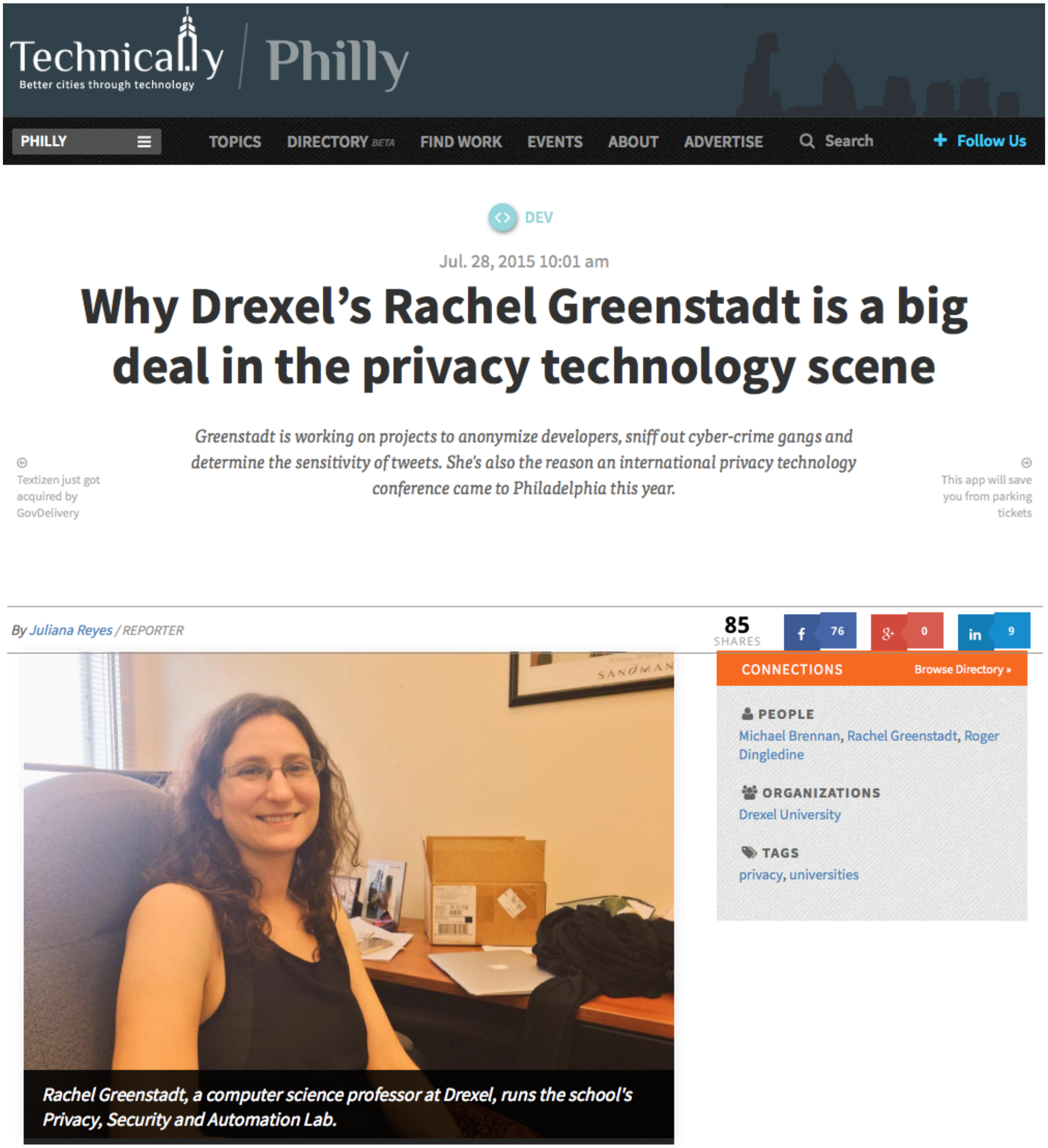
By Joel Wee, Inquirer Staff Writer
POSTED: August 17, 2015

One in an occasional series

The nation's future cyber sleuths are in training in a third-floor classroom in Drexel University's Bossone Hall.

Even as security breaches make headlines - the alleged Chinese hack attack on the U.S. government's federal personnel records in June, the compromise of 1.1 million Neiman Marcus credit cards in January - Kapil Dandekar's wireless network security class practices hacking into and defending make-believe information networks and communication systems.

Figure 14: Technical.ly Philly – August 17, 2015.



Jul. 28, 2015 10:01 am

Why Drexel's Rachel Greenstadt is a big deal in the privacy technology scene

Greenstadt is working on projects to anonymize developers, sniff out cyber-crime gangs and determine the sensitivity of tweets. She's also the reason an international privacy technology conference came to Philadelphia this year.

Textizen just got acquired by GovDelivery

This app will save you from parking tickets

By *Juliana Reyes* / *REPORTER*

CONNECTIONS Browse Directory »

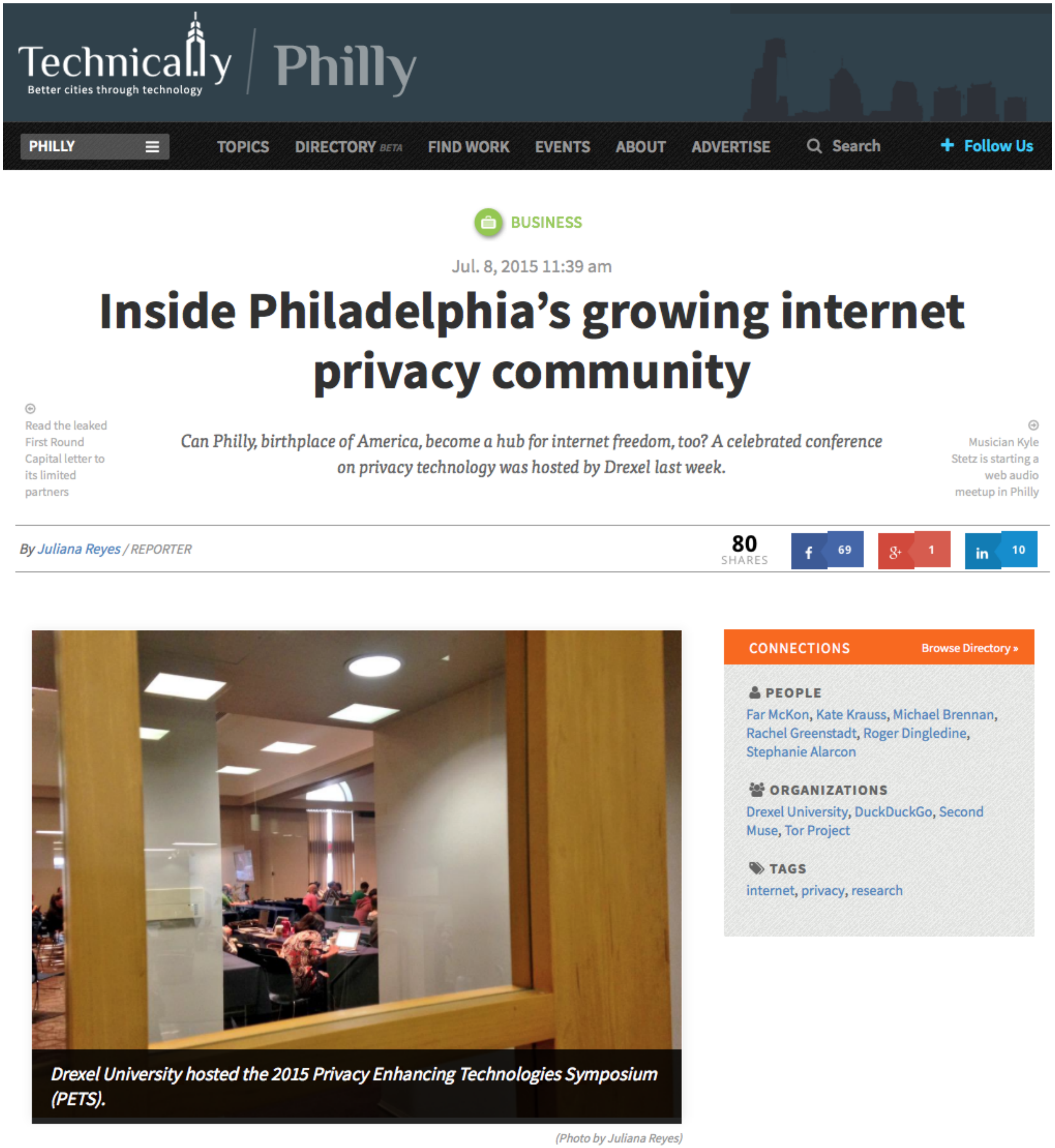
PEOPLE
Michael Brennan, Rachel Greenstadt, Roger Dingledine

ORGANIZATIONS
Drexel University

TAGS
privacy, universities

Rachel Greenstadt, a computer science professor at Drexel, runs the school's Privacy, Security and Automation Lab.

Figure 15: Technical.ly Philly – July 28, 2015.


Technical.ly
Better cities through technology
Philly
PHILLY
TOPICS
DIRECTORY BETA
FIND WORK
EVENTS
ABOUT
ADVERTISE
Search
+ Follow Us
Read the leaked First Round Capital letter to its limited partners
Musician Kyle Stetz is starting a web audio meetup in Philly
80 SHARES
69
1
10

BUSINESS

Jul. 8, 2015 11:39 am

Inside Philadelphia's growing internet privacy community

Can Philly, birthplace of America, become a hub for internet freedom, too? A celebrated conference on privacy technology was hosted by Drexel last week.

By Juliana Reyes / REPORTER

Drexel University hosted the 2015 Privacy Enhancing Technologies Symposium (PETS).

(Photo by Juliana Reyes)

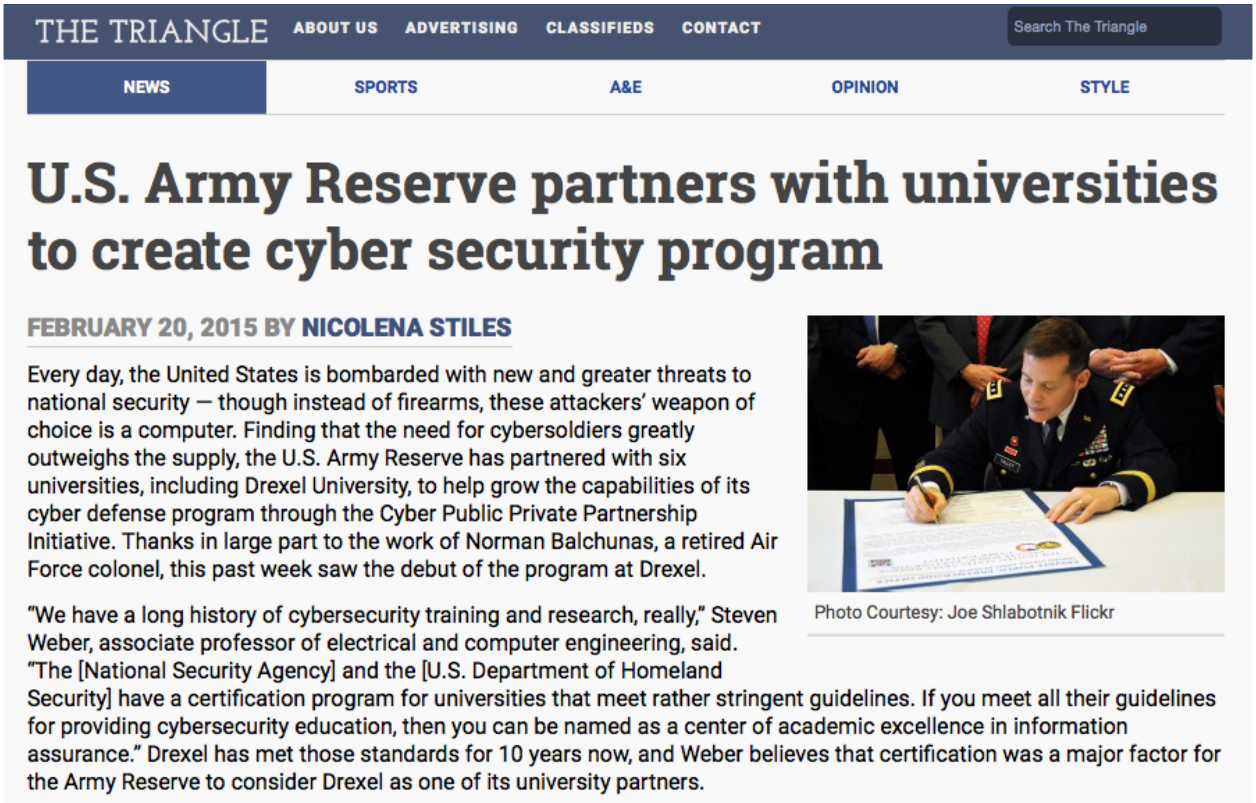
CONNECTIONS Browse Directory »

PEOPLE
Far McKon, Kate Krauss, Michael Brennan, Rachel Greenstadt, Roger Dingledine, Stephanie Alarcon

ORGANIZATIONS
Drexel University, DuckDuckGo, Second Muse, Tor Project

TAGS
internet, privacy, research

Figure 16: Technical.ly Philly – July 8, 2015.



U.S. Army Reserve partners with universities to create cyber security program

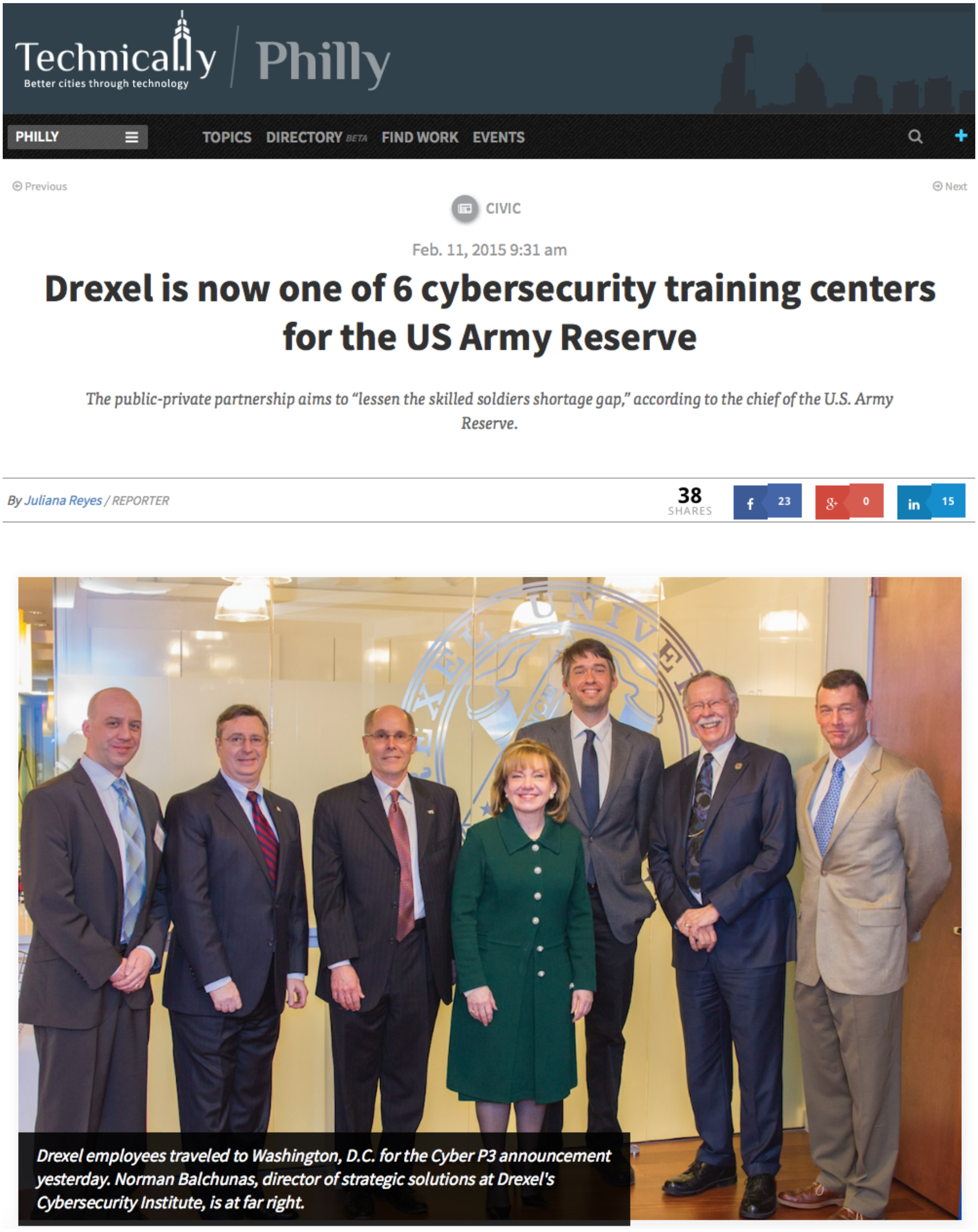
FEBRUARY 20, 2015 BY NICOLENA STILES

Every day, the United States is bombarded with new and greater threats to national security — though instead of firearms, these attackers' weapon of choice is a computer. Finding that the need for cybersoldiers greatly outweighs the supply, the U.S. Army Reserve has partnered with six universities, including Drexel University, to help grow the capabilities of its cyber defense program through the Cyber Public Private Partnership Initiative. Thanks in large part to the work of Norman Balchunas, a retired Air Force colonel, this past week saw the debut of the program at Drexel.

Photo Courtesy: Joe Shlabotnik Flickr

"We have a long history of cybersecurity training and research, really," Steven Weber, associate professor of electrical and computer engineering, said. "The [National Security Agency] and the [U.S. Department of Homeland Security] have a certification program for universities that meet rather stringent guidelines. If you meet all their guidelines for providing cybersecurity education, then you can be named as a center of academic excellence in information assurance." Drexel has met those standards for 10 years now, and Weber believes that certification was a major factor for the Army Reserve to consider Drexel as one of its university partners.

Figure 17: Drexel Triangle – February 20, 2015.



Feb. 11, 2015 9:31 am

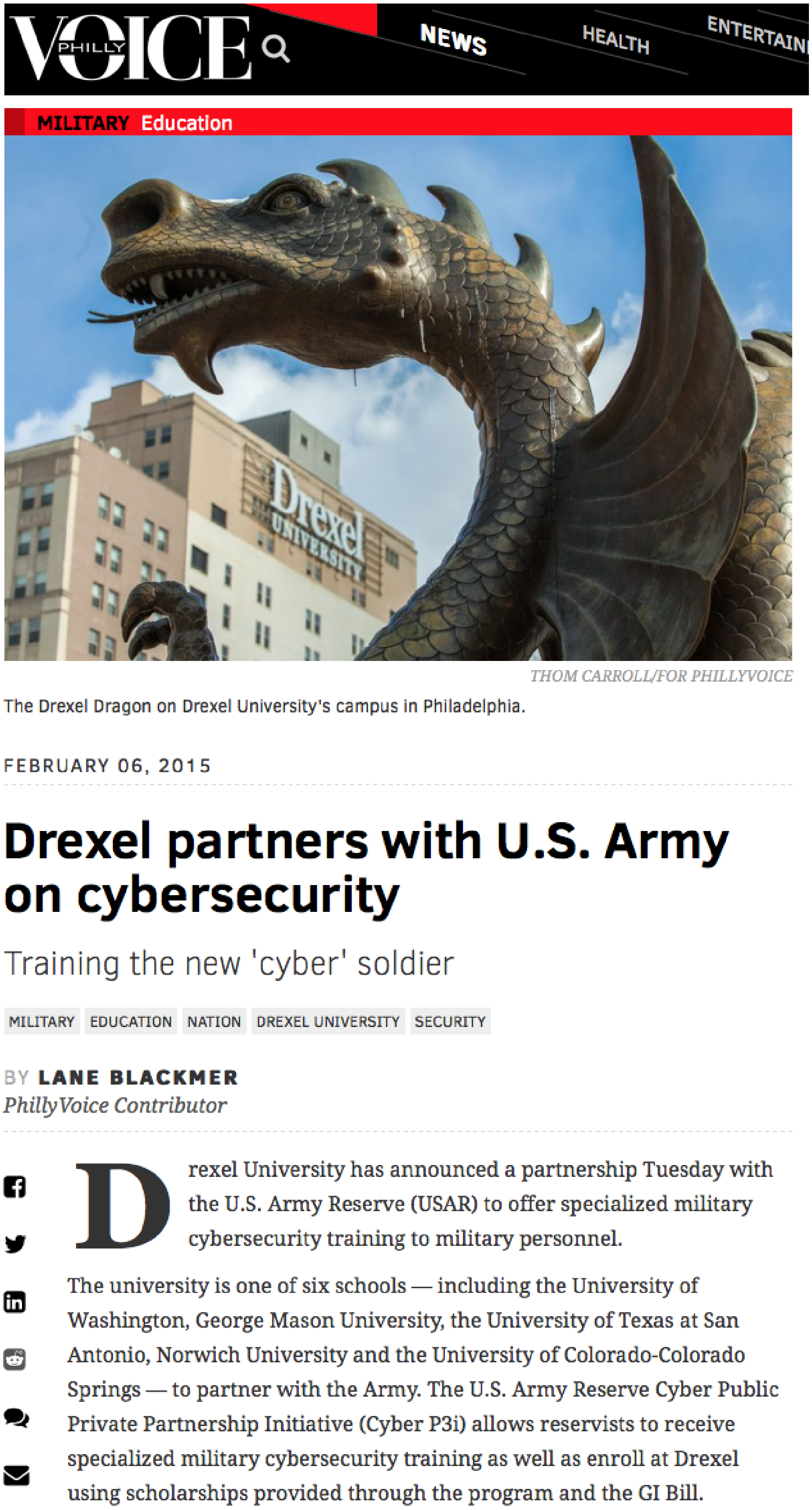
Drexel is now one of 6 cybersecurity training centers for the US Army Reserve

The public-private partnership aims to "lessen the skilled soldiers shortage gap," according to the chief of the U.S. Army Reserve.

By Juliana Reyes / REPORTER

Drexel employees traveled to Washington, D.C. for the Cyber P3 announcement yesterday. Norman Balchunas, director of strategic solutions at Drexel's Cybersecurity Institute, is at far right.

Figure 18: Technical.ly Philly – February 11, 2015.



THOM CARROLL/FOR PHILLYVOICE

The Drexel Dragon on Drexel University's campus in Philadelphia.

FEBRUARY 06, 2015

Drexel partners with U.S. Army on cybersecurity

Training the new 'cyber' soldier

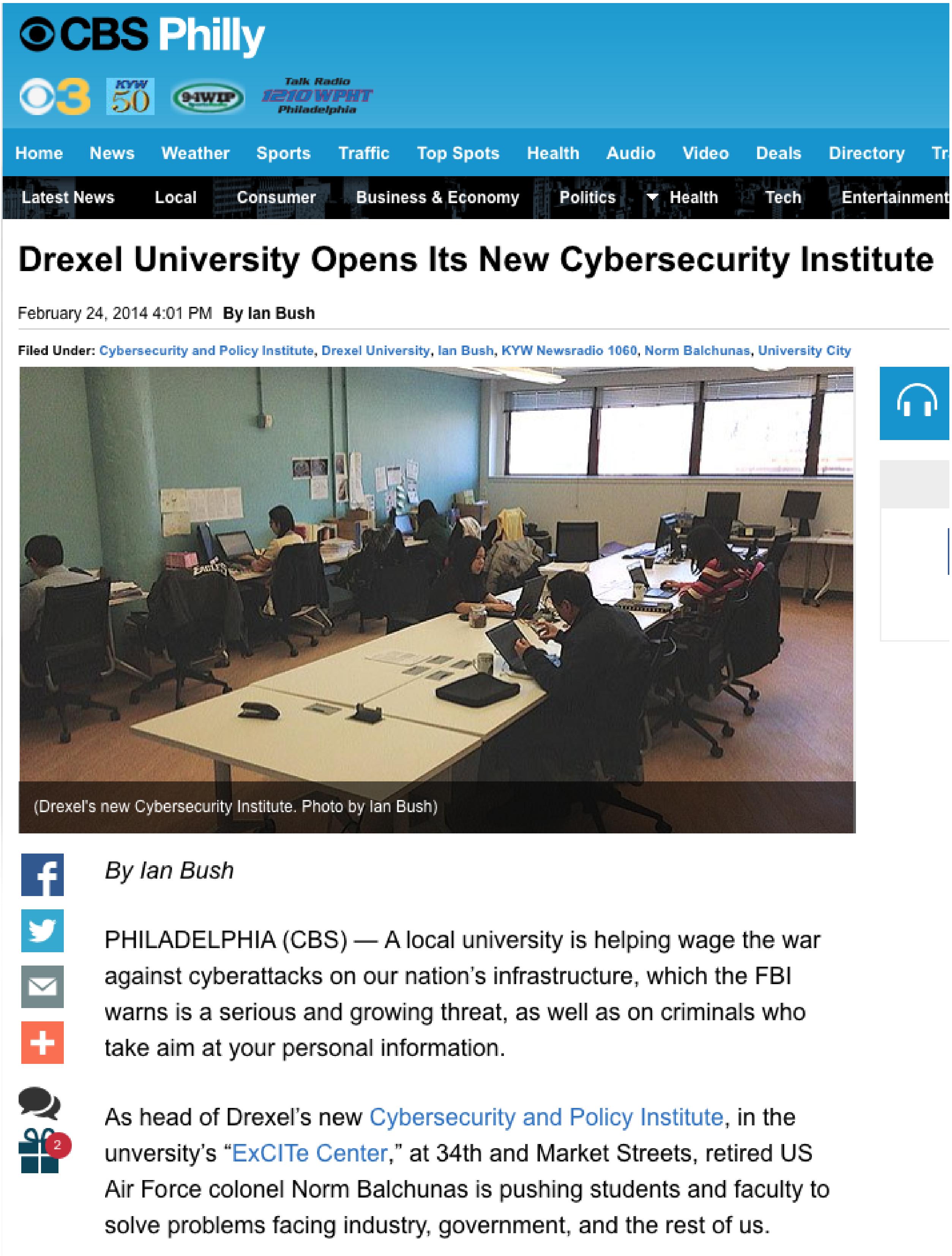
MILITARY EDUCATION NATION DREXEL UNIVERSITY SECURITY

BY **LANE BLACKMER**
PhillyVoice Contributor

Drexel University has announced a partnership Tuesday with the U.S. Army Reserve (USAR) to offer specialized military cybersecurity training to military personnel.

The university is one of six schools — including the University of Washington, George Mason University, the University of Texas at San Antonio, Norwich University and the University of Colorado-Colorado Springs — to partner with the Army. The U.S. Army Reserve Cyber Public Private Partnership Initiative (Cyber P3i) allows reservists to receive specialized military cybersecurity training as well as enroll at Drexel using scholarships provided through the program and the GI Bill.

Figure 19: Philly Voice – February 6, 2015.



Drexel University Opens Its New Cybersecurity Institute

February 24, 2014 4:01 PM **By Ian Bush**

Filed Under: Cybersecurity and Policy Institute, Drexel University, Ian Bush, KYW Newsradio 1060, Norm Balchunas, University City

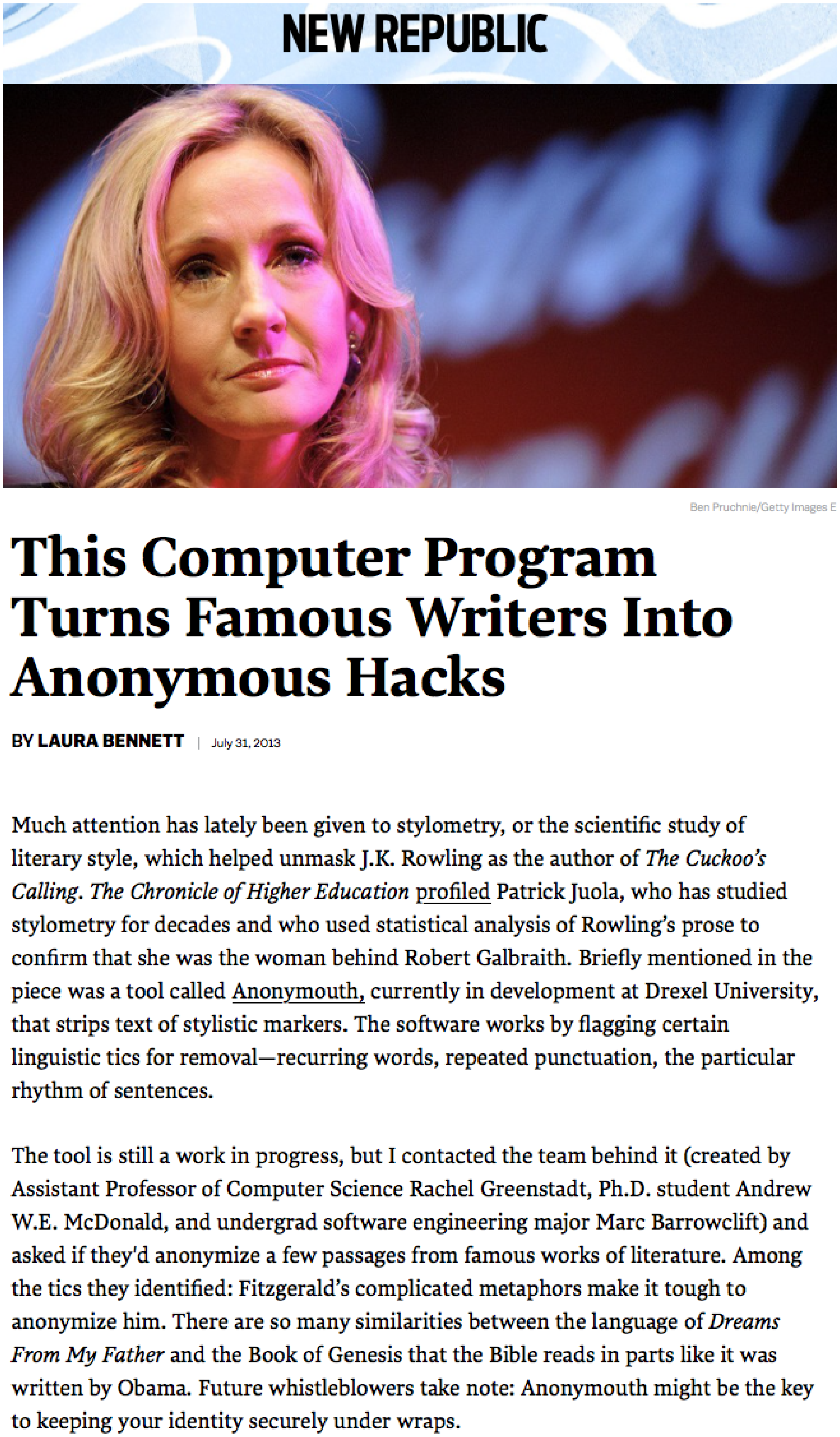
(Drexel's new Cybersecurity Institute. Photo by Ian Bush)

By Ian Bush

PHILADELPHIA (CBS) — A local university is helping wage the war against cyberattacks on our nation's infrastructure, which the FBI warns is a serious and growing threat, as well as on criminals who take aim at your personal information.

As head of Drexel's new Cybersecurity and Policy Institute, in the university's "ExCITe Center," at 34th and Market Streets, retired US Air Force colonel Norm Balchunas is pushing students and faculty to solve problems facing industry, government, and the rest of us.

Figure 20: CBS Philly – February 24, 2014.



NEW REPUBLIC

Ben Pruchnie/Getty Images E

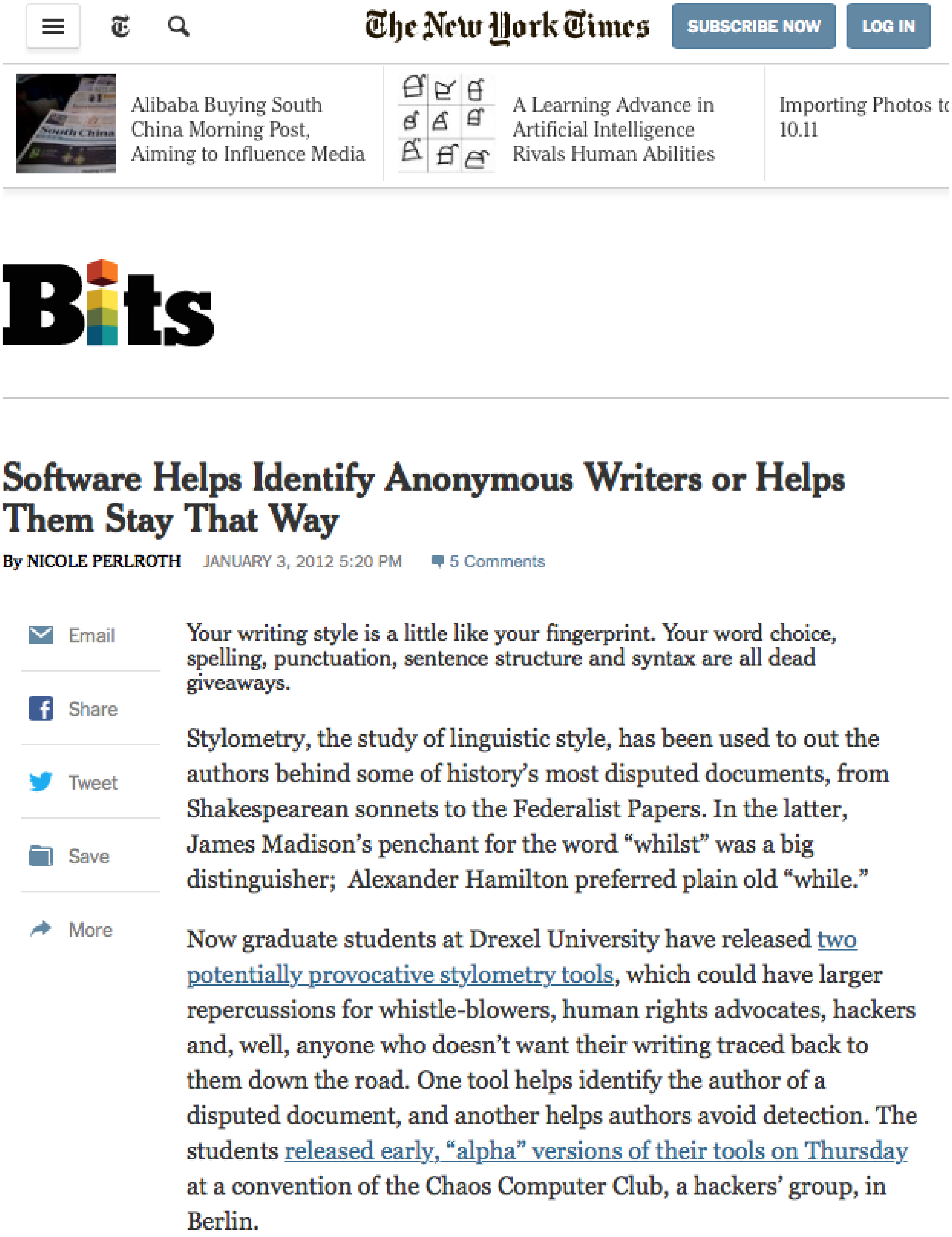
This Computer Program Turns Famous Writers Into Anonymous Hacks

BY **LAURA BENNETT** | July 31, 2013

Much attention has lately been given to stylometry, or the scientific study of literary style, which helped unmask J.K. Rowling as the author of *The Cuckoo's Calling*. *The Chronicle of Higher Education* profiled Patrick Juola, who has studied stylometry for decades and who used statistical analysis of Rowling's prose to confirm that she was the woman behind Robert Galbraith. Briefly mentioned in the piece was a tool called Anonymouth, currently in development at Drexel University, that strips text of stylistic markers. The software works by flagging certain linguistic tics for removal—recurring words, repeated punctuation, the particular rhythm of sentences.

The tool is still a work in progress, but I contacted the team behind it (created by Assistant Professor of Computer Science Rachel Greenstadt, Ph.D. student Andrew W.E. McDonald, and undergrad software engineering major Marc Barrowclift) and asked if they'd anonymize a few passages from famous works of literature. Among the tics they identified: Fitzgerald's complicated metaphors make it tough to anonymize him. There are so many similarities between the language of *Dreams From My Father* and the Book of Genesis that the Bible reads in parts like it was written by Obama. Future whistleblowers take note: Anonymouth might be the key to keeping your identity securely under wraps.

Figure 21: The New Republic – March 31, 2013.


The New York Times
SUBSCRIBE NOW
LOG IN
Alibaba Buying South China Morning Post, Aiming to Influence Media
A Learning Advance in Artificial Intelligence Rivals Human Abilities
Importing Photos tc 10.11
Bits
Email
Share
Tweet
Save
More

Software Helps Identify Anonymous Writers or Helps Them Stay That Way

By NICOLE PERLROTH JANUARY 3, 2012 5:20 PM 5 Comments

Your writing style is a little like your fingerprint. Your word choice, spelling, punctuation, sentence structure and syntax are all dead giveaways.

Stylometry, the study of linguistic style, has been used to out the authors behind some of history's most disputed documents, from Shakespearean sonnets to the Federalist Papers. In the latter, James Madison's penchant for the word "whilst" was a big distinguisher; Alexander Hamilton preferred plain old "while."

Now graduate students at Drexel University have released two potentially provocative stylometry tools, which could have larger repercussions for whistle-blowers, human rights advocates, hackers and, well, anyone who doesn't want their writing traced back to them down the road. One tool helps identify the author of a disputed document, and another helps authors avoid detection. The students released early, "alpha" versions of their tools on Thursday at a convention of the Chaos Computer Club, a hackers' group, in Berlin.

Figure 22: New York Times Bits Blog – January 3, 2012.

9 Contact Us

Steven Weber, Ph.D.
Director

Email: sweber@coe.drexel.edu
Phone: (215) 895-0254
Office: Bossone Research Enterprise Center, 413b

DREXEL UNIVERSITY

Isaac L. Auerbach
Cybersecurity Institute