This overview of the Drexel Cybersecurity Institute 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 Cyberscorps Scholarships for Service (SFS) - 2012–2015
4. NSF Faculty Early Career Development Program (CAREER) - 2013–2018, 2016–2020
8. Office of Naval Research (ONR) - 2015–2018
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

Recent corporate funding sources include Intel, Google, Comcast, the Cyber Security Research Alliance (CSRA), and the Casualty Actuarial Society (CAS).

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. 2015 IEEE International Workshop on Information Forensics and Security (WIFS)
2. 2015 Usenix Security Symposium
3. 2015 Information Security Solutions Europe (ISSE)
4. 2015 International Conference on Malicious and Unwanted Software (MALCON)
5. 2015 International Conference on Quality, Reliability, and Security (QRS)
6. 2015 IEEE International Symposium on Software Reliability Engineering (ISSRE)
7. 2014 ACM SIGCOMM Software Radio Implementation Forum (SRIF)
8. 2014 ACM Conference on Data and Application Security and Privacy (CODASPY)


Two recent examples of Drexel faculty leadership in the cybersecurity research communities include i) Chris Yang served as general chair of the November 2015 IEEE ICDM Workshop on Intelligence and Security Informatics in Atlantic City, NJ, and ii) Rachel Greenstadt served as general chair of the July 2015 Privacy Enhancing Technologies Symposium (2015), the premier conference of the privacy community.
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 Weber
Director, Drexel Cybersecurity Institute
## Contents

1. Mission Statement .................................................. 5
2. Governance ........................................................... 6
3. Faculty Affiliates ..................................................... 8
4. Research .............................................................. 36
   4.1 Research projects ............................................... 36
   4.2 Research funding ............................................... 41
   4.3 Research articles ............................................... 51
   4.4 Graduate students ............................................... 53
   4.5 Research community engagement ......................... 56
   4.6 Technology commercialization .............................. 56
5. Business Development ............................................. 58
6. Education ............................................................ 60
   6.1 Courses, degrees, certificates ................................ 60
   6.2 NSA/DHS CAE-IAE recertification ......................... 63
   6.3 U.S. Army Reserve Private Public Partnership Initiative (USAR-P3i) ........................................ 64
   6.4 Other educational development activities ............... 68
7. Community Engagement .......................................... 69
   7.1 Invited talks by Drexel faculty ............................... 69
   7.2 Events organized by the Drexel Cybersecurity Institute ........................... 69
   7.3 Newsletter ....................................................... 71
8. In The News .......................................................... 73
9. Contact Us ......................................................... 84
1 Mission Statement

The mission statement of the Drexel Cybersecurity Institute is:

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

The DCI is advised internally by the DCI 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 DCI Director, Steven Weber, reports directly to the Senior Vice Provost for Research, Aleister Saunders, who also sits on the Members Council.

Figure 1: The DCI Members Council.
The DCI is advised externally by the DCI 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 DCI Senior Advisory Board (as of March, 2015).
3 Faculty Affiliates

To date twenty three (23) Drexel faculty from across the university have affiliated with the DCI, 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.

<table>
<thead>
<tr>
<th>Faculty Name</th>
<th>Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pramod Abichandani</td>
<td>keyword 1; keyword 2; keyword 3</td>
</tr>
<tr>
<td>Murugan Anandarajan</td>
<td>data mining and identity theft; text mining; predictive modeling; cyber deviant behavior</td>
</tr>
<tr>
<td>Marcello Balduccini</td>
<td>detection in cyber-physical systems, automated malware detection and mitigation, ontology-driven data semantics discovery for cyber-security</td>
</tr>
<tr>
<td>Kapil Dandekar</td>
<td>wireless security; reactive jamming; wireless penetration testing; visualization</td>
</tr>
<tr>
<td>Rob D’Ovidio</td>
<td>intersection of computer technology, crime, and the criminal justice system</td>
</tr>
<tr>
<td>David Gefen</td>
<td>trust management systems; behavioral effects of fraud; privacy management</td>
</tr>
<tr>
<td>Christopher Giib</td>
<td>computer network security</td>
</tr>
<tr>
<td>Rachel Greenstadt</td>
<td>privacy &amp; security of multi-agent systems; economics of electronic privacy &amp; information security</td>
</tr>
<tr>
<td>Nagarajan Kandasamy</td>
<td>network anomaly detection</td>
</tr>
<tr>
<td>Constantine Katsinis</td>
<td>computer security; network security; information assurance</td>
</tr>
<tr>
<td>Geoffrey Mainland</td>
<td>program analysis; anomaly detection</td>
</tr>
<tr>
<td>Spiros Mancoridis</td>
<td>malware detection, classification, and mitigation; software security; reverse engineering; code analysis</td>
</tr>
<tr>
<td>Gaurav Naik</td>
<td>mobile network security; computer network security</td>
</tr>
<tr>
<td>Omkant Pandey</td>
<td>public-key cryptography; secure computation; program obfuscation; non-malleable cryptography; differential privacy</td>
</tr>
<tr>
<td>Ioannis Savidis</td>
<td>hardware security; Trojan detection and mitigation; gate level logic encryption; side-channel analysis; circuit-level intellectual property protection; design for trust</td>
</tr>
<tr>
<td>Harish Sethu</td>
<td>web security and privacy; network anomaly detection</td>
</tr>
<tr>
<td>James Shackleford</td>
<td>runtime code injection; virtual address space manipulation; transparent library redirection</td>
</tr>
<tr>
<td>Matthew Stamm</td>
<td>information security; multimedia forensics and anti-forensics; information verification</td>
</tr>
<tr>
<td>Baris Taskin</td>
<td>hardware security; hardware/software co-design for exascale system performance</td>
</tr>
<tr>
<td>Kristene Unsworth</td>
<td>surveillance; national security policy</td>
</tr>
<tr>
<td>Steven Weber</td>
<td>network performance; statistical analysis; anomaly detection; security overhead analysis</td>
</tr>
<tr>
<td>Scott White</td>
<td>homeland security; intelligence analysis</td>
</tr>
<tr>
<td>Christopher Yang</td>
<td>security informatics; information sharing and privacy; sentiment analysis</td>
</tr>
</tbody>
</table>

Table 1: The DCI Faculty Affiliates and their cybersecurity keywords.
Figure 3: The DCI Faculty Affiliates.
<table>
<thead>
<tr>
<th>Name</th>
<th>Academic Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pramod Abichandani</td>
<td>Assistant Clinical Professor, Department of Decision Sciences; Director of the</td>
</tr>
<tr>
<td></td>
<td>Business Analytics Program, LeBoW College of Business</td>
</tr>
<tr>
<td>Murugan Anandarajan</td>
<td>Professor and Department Head, Departments of Management, Decision Sciences &amp; MIS, LeBow College of Business</td>
</tr>
<tr>
<td>Marcello Balduccini</td>
<td>Assistant Research Professor, Department of Computer Science, College of Computing and Informatics</td>
</tr>
<tr>
<td>Kapil Dandekar</td>
<td>Professor, Department of Electrical and Computer Engineering; Associate Dean of Research and Graduate Studies, College of Engineering. Director, Drexel Wireless Systems Laboratory (DWSL)</td>
</tr>
<tr>
<td>Rob D’Ovidio</td>
<td>Associate Professor, Department of Criminology and Justice Studies; Associate Dean for Humanities and Social Science Research and Graduate Education, College of Arts and Sciences</td>
</tr>
<tr>
<td>David Gefen</td>
<td>Professor and Provost Distinguished Research Professor, Department of Decision Sciences and MIS, LeBow College of Business</td>
</tr>
<tr>
<td>Christopher Geib</td>
<td>Associate Professor, Department of Computer Science, College of Computing and Informatics</td>
</tr>
<tr>
<td>Rachel Greenstadt</td>
<td>Associate Professor, Department of Computer Science, College of Computing and Informatics. Director, Privacy, Security and Automation Lab (PSAL)</td>
</tr>
<tr>
<td>Nagarajan Kandasamy</td>
<td>Associate Professor and Associate Department Head of Graduate Affairs, Department of Electrical and Computer Engineering, College of Engineering</td>
</tr>
<tr>
<td>Constantine Katsinis</td>
<td>Associate Teaching Professor, Department of Computer Science, College of Computing and Informatics</td>
</tr>
<tr>
<td>Geoffrey Mainland</td>
<td>Assistant Professor, Department of Information Science, College of Computing and Informatics</td>
</tr>
<tr>
<td>Spiros Mancoridis</td>
<td>Isaac L. Auerbach Professor, Department of Computer Science; Interim Dean, College of Computing and Informatics</td>
</tr>
<tr>
<td>Gaurav Naik</td>
<td>Assistant Research Professor, Department of Computer Science, College of Computing and Informatics</td>
</tr>
<tr>
<td>Omkant Pandey</td>
<td>Assistant Professor, Department of Computer Science, College of Computing and Informatics</td>
</tr>
<tr>
<td>Ioannis Savidis</td>
<td>Assistant Professor, Department of Electrical and Computer Engineering, College of Engineering. Director, Integrated Circuits and Electronics (ICE) Design and Analysis Laboratory</td>
</tr>
<tr>
<td>Harish Sethu</td>
<td>Associate Professor, Department of Electrical and Computer Engineering, College of Engineering</td>
</tr>
<tr>
<td>James Shackleford</td>
<td>Assistant Professor, Department of Electrical and Computer Engineering, College of Engineering</td>
</tr>
<tr>
<td>Matthew Stamm</td>
<td>Assistant Professor, Department of Electrical and Computer Engineering, College of Engineering. Director, Multimedia and Information Security Laboratory (MISL)</td>
</tr>
<tr>
<td>Baris Taskin</td>
<td>Associate Professor, Department of Electrical and Computer Engineering, College of Engineering. Director, Drexel VLSI and Architecture Laboratory</td>
</tr>
<tr>
<td>Kristene Unsworth</td>
<td>Assistant Professor, Department of Information Science, College of Computing and Informatics</td>
</tr>
<tr>
<td>Steven Weber</td>
<td>Professor, Department of Electrical and Computer Engineering, College of Engineering; Director, Drexel Cybersecurity Institute. Director, Drexel Modeling and Analysis of Networks Laboratory (MANLab)</td>
</tr>
<tr>
<td>Scott White</td>
<td>Associate Clinical Professor, Department of Information Science, College of Computing and Informatics</td>
</tr>
<tr>
<td>Christopher Yang</td>
<td>Associate Professor, Department of Information Science, College of Computing and Informatics</td>
</tr>
</tbody>
</table>

Table 2: The DCI Faculty Affiliates and their academic titles, affiliations, and positions.
Faculty profile: Pramod Abichandani, Ph.D.

<table>
<thead>
<tr>
<th>Title</th>
<th>Assistant Clinical Professor</th>
</tr>
</thead>
<tbody>
<tr>
<td>College</td>
<td>LeBow College of Business</td>
</tr>
<tr>
<td>Department</td>
<td>Decision Sciences</td>
</tr>
<tr>
<td>Position</td>
<td>Director of the LeBow Business Analytics Program</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:pva23@drexel.edu">pva23@drexel.edu</a></td>
</tr>
<tr>
<td>Phone</td>
<td>(215) 895-0301</td>
</tr>
<tr>
<td>University page</td>
<td><a href="http://www.lebow.drexel.edu/people/pramodabichandani">http://www.lebow.drexel.edu/people/pramodabichandani</a></td>
</tr>
<tr>
<td>Personal page</td>
<td><a href="http://www.pramod.co">http://www.pramod.co</a></td>
</tr>
</tbody>
</table>

**Research/teaching keywords:** keyword 1; keyword 2; keyword 3.

**Cybersecurity expertise:** keyword 1; keyword 2; keyword 3.

**Background:**

**Publications:**

**Research funding:**

**Courses taught:**

**Professional service:**
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:


Research funding:


Faculty profile: Marcello Balduccini, Ph.D.

Title: Assistant Research Professor
College: Computing and Informatics
Department: Computer Science
Email: mbalduccini@drexel.edu
Phone: (215) 571-3603
University page: http://drexel.edu/cci/contact/Faculty/Balduccini-Marcello/
Personal page: http://www.mbal.tk

Research/teaching keywords: knowledge representation; non-monotonic reasoning; declarative programming; planning; scheduling; diagnostics; inductive learning.

Cybersecurity expertise: detection in cyber-physical systems; automated malware detection and mitigation; ontology-driven data semantics discovery for cyber-security.

Background: My fundamental research interests are focused on knowledge representation and reasoning, including ontologies, agent architectures, commonsense, natural language understanding, and constraint satisfaction. Application domains of interest include decision-making/decision-support systems, cyber-security and cyber-physical systems, cognitive robotics, intelligent unmanned vehicles, behavior modeling, and model-based user interfaces. Prior to joining Drexel, I served as principal research scientist at Kodak Research Labs, Eastman Kodak Company for six years. I have authored or co-authored more than 50 refereed technical publications, including three book chapters, and have edited two volumes.

Publications:

Research funding:

Professional service:
1. Member of the NIST Cyber-Physical Systems Public Working Group
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:


Research funding:


Courses taught:

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECES 306</td>
<td>Analog &amp; Digital Communication</td>
</tr>
<tr>
<td>ECET 512</td>
<td>Wireless Systems</td>
</tr>
<tr>
<td>ECEL 404</td>
<td>Software Defined Radio Laboratory</td>
</tr>
<tr>
<td>ECET 890</td>
<td>Software Defined Radio Security Lab</td>
</tr>
</tbody>
</table>
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:

Research funding:


courses taught:

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CJS 274</td>
<td>Sex, Violence, and Crime on the Internet</td>
</tr>
<tr>
<td>CJS 276</td>
<td>Computer Crime</td>
</tr>
<tr>
<td>CJ 377</td>
<td>Intellectual Property Theft in the Digital Age</td>
</tr>
</tbody>
</table>

Professional service:

1. Member, International Association of Chiefs of Police, Computer Crime and Digital Evidence Committee
Faculty profile: David Gefen, Ph.D.

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:


Research funding:


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.

Publications:

Research funding:

Courses taught:

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
<th>Section</th>
<th>Title</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFO</td>
<td>Foundations of Software</td>
<td>108</td>
<td>INFO</td>
<td>336</td>
</tr>
<tr>
<td>CS</td>
<td>Artificial Intelligence</td>
<td>380</td>
<td>CS</td>
<td>510</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Distributed Network Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Introduction to Artificial Intelligence</td>
<td></td>
</tr>
</tbody>
</table>

Professional service:
Faculty profile: Rachel Greenstadt, Ph.D.

<table>
<thead>
<tr>
<th>Title</th>
<th>Associate Professor</th>
</tr>
</thead>
<tbody>
<tr>
<td>College</td>
<td>Computing and Informatics</td>
</tr>
<tr>
<td>Department</td>
<td>Computer Science</td>
</tr>
<tr>
<td>Research Lab</td>
<td>Privacy, Security and Automation Lab (PSAL)</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:greenstadt@gmail.com">greenstadt@gmail.com</a></td>
</tr>
<tr>
<td>Phone</td>
<td>(215) 895-2920</td>
</tr>
<tr>
<td>University page</td>
<td><a href="http://drexel.edu/cci/contact/Faculty/Greenstadt-Rachel/">http://drexel.edu/cci/contact/Faculty/Greenstadt-Rachel/</a></td>
</tr>
<tr>
<td>Personal page</td>
<td><a href="https://www.cs.drexel.edu/~greenie/">https://www.cs.drexel.edu/~greenie/</a></td>
</tr>
<tr>
<td>Lab page</td>
<td><a href="https://psal.cs.drexel.edu/">https://psal.cs.drexel.edu/</a></td>
</tr>
</tbody>
</table>

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:


Research funding:
Courses taught:
CS 613 Machine Learning  
CS 475 Computer and Network Security  
CS 590 Privacy

Professional service:
Faculty profile: Nagarajan Kandasamy, Ph.D.

<table>
<thead>
<tr>
<th>Title</th>
<th>Associate Professor</th>
</tr>
</thead>
<tbody>
<tr>
<td>College</td>
<td>Engineering</td>
</tr>
<tr>
<td>Department</td>
<td>Electrical and Computer Engineering</td>
</tr>
<tr>
<td>Position</td>
<td>Associate Department Head for Graduate Affairs</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:kandasamy@drexel.edu">kandasamy@drexel.edu</a></td>
</tr>
<tr>
<td>Phone</td>
<td>(215) 895-1996</td>
</tr>
</tbody>
</table>

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:


Research funding:


Courses taught:

<table>
<thead>
<tr>
<th>ENGR 121</th>
<th>Computation Lab I</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECEC 413</td>
<td>Introduction to Parallel Computer Architecture</td>
</tr>
<tr>
<td>ECE 200</td>
<td>Digital Logic</td>
</tr>
<tr>
<td>ECEC 520</td>
<td>Dependable Computing</td>
</tr>
<tr>
<td>ECEC 414</td>
<td>High Performance Computing</td>
</tr>
<tr>
<td>ENGR 122</td>
<td>Computation Lab II</td>
</tr>
<tr>
<td>ECEC 622</td>
<td>Parallel Computer Architecture</td>
</tr>
<tr>
<td>ECEC 353</td>
<td>Introduction to Operating Systems</td>
</tr>
<tr>
<td>ECEC 355</td>
<td>Computer Architecture and Organization</td>
</tr>
</tbody>
</table>
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.

Publications:

Research funding:

Courses taught:

Professional service:
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:


Faculty profile: Spiros Mancoridis, Ph.D.

<table>
<thead>
<tr>
<th>Title</th>
<th>Isaac L. Auerbach Professor</th>
</tr>
</thead>
<tbody>
<tr>
<td>College</td>
<td>Computing and Informatics</td>
</tr>
<tr>
<td>Department</td>
<td>Computer Science</td>
</tr>
<tr>
<td>Position</td>
<td>Interim Dean – College of Computing and Informatics</td>
</tr>
<tr>
<td>Research Lab</td>
<td>Software Engineering Research Group (SERG)</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:spiros@drexel.edu">spiros@drexel.edu</a></td>
</tr>
<tr>
<td>Phone</td>
<td>(215) 895-6824</td>
</tr>
<tr>
<td>University page</td>
<td><a href="http://drexel.edu/cci/contact/Faculty/Mancoridis-Spiros/">http://drexel.edu/cci/contact/Faculty/Mancoridis-Spiros/</a></td>
</tr>
<tr>
<td>Personal page</td>
<td><a href="https://www.cs.drexel.edu/~spiros/">https://www.cs.drexel.edu/~spiros/</a></td>
</tr>
</tbody>
</table>

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:


Research funding:


Faculty profile: Gaurav Naik

<table>
<thead>
<tr>
<th>Title</th>
<th>Assistant Research Professor</th>
</tr>
</thead>
<tbody>
<tr>
<td>College</td>
<td>Computing and Informatics</td>
</tr>
<tr>
<td>Department</td>
<td>Computer Science</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:gn@drexel.edu">gn@drexel.edu</a></td>
</tr>
<tr>
<td>Phone</td>
<td>(215) 571-4512</td>
</tr>
<tr>
<td>University page</td>
<td><a href="http://drexel.edu/cci/contact/Faculty/Naik-Gaurav/">http://drexel.edu/cci/contact/Faculty/Naik-Gaurav/</a></td>
</tr>
</tbody>
</table>

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:


Research funding:


Courses taught:
CS 675  Reverse Engineering
Faculty profile: Omkant Pandey, Ph.D.

<table>
<thead>
<tr>
<th>Title</th>
<th>Assistant Professor</th>
</tr>
</thead>
<tbody>
<tr>
<td>College</td>
<td>Computing and Informatics</td>
</tr>
<tr>
<td>Department</td>
<td>Computer Science</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:omkant@drexel.edu">omkant@drexel.edu</a></td>
</tr>
<tr>
<td>Phone</td>
<td>(215) 571-4599</td>
</tr>
<tr>
<td>University page</td>
<td><a href="http://drexel.edu/cci/contact/Faculty/Pandey-Omkant/">http://drexel.edu/cci/contact/Faculty/Pandey-Omkant/</a></td>
</tr>
</tbody>
</table>

Research/teaching keywords: cryptography; cybersecurity; privacy; theoretical computer science.

Cybersecurity expertise: public-key cryptography; secure computation; program obfuscation; non-malleable cryptography; differential privacy.

Background: My research interests are in cryptography, cybersecurity, and more broadly theoretical computer science. My recent work in cryptography deals with program obfuscation, non-malleable cryptography, and next-generation encryption systems such as functional encryption. I am interested in both applied as well as theoretical aspects of cryptography.

Publications:


Courses taught:

CS T680 Topics in Cryptography

Professional service:


2. *Program Committee Member*, Public Key Cryptography (PKC), 2016.
Faculty profile: Ioannis Savidis, Ph.D.

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:


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/](http://drexel.edu/ece/contact/faculty-directory/SethuHarish/)  
Personal page | [http://www.ece.drexel.edu/sethu/](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:


Research funding:


Courses taught:

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
<th>Course Code</th>
<th>Course Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>EEC 690</td>
<td>Web Security I</td>
<td>EEC 690</td>
<td>Web Security II</td>
</tr>
<tr>
<td>EEC 631</td>
<td>Principles of Computer Networking</td>
<td>EEC 632</td>
<td>Performance Analysis of Computer Networks</td>
</tr>
<tr>
<td>EEC 633</td>
<td>Advanced Topics in Computer Networks</td>
<td>EEC 203</td>
<td>Programming for Engineers</td>
</tr>
<tr>
<td>EEC 301</td>
<td>Advanced Programming for Engineers</td>
<td>EEC 433</td>
<td>Network Programming</td>
</tr>
</tbody>
</table>
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:


Courses taught:

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECE</td>
<td>200 Digital Logic Design</td>
<td></td>
</tr>
<tr>
<td>ECEC</td>
<td>353 Systems Programming</td>
<td></td>
</tr>
<tr>
<td>ECEC</td>
<td>631 Principles of Computer Networking</td>
<td></td>
</tr>
<tr>
<td>ECE</td>
<td>301 Advanced Programming for Engineers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>632 Performance Analysis of Computer Networks</td>
<td></td>
</tr>
</tbody>
</table>
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:


Research funding:


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

Professional service:

Faculty profile: Baris Taskin, Ph.D.

Title: Associate 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:


Research funding:


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.

<table>
<thead>
<tr>
<th>Title</th>
<th>Assistant Professor</th>
</tr>
</thead>
<tbody>
<tr>
<td>College</td>
<td>Computing and Informatics</td>
</tr>
<tr>
<td>Department</td>
<td>Information Science</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:unsworth@drexel.edu">unsworth@drexel.edu</a></td>
</tr>
<tr>
<td>Phone</td>
<td>(215) 895-6016</td>
</tr>
<tr>
<td>University page</td>
<td><a href="http://drexel.edu/cci/contact/Faculty/Unsworth-Kristene/">http://drexel.edu/cci/contact/Faculty/Unsworth-Kristene/</a></td>
</tr>
<tr>
<td>Personal page</td>
<td><a href="http://cci.drexel.edu/faculty/kunsworth/">http://cci.drexel.edu/faculty/kunsworth/</a></td>
</tr>
</tbody>
</table>

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.

Publications:

Research funding:

Courses taught:

Professional service:
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:


Research funding:


Courses taught:

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
<th>Department</th>
<th>Credits</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECE 361</td>
<td>Probability for engineers</td>
<td>ECE</td>
<td>523</td>
<td>Detection and estimation theory</td>
</tr>
<tr>
<td>ECES 302</td>
<td>Transform methods and filtering</td>
<td>EC</td>
<td>631</td>
<td>Principles of computer networking</td>
</tr>
<tr>
<td>ECES 521</td>
<td>Probability and random variables</td>
<td>ECEC</td>
<td>632</td>
<td>Performance analysis of comp. networks</td>
</tr>
<tr>
<td>ECES 522</td>
<td>Random proc. &amp; spectral analysis</td>
<td>ECEC</td>
<td>633</td>
<td>Advanced topics in comp. networking</td>
</tr>
</tbody>
</table>
Faculty profile: Scott White, Ph.D.

<table>
<thead>
<tr>
<th>Title</th>
<th>Associate Clinical Professor</th>
</tr>
</thead>
<tbody>
<tr>
<td>College</td>
<td>Computing and Informatics</td>
</tr>
<tr>
<td>Department</td>
<td>Information Science</td>
</tr>
<tr>
<td>Position</td>
<td>Director of Computing and Security Technology Program</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:sjw@drexel.edu">sjw@drexel.edu</a></td>
</tr>
<tr>
<td>Phone</td>
<td>(215) 895-0910</td>
</tr>
<tr>
<td>University page</td>
<td><a href="http://drexel.edu/cci/contact/Faculty/White-Scott/">http://drexel.edu/cci/contact/Faculty/White-Scott/</a></td>
</tr>
</tbody>
</table>

Research/teaching keywords: emergency management; terrorism & counter-terrorism; infrastructure protection.

Cybersecurity expertise: homeland security; intelligence analysis.

Background: My areas of expertise include homeland security & emergency management, terrorism & counter-terrorism, infrastructure protection, and intelligence analysis. My research interests include homeland security, terrorism and intelligence analysis, and counter-terrorism & infrastructure protection. I previously served as Associate Clinical Professor, Emergency Management and Homeland Security at Drexel’s Goodwin College of Professional Studies. My professional experience includes serving as Founder and Director of the Institute of Homeland Security at Westfield State University; as Associate Consultant, Security and Intelligence at MONAD Security Audit Systems, Inc.; as a Commissioned officer in the Canadian Armed Forces, Military Intelligence Branch (G2); and in the Canadian Security Intelligence Service (CSIS), Office of the Solicitor General, Canada. My academic program associations include the BS in Emergency Management; MS in National Security Management; MS in Professional Studies, Concentration, Homeland Security Management; Minor in Emergency Management; Undergraduate Certificate in Emergency Management; Graduate Certificate in Homeland Security Management; and Graduate Certificate in Cybersecurity, Law & Policy.

Publications:

Research funding:

Courses taught:

Professional service:
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:


Research funding:


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

<table>
<thead>
<tr>
<th>Investigators</th>
<th>Lex Fridman</th>
<th>Post-doc</th>
<th>Steven Weber</th>
<th>Professor</th>
<th>Rachel Greenstadt</th>
<th>Associate Professor</th>
<th>Moshe Kam</th>
<th>Professor</th>
</tr>
</thead>
</table>

**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.](image)

Publications related to this research project include:


This research is partially supported by the following grants:

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

<table>
<thead>
<tr>
<th>Investigators</th>
<th>Bander Alsulamy</th>
<th>Ph.D. student</th>
<th>Raymond Canzanese</th>
<th>Ph.D.</th>
<th>Marcello Balduccini</th>
<th>Assistant Research Professor</th>
<th>Spiros Mancoridis</th>
<th>Isaac L. Auerbach Professor</th>
<th>Moshe Kam</th>
<th>Professor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CS Dept.</td>
<td>Drexel University</td>
<td>CS Dept.</td>
<td>Drexel University</td>
<td>CS Dept.</td>
<td>Drexel University</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Sift Security</td>
<td></td>
<td></td>
<td></td>
<td>Dept. of ECE</td>
<td>NJIT</td>
</tr>
</tbody>
</table>

**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:


This research is partially supported by the following grants:

Research project profile: **network anomaly detection**

<table>
<thead>
<tr>
<th>Investigators</th>
<th>Tingshan Huang</th>
<th>Ph.D.</th>
<th>Ni An</th>
<th>Ph.D. student</th>
<th>Dept. of ECE</th>
<th>Akamai</th>
<th>Drexel University</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Harish Sethu</td>
<td>Associate Professor</td>
<td>Naga Kandasamy</td>
<td>Associate Professor</td>
<td>Dept. of ECE</td>
<td>Drexel University</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Matthew C. Stamm</td>
<td>Assistant Professor</td>
<td>Steven Weber</td>
<td>Professor</td>
<td>Dept. of ECE</td>
<td>Drexel University</td>
<td></td>
</tr>
</tbody>
</table>

**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:


This research is partially supported by the following grants:


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

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:


This research is partially supported by the following grants:


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).

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

<table>
<thead>
<tr>
<th>Agency</th>
<th>Amount (in thousands of dollars)</th>
<th>Year(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Science Foundation Secure and Trustworthy Computing (SaTC)</td>
<td>2012–2016</td>
<td></td>
</tr>
<tr>
<td>National Science Foundation Division of Advanced Cyber Infrastructure (ACI)</td>
<td>2014–2017</td>
<td></td>
</tr>
<tr>
<td>National Science Foundation Cybertechnological Scholarships for Service (SFS)</td>
<td>2012–2015</td>
<td></td>
</tr>
<tr>
<td>National Science Foundation Faculty Early Career Development Program (CAREER)</td>
<td>2013–2018, 2016–2020</td>
<td></td>
</tr>
<tr>
<td>Defense Forensics and Biometrics Agency (DFBA) and Army Research Office (ARO)</td>
<td>2015–2016</td>
<td></td>
</tr>
<tr>
<td>Defense Advanced Research Projects DARPA</td>
<td>Active Authentication Program</td>
<td>2012–2013</td>
</tr>
<tr>
<td>Office of Naval Research (ONR)</td>
<td></td>
<td>2015–2018</td>
</tr>
<tr>
<td>Air Force Research Labs (AFRL)</td>
<td></td>
<td>2011–2014</td>
</tr>
<tr>
<td>National Security Agency (NSA)</td>
<td></td>
<td>2013–2015</td>
</tr>
<tr>
<td>Department of Justice (DoJ)</td>
<td>Office of Justice Programs, Bureau of Justice Assistance</td>
<td>2012–2013</td>
</tr>
<tr>
<td>Department of Justice (DoJ) / National Institute of Justice (NIJ)</td>
<td></td>
<td>2009–2011</td>
</tr>
</tbody>
</table>

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 $10.3M in cybersecurity research over past nine years, from 7+ agencies, 4+ companies, for 25+ projects, supporting 15+ faculty.

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NSF</td>
<td>200</td>
<td>360</td>
<td></td>
<td>1081,888</td>
<td>418,189</td>
<td>150</td>
<td>587</td>
<td></td>
<td></td>
<td>3,873</td>
</tr>
<tr>
<td>DoJ/NIJ</td>
<td>223</td>
<td>489,500</td>
<td></td>
<td>500,987</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2,699</td>
</tr>
<tr>
<td>DARPA</td>
<td>100</td>
<td>393</td>
<td>699</td>
<td>230</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1,422</td>
</tr>
<tr>
<td>ONR</td>
<td></td>
<td></td>
<td></td>
<td>750</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>750</td>
</tr>
<tr>
<td>DFBA/ARO</td>
<td></td>
<td></td>
<td></td>
<td>375</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>375</td>
</tr>
<tr>
<td>AFRL</td>
<td></td>
<td></td>
<td></td>
<td>293</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>293</td>
</tr>
<tr>
<td>NSA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>540</td>
<td>540</td>
</tr>
<tr>
<td>Comcast</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>200,88</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>288</td>
</tr>
<tr>
<td>CSRA</td>
<td></td>
<td></td>
<td></td>
<td>60</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>60</td>
</tr>
<tr>
<td>CAS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>Total</td>
<td>223</td>
<td>1,189</td>
<td>460</td>
<td>1,226</td>
<td>4,155</td>
<td>897</td>
<td>150</td>
<td>1,413</td>
<td>617</td>
<td>10,330</td>
</tr>
</tbody>
</table>

41
The following is a list of cybersecurity research grants active over the past five years, listed in reverse chronological order:


42


The following pages give overviews of several ongoing funded cybersecurity research projects.
Funded research project profile: NSF CAREER (M. Stamm)

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

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

<table>
<thead>
<tr>
<th>Project title</th>
<th>CAREER: Privacy Analytics for End-Users in a Big Data World</th>
</tr>
</thead>
<tbody>
<tr>
<td>Funding agency</td>
<td>National Science Foundation</td>
</tr>
<tr>
<td>Program</td>
<td>Faculty Early Career Development Program (CAREER)</td>
</tr>
<tr>
<td>Investigator</td>
<td>Rachel Greenstadt (PI)</td>
</tr>
<tr>
<td>Dates</td>
<td>February, 2013 – January, 2018</td>
</tr>
<tr>
<td>Award #</td>
<td>CNS-1253418</td>
</tr>
</tbody>
</table>

**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)**

<table>
<thead>
<tr>
<th>Project title</th>
<th>TTP: Medium: Securing the Wireless Philadelphia Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Funding agency</td>
<td>National Science Foundation</td>
</tr>
<tr>
<td>Program</td>
<td>Secure and Trustworthy Computing Program (NSF-SaTC)</td>
</tr>
<tr>
<td>Investigators</td>
<td>Steven Weber (PI)</td>
</tr>
<tr>
<td></td>
<td>Spiros Mancoridis</td>
</tr>
<tr>
<td></td>
<td>Harish Sethu</td>
</tr>
<tr>
<td></td>
<td>Kapil R. Dandekar</td>
</tr>
<tr>
<td>Dates</td>
<td>September, 2012 – August, 2016</td>
</tr>
<tr>
<td>Award #</td>
<td>CNS-1228847</td>
</tr>
</tbody>
</table>

**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

**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)**

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

**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

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  

---

**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

- 2016 IEEE Systems Journal
- 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 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)


The following is a list of cybersecurity research articles published in 2014–2015, listed in reverse chronological order:


52


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


Figure 6: Drexel Ph.D. graduates with cybersecurity-related theses.
4.5 Research community engagement

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


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:


5 Business Development

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

1. Huawei North America Network Division (December, 2015 – present)
2. Bowhead IT Group (November, 2015 – present)
4. FAA ASSURE Center of Excellence in Unmanned Aerial Systems Research (October, 2015 – present)
5. Pro2Serve (September, 2015 – present)
9. U.S. Army CERDEC and ARDEC (persistent relationship)
10. The Judge Group (July, 2015 – present)
11. Areva Nuclear (June, 2015)
12. Exelon/PECO (June, 2015 – present)
13. Turkish Air Force Academy (April, 2015)
16. DSA, Inc. (March, 2015)
17. Northrup Grummman (March, 2015 – present)
18. Comcast (March, 2015 – present)
20. Fitlinxx Inc. (March, 2015)
23. National Security Agency (persistent relationship)
24. Gnostech (February, 2015)
25. L3 Communications (January, 2015 – present)
26. Office of the Mayor of Seoul City, Korea (December, 2014)
27. Unisys Stealth Platform Team (December, 2014 – May, 2015)
29. Federal Bureau of Investigation (FBI) (December, 2014 – present)
30. Vanguard (October, 2014 – present)
32. Momentum Aviation Group (MAG-DS) (October, 2014)
33. Probaris (October, 2014 – present)
34. F-Secure (Helsinki, Finland) (September – October, 2014)
35. Digile (Helsinki, Finland) (September, 2014 – May, 2015)
37. U.S. Bank (August, 2014)
38. Melamedia (August, 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-IAE recertification (§6.2)
4. other educational development activities (§6.4)

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. Masters of Science in National Security Management (MSNSM)
3. Bachelor of Science in Computing and Security Technology (CST)
4. Bachelor of Science in Computer Science – Computer Security Concentration.
5. Certificate in Computing and Security Technology
6. Professional Development Certificates in National Security Management, including:
   (a) Cybersecurity, Law & Policy (online)
   (b) Continuity Management (online)
   (c) Homeland Security (online)
7. Undergraduate Minor in Computer Crime

We briefly comment on the CYBR and MSNSM 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)).

Master of Science in National Security Management (MSNSM):

- Offered through the College of Computing and Informatics (CCI).
• From the program page, “The CCI MSNSM involves an understanding of national and homeland security, policy, law, social, and technological environments. As such, modern national security management is an interdisciplinary field built upon the expertise of a wide variety of disciplines. The online MSNSM uses a multidisciplinary approach to targeting advanced topics in security management, emergency management, information technology, risk management, law and policy”.

• Launched as an online program in Fall 2014.

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
  Digital certificates and authentication
  A security-conscious intro. to HTML & CSS
  A security-conscious intro. to JavaScript
  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

• Privacy (R. Greenstadt). Learning outcomes are on the left, and the list of topics are on the right:

  Motivation for privacy protection.
  Anonymity, unlinkability, unobservability.
  Formalization, modeling, & measurement.
  State-of-the-art in privacy technologies.

  Measuring privacy using information theory
  Data privacy threats and protection measures
  Privacy and web mining
  Privacy at the communications layer
  Privacy and usability
  Social media & implications for elec. privacy

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

• AY 2015-2016
<table>
<thead>
<tr>
<th>Term</th>
<th>Course</th>
<th>Title</th>
<th>Instructor</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Win 2016</td>
<td>ECES T680</td>
<td>ST: Media Forensics and Security</td>
<td>M. Stamm</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>CS 303</td>
<td>Algorithmic Number Theory and Cryptography</td>
<td>J. Johnson</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>INFO 333</td>
<td>Introduction to Information Security</td>
<td>C. McCain</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>INFO 712</td>
<td>Information Assurance</td>
<td>P. Grillo</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>CST 614</td>
<td>Counterintelligence</td>
<td>S. White</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>HSM 549</td>
<td>Terrorism and Homeland Security</td>
<td>S. White</td>
<td>7</td>
</tr>
<tr>
<td>Fall 2015</td>
<td>ECEC 457</td>
<td>Security in Computing</td>
<td>L. Trachtenberg</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>INFO 375</td>
<td>Introduction to Information Systems Assurance</td>
<td>C. Mascaro</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>INFO 517</td>
<td>Principles of Cybersecurity</td>
<td>S. White</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>CST 609</td>
<td>National Security Intelligence</td>
<td>S. White</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>HSM 544</td>
<td>Introduction to Homeland Security</td>
<td>S. White</td>
<td>13</td>
</tr>
</tbody>
</table>

• AY 2014-2015

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

• AY 2013-2014
<table>
<thead>
<tr>
<th>Term</th>
<th>Course</th>
<th>Title</th>
<th>Instructor</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spr 2014</td>
<td>ECET 890</td>
<td>ST: SDR Security Laboratory</td>
<td>K. Dandekar</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>CS 303</td>
<td>Algebraic Number Theory and Cryptography</td>
<td>B. Char</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>CS 675</td>
<td>Reverse Software Engineering</td>
<td>G. Naik</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>INFO 333</td>
<td>Introduction to Information Security</td>
<td>C. Carroll</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>INFO 336</td>
<td>Distributed Systems Security</td>
<td>C. Geib</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>INFO 517</td>
<td>Principles of Cybersecurity</td>
<td>S. White</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>INFO 710</td>
<td>Information Forensics</td>
<td>C. McClain</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>INFO 718</td>
<td>Cybersecurity Policy</td>
<td>H. Rishikof</td>
<td>7</td>
</tr>
<tr>
<td>Win 2014</td>
<td>ECEC 690</td>
<td>ST: Web Security II</td>
<td>H. Sethu</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>CS 475</td>
<td>Computer and Network Security</td>
<td>R. Greenstadt</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>INFO 712</td>
<td>Information Assurance</td>
<td>P. Grillo</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>INFO 717</td>
<td>Cyber Crime Law</td>
<td>H. Rishikof</td>
<td>11</td>
</tr>
<tr>
<td>Fall 2013</td>
<td>ECEC 690</td>
<td>ST: Web Security I</td>
<td>H. Sethu</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>CS 680</td>
<td>ST: Privacy in Electronic Society</td>
<td>R. Greenstadt</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>INFO 333</td>
<td>Introduction to Information Security</td>
<td>C. Carroll</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td>CJ 276</td>
<td>Introduction to Computer Crime</td>
<td>I. Schlanger</td>
<td>23</td>
</tr>
</tbody>
</table>

### 6.2 NSA/DHS CAE-IAE recertification

- Drexel has held the designation as a National Security Agency (NSA) / Department of Homeland Security (DHS) Center of Academic Excellence (CAE) in Information Assurance Education (IAE) for over ten years.
- The CAE designation is a credential conferred by the NSA and DHS upon those 2-year and 4-year academic institutions with cybersecurity-related education programs in line with recommended best practices and having the required depth and breadth for its graduates to contribute to the national cybersecurity workforce.
- The DCI has been coordinating the recertification effort since May, 2014. Participants include Steven Weber, Kapil Dandekar, Sherry Levin, Chad Morris, Doug Pfeil, Alex Olivares, Constantine Katsinis, and Rich Primerano.
- Recertification requires 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

Each KU has an associated set of topics to be matched with topics covered in courses.
- This designation was critical for Drexel to be named as one of the six universities selected to participate in the USAR P3i program, discussed below.
6.3 U.S. Army Reserve Private Public Partnership Initiative (USAR-P3i)

Following the meeting of the Delaware Valley Chapter of the National Defense Infrastructure Association (NDIA) at Drexel on September 9, 2014, Drexel began discussion with LtC. Scott Nelson about the U.S. Army Reserve Private Public Partnership Office initiative (P3i) on cybersecurity education.

The USAR P3i program brings together three key stakeholders for the USAR citizen soldiers: the USAR itself, cybersecurity-related employers, and universities offering cybersecurity-related degree programs. Drexel was identified as one of six initial universities to participate in this program, along with Norwich University, the University of Washington, George Mason University, the University of Texas at San Antonio, and the University of Colorado – Colorado Springs.

As described in the events below, representatives of the six universities attended a ceremony hosted by Lt. Gen. Jeffrey Talley, head of the USAR, in the Raeburn U.S. House of Representatives building in Washington, D.C., on February 10, 2015, wherein a Memorandum of Understanding (MoU) was signed.

A subsequent logistic and planning meeting was held at the University of Colorado – Colorado Springs campus in April, 2015, attended by Drexel representatives Norm Balchunas and Steven Weber. Although the federal funding for this project has been delayed for this fiscal year, Drexel stands ready and willing to work with the USAR on this important program.

Figure 7: Attendees at the Drexel Cybersecurity Education Summit at Drexel’s Washington, D.C. facility, before USAR P3i signing ceremony.
Figure 8: LtG. Talley (head of the USAR) and representatives from the six USAR P3i-Cyber universities and industry partners at the MoU signing ceremony in the U.S. House of Representatives Raeburn Building, February 10, 2015.
Figure 9: LtG. Talley signing the MoU.
30 February 2015

The United States Army Reserve (USAR) works tirelessly to increase the overall readiness of Soldiers in order to support crucial national initiatives in times of peace and war. The Army Reserve created the Private Public Partnership (P3) Office to facilitate strategic and mutually beneficial relationships with employers, universities, and organizations to ensure comprehensive support for Soldier readiness.

Members of the P3 Cyber Initiative are uniquely suited to provide critical training and employment opportunities to members of the USAR. Jointly, the USAR, and its Employer Partner enter into this statement of support to facilitate a strategic and mutually beneficial relationship and encourage the exploration of cyber initiatives providing America’s Warrior-Citizens and Veterans with employment and training opportunities.

The undersigned are representatives of each Phase I entity, university and employer partner, that support the USAR and P3 in the mission to educate and employ cyber Soldiers.

Figure 10: The signed MoU.
6.4 Other educational development activities

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

- 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)
Community Engagement

Invited talks given by Drexel faculty are listed in §7.1. Events, symposia, invited speakers, and panels organized or co-organized by the Drexel Cybersecurity Institute are listed in §7.2. The DCI newsletters are listed in §7.3.

7.1 Invited talks by Drexel faculty

Drexel faculty have given the following invited presentations:


7.2 Events organized by the Drexel Cybersecurity Institute

The seventeen (17) events, guest lectures, symposia organized or co-organized by DCI to date are listed below. **Bold** items denote major symposia (half-day events). Credit to Norm Balchunas for coordination and leadership.


[11] Norm Balchunas (coordinator) and Rachel Greenstadt (moderator). Panelists Roger Dinglyline (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.

[12] 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 Economides (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.


### 7.3 Newsletter

The DCI has produced a “near-monthly” newsletter, which is distributed to the DCI “community”. The newsletters have been developed by Norm Balchunas, Dionne Queen, Brenda Sheridan, and Kerry Boland.

<table>
<thead>
<tr>
<th>December, 2014</th>
<th>December, 2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>November, 2014</td>
<td>November, 2015</td>
</tr>
<tr>
<td>October, 2014</td>
<td>October, 2015</td>
</tr>
<tr>
<td></td>
<td>September, 2015</td>
</tr>
<tr>
<td>August, 2014</td>
<td></td>
</tr>
<tr>
<td>July, 2014</td>
<td></td>
</tr>
<tr>
<td>June, 2014</td>
<td>June, 2015</td>
</tr>
<tr>
<td>May, 2014</td>
<td>May, 2015</td>
</tr>
<tr>
<td>March, 2014</td>
<td>March, 2015</td>
</tr>
<tr>
<td>February, 2014</td>
<td>February, 2015</td>
</tr>
<tr>
<td></td>
<td>January, 2015</td>
</tr>
</tbody>
</table>

A snapshot of a portion of the December, 2015 newsletter is shown in Fig. 12.
Figure 12: Snapshot of the December, 2015 newsletter.
8 In The News

Three Drexel faculty regularly interviewed by the media are i) Scott White (CCI), ii) Rob D'Ovidio (CoAS), and iii) Rachel Greenstadt (CCI).

![Scott White](image1.jpg)
Teaching Professor, CCI
National security, cybersecurity

![Rob D'Ovidio](image2.jpg)
Associate Professor, CoAS
Digital forensics and cyber crime

![Rachel Greenstadt](image3.jpg)
Associate Professor, CCI
Privacy and security

Figure 13: Three Drexel faculty regularly interviewed by the media.

Drexel cybersecurity-related activities mentioned in the news include:


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

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

By Juliana Reyes / REPORTER

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

(Photography by Juliana Reyes)
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.

"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.
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.

Figure 18: Technically Philly – February 11, 2015.
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

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.
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.
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 Barrowcliff) 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.
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.

9 Contact Us

Steven Weber, Ph.D.
Director

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