Curriculum Vitae of Irfan Ahmed

2000 Lakeshore Dr.
New Orleans LA 70148

Tel No.: (+1) 504 - 280 - 4409
Email: irfan@cs.uno.edu

PERSONAL

I am a Permanent Resident (Green Card Holder) of the USA.

RESEARCH INTERESTS

Digital Forensics
Industrial Control System (ICS) Security
Malware Detection and Analysis
Security via Virtualization
Cybersecurity Education

CURRENT PROFESSIONAL AFFILIATIONS

Canizaro-Livingston Endowed Assistant Professor in Cybersecurity — August 2017 - To-date
Tenure-track Assistant Professor — August 2013 - To-date
Department of Computer Science — `www.cs.uno.edu`
University of New Orleans (UNO)

Director, Cyber-Physical Systems (CyPhy) Lab — January 2016 - To-date
Department of Computer Science — `cyphy.cs.uno.edu`
University of New Orleans

Associate Director — January 2017 - To-date
Research Affiliation — January 2012 - To-date
Greater New Orleans Center for Information Assurance (GNOCIA) — `gnocia.cs.uno.edu`
University of New Orleans

Member — January 2017 - To-date
ACM Special Interest Group on Computer Science Education (SIGCSE) — `sigcse.org/sigcse`

Associate Member — April 2015 - To-date
American Academy of Forensic Sciences (AAFS) — `www.aafs.org`

PROFESSIONAL PREPARATION

Postdoctoral Research Associate (Postdoc) — Jan 2012-Aug 2013
University of New Orleans, New Orleans, LA, United States
`http://www.uno.edu`
Project: Virtual Machine Introspection-based Live Forensics for Detection of Malicious Software
Funded by: National Science Foundation (Award No.: 1016807)

Postdoctoral Research Associate (Postdoc) — Sept 2010-Sept 2011
Queensland University of Technology, Brisbane, Australia
`http://www.qut.edu.au`

Project: Forensic Readiness in Control Systems: Tools and Methods
Funded by: Department of Prime Minister and Cabinet's Research Support for National Security

Doctor of Philosophy (PhD), Computer Science — June 2010
Ajou University, Suwon, South Korea
`http://www.ajou.ac.kr`

Master of Science (M.S.), Computer Science — April 2005
SZABIST, Karachi, Pakistan
`http://szabist.edu.pk`

Bachelor of Engineering (B.E.), Computer System — Feb 2003
NED University of Engineering and Technology, Karachi, Pakistan
`http://www.neduet.edu.pk`

Oracle Certified Professional (OCP), Database Administration — May 2001
`http://www.oracle.com/education/professional.html`

HONORS AND AWARDS

Canizaro-Livingston Endowed Professorship in Cybersecurity — August 2017
University of New Orleans, New Orleans, LA

Early Career Research Prize — December 2016
University of New Orleans, New Orleans, LA

Outstanding Poster Award — March 2016
6^{th} ACM Conference on Data and Application Security and Privacy (CODASPY'16), New Orleans, LA

Outstanding Research Award — February 2014
66^{th} Annual Meeting of the American Academy of Forensic Sciences, Washington, USA

Best Paper Award — November 2013
16^{th} Information Security Conference (ISC'13), Dallas, Texas, USA

Best Paper Award — August 2011
International Cyber Resilience Conference, Perth, Australia

Korean Government Scholarship — Sept 2006 - Aug 2010
Institute of Information Technology Advancement (IITA), South Korea

Ajou University Full Tuition Scholarship — Sept 2006 - Aug 2008
Ajou University, South Korea

Silver Medalist — 1993
23^{rd} International Art Exhibition, Tokyo, Japan

GRANTS/CONTRACTS

(UNO Share: $2,304,943, Total Funding: $2,510,856)

Funded Grants:

NSF	DoD	ONR	LA-BoR	UNO	Miscellaneous
4	7	1	3	3	3

- National Science Foundation (NSF)
- Department of Defense (DoD)
- Office of Naval Research (ONR)
- Louisiana State Board of Regents (LA-BoR)
- University of New Orleans (UNO)

*Principal Investigator (PI)
*Co-Principal Investigator (Co-PI)

Research (R)

R-1: **[UNO].** "Gap Analysis of Digital Forensics on SCADA Testbed", UNO Office of Research and Sponsored Programs (ORSP) - SCoRe (Stimulating Competitive Research), University of New Orleans, Role: Sole PI, Funding: $12,000, Project Duration: 1 year (July 2016 - June 2017)

R-2: **[ONR].** "Digital Forensic Toolkit for Machine Control Systems (TRACE)", Office of Naval Research - STTR Phase 1, Role: PI (with Intelligent Automation Inc.), Funding: $80,000 (UNO Share: $24,000), Project Duration: 7 Months (2016-2017)

R-3: **[UNO].** "Fuzzing Infrastructure for the Cloud", UNO ORSP Internal Grant Program funded by the Louisiana Working and Innovation for a Stronger Economy (WISE) initiative, Role: Sole PI, Funding: $20,000, Project Duration: 8 Months (2015 - 2016)

R-4: **[DoD].** "Automatic Run-time Mitigation of Kernel Exploits in Cloud Environments", Department of Defense (DoD), Role: PI (Co-PIs: Vassil Roussev and Golden G. Richard III), Funding: $75,000 (UNO Share: $75,000), Project Duration: 1 year (2015 - 2016)

R-5: **[BoR RCS].** "Towards Effective Vulnerability Analysis of Application Code in a Cloud-computing Environment", LA Board of Regents (BoR) - Research Competitiveness Subprogram (RCS), Role: Sole PI, Funding: $146,700, Project Duration: 3 years (2015 - 2018) Award No.: LEQSF(2015-18)-RD-A-34 *(awarded, but due to LA state budget cut, not funded)*

R-6: **[NSF].** "CNS-SaTC: EAGER: Integrating Cognitive and Computer Science to Improve Cyber Security: Selective Attention and Personality Traits for the Detection and Prevention of Risk", National Science Foundation (NSF) - Secure & Trustworthy Cyberspace (SaTC), Role: PI since January 2017 and Co-PI from 2014 to 2016 (with Carl Weems from Iowa State University and Golden G. Richard III from UNO), Funding: $223,022, Project Duration: 4 years (2014 - 2018) *Award No.: 1358723*

R-7: **[UNO].** "Botnet Detection in Cloud-computing Environments", UNO Office of Research and Sponsored Programs (ORSP) - SCoRe (Stimulating Competitive Research), University of New Orleans, Role: Sole PI, Funding: $12,000, Project Duration: 3 months (May 2014 - Aug 2014)

Education (E)

E-8: **[DoD].** "Automated Platform for Comprehensive Hands-on Cybersecurity Training", Department of Defense, Role: Co-PI (with Vassil Roussev), Funding: $274,370, Project Duration: 1 year (2017 - 2018)

E-9: **[DoD].** "Portable Hands-on Training Environment for SCADA Security", Department of Defense, Role: PI (Co-PI: Vassil Roussev), Funding: $280,310, Project Duration: 1 year (2017 - 2018)

E-10: **[DoD].** "Instructional Material for SCADA Security Course", Department of Defense, Role: PI (Co-PI: Vassil Roussev from UNO and Sajal Bhatia from Fordham University), Funding: $187,964, Project Duration: 1 year (2017 - 2018)

E-11: **[DoD].** "Concept Maps for Cybersecurity Education", Department of Defense, Role: PI (Co-PI: Vassil Roussev), Funding: $163,803, Project Duration: 1 year (2017 - 2018)

E-12: **[DoD].** "GenCyber@UNO: An Intensive Cybersecurity Bootcamp for Secondary School Teachers", Department of Defense (DoD), Role: Co-PI (with Vassil Roussev), Funding: $116,418, Project Duration: 1 year (2017 - 2018)

E-13: **[NSF].** "EDU: Collaborative: Using Virtual Machine Introspection for Deep Cyber Security Education", National Science Foundation (NSF) - Secure & Trustworthy Cyberspace (SaTC), Role: PI (with Zhiqiang Lin from University of Texas at Dallas), Funding: $299,913 (UNO Share: $150,000), Project Duration: 2 years (2016 - 2018) *Award No.: 1623276*

E-14: **[NSF].** "SaTC-EDU: EAGER: Peer Instruction for Cybersecurity Education", National Science Foundation (NSF) - Secure & Trustworthy Cyberspace (SaTC), Role: PI (Co-PIs: Cynthia B. Lee from Stanford University and Golden G. Richard III and Vassil Roussev from UNO), Funding: $300,000, Project Duration: 3 years (2015 - 2018)) *Award No.: 1500101*

E-15: **[NSF].** "EDU: Lightweight Environment for Network Security Education (LENSE)", National Science Foundation (NSF) - Secure & Trustworthy Cyberspace (SaTC), Role: Co-PI (with Vassil Roussev and Golden G. Richard III), Funding: $299,846, Project Duration: 3 years (2014 - 2017) *Award No.: 1419358*

Equipment (Q)

Q-16: **[DoD].** "SCADA Testbed for Security and Forensics Research", Department of Defense (DoD) Army Research Office (ARO)- Defense University Research Instrumentation Program (DURIP), Role: PI (Co-PIs: Golden G. Richard III and Vassil Roussev), Funding: $96,310, Project Duration: 1 year (2015 - 2016)

Travel (T)

T-17: "**[BoR].** Travel Grants for Emerging Faculty (TGEF)", Board of Regents - Louisiana, Funding: $1,200, 2016

T-18: "**[BoR].** Travel Grants for Emerging Faculty (TGEF)", Board of Regents - Louisiana, Funding: $1,200, 2014

Others (O)

O-19: $50,000 from UNO Foundation for ICS Equipment in 2016

O-20: $7,500 from UNO ORSP for Early Career Research Prize in December 2016

O-21: $10,000 from UNO CS Department for Equipment (PLC Trainers) in 2015

PEER-REVIEWED PUBLICATIONS

Journals/Book Chapters:

J-1: **[IEEE S&P]. Irfan Ahmed**, Vassil Roussev, "Peer Instruction Teaching Methodology for Cybersecurity Education", IEEE Security & Privacy. *(Invited article, Submitted)*

J-2: **[IEEE S&P]. Irfan Ahmed**, Sebastian Obermeier, Sneha Sudhakaran, Vassil Roussev, "Programmable Logic Controller Forensics", IEEE Security & Privacy, Vol. 15, No. 6, November 2017. *(Impact Factor: 1.38 in 2017)*

J-3: **[Taylor & Francis JCST].** Justin Russell, Carl Weems, **Irfan Ahmed**, Golden G. Richard III, "Self-reported secure and insecure cyber behaviour: factor structure and associations with personality factors", Journal of Cyber Security Technology, Taylor & Francis, 2017.

J-4: **[Book Chapter]. Irfan Ahmed**, Vassil Roussev, "Analysis of Cloud Digital Evidence", In Security, Privacy, and Digital Forensics in the Cloud, L. Chen, and H. Takabi (Eds.), IGI Global, 2017.

J-5: **[Elsevier DI].** Vassil Roussev, **Irfan Ahmed**, Andres Barreto, Shane McCulley, Vivek Shanmughan, "Cloud Forensics-Tool Development Studies & Future Outlook", Digital Investigation, Elsevier, Vol. 18, No. 3, September 2016. *(Impact Factor: 1.77 in 2017)*

J-6: **[IEEE Computer]. Irfan Ahmed**, Sebastian Obermeier, Martin Naedele, Golden G. Richard III, "SCADA Systems: Challenges for Forensic Investigators", In IEEE Computer, Vol. 45, No. 12, December 2012. *(Impact Factor: 1.75 in 2017)*

J-7: **[Springer IJIS]. Irfan Ahmed**, Martin Naedele, Bradley Schatz, Ryoichi Sasaki, Andrew West, "SCADA System Security", In International Journal of Information Security, Springer, Vol. 11, No. 4, August 2012. *(Editorial) (Impact Factor: 1.91 in 2016)*

J-8: **[Springer JCV]. Irfan Ahmed**, Kyung-suk Lhee, "Classification of Packet Contents for Malware Detection", In Journal in Computer Virology, Springer, Vol. 7, No. 4, pp. 279-295, October 2011. *(Impact Factor: 0.368 in 2016)*

J-9: **[IETE TR]. Irfan Ahmed**, Kyung-suk Lhee, Hyunjung Shin, and ManPyo Hong, "Content-based File-type Identification using Cosine Similarity and a Divide-and-Conquer approach", In IETE Technical Review, Vol. 27, No. 6, pp. 465-477, Nov 2010. *(Impact Factor: 1.33 in 2017)*

Conferences/Workshops:

C-10: **[ACM CODASPY].** Saranyan Senthivel, Shrey Dhungana, Hyunguk Yoo, **Irfan Ahmed**, Vassil Roussev, "Denial of Engineering Operations Attacks in Industrial Control Systems", In 8^{th} ACM Conference on Data and Application Security and Privacy (CODASPY'18), March 2018, Tempe, AZ, USA.

C-11: **[ACM SIGCSE].** Manish Bhatt, **Irfan Ahmed**, Zhiqiang Lin, "On the Use of Virtual Machine Introspection for OS Kernel Security Education", In 49^{th} ACM Technical Symposium on Computer Science Education (SIGCSE), February 2018, Baltimore, Maryland, USA.

C-12: **[Springer WISA].** Jonathan Grimm, **Irfan Ahmed**, Vassil Roussev, Manish Bhatt, ManPyo Hong, "Automatic Mitigation of Kernel Rootkits in Cloud Environments", In the 18^{th} World Conference on Information Security Applications (WISA'17), Lecture Notes in Computer Science (LNCS) Springer, August 2017, Jeju Island, South Korea

C-13: **[USENIX ASE].** William Johnson, **Irfan Ahmed**, Vassil Roussev, Cynthia B. Lee, "Peer Instruction for Digital Forensics", USENIX Advances in Security Education Workshop (ASE'17), co-located with 26^{th} USENIX Security Symposium, August 2017, Vancouver, BC, Canada

C-14: **[DFRWS].** Saranyan Senthivel, **Irfan Ahmed**, Vassil Roussev, "SCADA Network Forensics of the PCCC Protocol", In the 17^{th} Annual Digital Forensics Research Conference (DFRWS'17), August 2017, Austin, USA.
(Acceptance rate (32%): 13 full-papers / 41 full-paper submissions)

C-15: **[AAFS]. Irfan Ahmed**, "Supervisory Control and Data Acquisition (SCADA) Forensics: Network Traffic Analysis for Extracting a Programmable Logic Controller (PLC) System and Programming Logic Files", In the 69^{th} Annual Meeting of the American Academy of Forensic Sciences, February 2017, New Orleans, USA. *(Extended Abstract)*

C-16: **[ACSAC ICSS]. Irfan Ahmed**, Vassil Roussev, William Johnson, Saranyan Senthivel, Sneha Sudhakaran, "A SCADA System Testbed for Cybersecurity and Forensic Research and Pedagogy", In the 2^{nd} Annual Industrial Control System Security Workshop (ICSS'16), In conjunction with 32^{nd} Annual Computer Security Applications Conference (ACSAC'16), December 2016, Los Angeles, CA.

C-17: **[USENIX ASE].** William Johnson, Allison Luzader, **Irfan Ahmed**, Vassil Roussev, Golden G. Richard III, Cynthia B. Lee, "Development of Peer Instruction Questions for Cybersecurity Education", USENIX Advances in Security Education Workshop (ASE'16), co-located with 25^{th} USENIX Security Symposium, August 2016, Austin, TX

C-18: **[ACM WiSec].** Aisha Ali-Gombe, Golden G. Richard III, **Irfan Ahmed**, Vassil Roussev, "Don't Touch that Column: Portable, Fine-Grained Access Control for Android's Native Content Providers", In the 9^{th} ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'16), July 2016, Darmstadt, Germany.
(Acceptance rate (25.5%): 13 full-papers / 51 full-paper submissions)

C-19: **[IFIP DF].** Vassil Roussev, Andres Barreto, **Irfan Ahmed**, "Forensic Acquisition of Cloud Drives", In the 12^{th} IFIP WG 11.9 International Conference on Digital Forensics, January 2016, New Delhi, India

C-20: **[ACSAC PPREW].** Aisha Ali-Gombe, **Irfan Ahmed**, Golden G. Richard III, Vassil Roussev, "OpSeq: Android Malware Fingerprinting", In the 5^{th} Program Protection and Reverse Engineering Workshop (PPREW'15), In conjunction with 31^{st} Annual Computer Security Applications Conference (ACSAC'15), December 2015, Los Angeles, CA, USA.

C-21: **[ACM CODASPY]. Irfan Ahmed**, Vassil Roussev, Aisha Ali Gombe, "Robust Fingerprinting for Relocatable Code", In the 5^{th} ACM Conference on Data and Application Security and Privacy (CODASPY'15), March 2015, San Antonio, TX, USA.
(Acceptance rate (21%): 19 full papers / 91 submissions)

C-22: **[AAFS]. Irfan Ahmed**, Vassil Roussev, Aisha Ali Gombe, "Memory Forensics: Reliable In-Memory Code Identification Using Relocatable Pointers", In the 67^{th} Annual Meeting of the American Academy of Forensic Sciences, February 2015, Orlando, FL, USA. (Extended Abstract)

C-23: **[DFRWS].** Vassil Roussev, **Irfan Ahmed**, Thomas Sires, "Image-Based Kernel Fingerprinting", In the 14^{th} Annual Digital Forensics Research Conference (DFRWS'14), August 2014, Denver CO, USA.
(Acceptance rate (28.8%): 15 regular papers / 52 submissions)

C-24: **[AAFS]. Irfan Ahmed**, Golden G. Richard III, "Kernel Pool Monitoring to Support Malware Forensics in a Cloud Computing Environment", In the 66^{th} Annual Meeting of the American Academy of Forensic Sciences, February 2014, Washington, USA. *(Extended Abstract)*

C-25: **[AAFS].** Golden G. Richard III, **Irfan Ahmed**, "Compressed RAM and Live Forensics", In the 66^{th} Annual Meeting of the American Academy of Forensic Sciences, February 2014, Washington, USA. *(Extended Abstract)*

C-26: **[Springer ISC]. Irfan Ahmed**, Golden G. Richard III, Aleksandar Zoranic, Vassil Roussev, "Integrity Checking of Function Pointers in Kernel Pools via Virtual Machine Introspection", In the 16^{th} Information Security Conference (ISC'13), November 2013, Dallas, Texas, USA.
(Acceptance rate (23%): 16 regular papers / 70 submissions) ***(Best Paper Award)***

C-27: **[AAFS]. Irfan Ahmed**, Golden G. Richard III, "Live Forensic Analysis of Kernel Code for Malware Detection in Cloud Computing Environments", In the 65^{th} Annual Meeting of the American Academy of Forensic Sciences, February 2013, Washington, USA. *(Extended Abstract)* ***(Outstanding Research Award)***

C-28: **[IFIP DF]. Irfan Ahmed**, Aleksandar Zoranic, Salman Javaid, Golden G. Richard III, Vassil Roussev "Rule-based Integrity Checking of Interrupt Descriptor Table in Cloud Environments", In the 9^{th} IFIP WG 11.9 International Conference on Digital Forensics, January 2013, Orlando, Florida.

C-29: **[ACSAC LAW].** Salman Javaid, Aleksandar Zoranic, **Irfan Ahmed**, Golden G. Richard III, "Atomizer: Fast, Scalable and Lightweight Heap Analyzer for Virtual Machines in a Cloud Environment", In the 6^{th} Layered Assurance Workshop (LAW'12), In conjunction with 28^{th} Annual Computer Security Applications Conference (ACSAC'12), December 2012, Orlando, Florida, USA.

C-30: **[ICPP CloudSec]. Irfan Ahmed**, Aleksandar Zoranic, Salman Javaid, Golden G. Richard III, "ModChecker: Kernel Module Integrity Checking in the Cloud Environment", In the 4^{th} International Workshop on Security in Cloud Computing (CloudSec'12), In conjunction with 41^{st} International Conference on Parallel Processing (ICPP'12), Sept 2012, Pittsburgh, Pennsylvania.

C-31: **[IEEE NSS].** Eesa Al Soalmi, Colin Boyd, Andrew Clark and **Irfan Ahmed**, "User-Representative Feature Selection for Keystroke Dynamics" In the 5^{th} IEEE International Conference on Network and System Security (NSS' 11), pp. 229-233, September 2011, Milan, Italy.

C-32: **[ICRC].** Nishchal Kush, Ernest Foo, Ejaz Ahmed, **Irfan Ahmed**, Andrew Clark, "Gap Analysis of Intrusion Detection in Smart Grids", In International Cyber Resilience Conference, pp. 38-46, August 2011, Perth, Australia. ***(Best Paper Award)***

C-33: **[IFIP DF]. Irfan Ahmed**, Kyung-suk Lhee, Hyunjung Shin, and ManPyo Hong, "Fast Content-based File-type Identification", In the 7^{th} IFIP WG 11.9 International Conference on Digital Forensics, pp. 65-75, February 2011, Orlando, Florida, USA.

C-34: **[ACM SAC]. Irfan Ahmed**, Kyung-suk Lhee, Hyunjung Shin, and ManPyo Hong, "Fast File-type Identification", In the 25^{th} Annual ACM Symposium on Applied Computing, (SAC'10), ACM Special Interest Group on Applied Computing (SIGAPP), March 2010, Sierre, Switzerland.

C-35: **[Springer ACISP]. Irfan Ahmed**, Kyung-suk Lhee, Hyunjung Shin, and ManPyo Hong, "On Improving the Accuracy and Performance of Content-based File-type Identification", In the 14^{th} Australasian conference on information security and privacy (ACISP'09), Lecture notes in computer science (LNCS), pp. 44-59, July 2009, Brisbane, Australia.
(Acceptance rate (28.3%): 30 regular papers / 106 submissions)

C-36: **[IEEE ARES]. Irfan Ahmed**, Kyung-suk Lhee, "Detection of Malcodes by Packet Classification", In the International Workshop on Privacy and Security by means of Artificial Intelligence (PSAI'08), In conjunction with the 3^{rd} IEEE International Conference on Availability Reliability and Security (ARES'08), March 2008, Barcelona, Spain.

C-37: **[IEEE IAS]. Irfan Ahmed**, Usman Tariq, Shoaib Mukhtar, Kyung-suk Lhee, Seung-Wha Yoo, Piao Yanji and Manpyo Hong, "Binding Update Authentication Scheme for Mobile IPv6", In the 3^{rd} IEEE International Symposium on Information Assurance and Security (IAS'07), pp. 109-114, August 2007, Manchester, United Kingdom.

Posters/Work-in-progress Presentations:

P-1: **[ACM CODASPY].** Aisha Ibrahim Ali-Gombe, **Irfan Ahmed**, Golden G. Richard III, Vassil Roussev, "AspectDroid: Android App Analysis System", In 6^{th} ACM Conference on Data and Application Security and Privacy (CODASPY'16), March 2016, New Orleans, LA, USA.
(Outstanding Poster Award)

P-2: **[ACM CODASPY].** Anjila Tamrakar, Justin D. Russell, **Irfan Ahmed**, Golden G. Richard III, Carl F. Weems, "SPICE: A Software Tool for Bridging the Gap Between End-user's Insecure Cyber Behavior and Personality Traits", In 6^{th} ACM Conference on Data and Application Security and Privacy (CODASPY'16), March 2016, New Orleans, LA, USA.

P-3: **[ACSAC]. Irfan Ahmed**, Aleksandar Zoranic, "HookLocator: Function Pointer Integrity Checking in Kernel Pools via Virtual Machine Introspection", In 29^{th} Annual Computer Security Applications Conference (ACSAC'13), December 2013, New Orleans, LA, USA.

P-4: **[ACSAC].** Aisha Ali-Gombe, **Irfan Ahmed**, Golden G. Richard III, "DROIDHOOK: Android MalApp Detection Through Context", In 29^{th} Annual Computer Security Applications Conference (ACSAC'13), December 2013, New Orleans, LA, USA.

PhD Dissertation:

- **Irfan Ahmed**, "Fast and Accurate Content-classification Techniques for Malware Detection and File-type Identification", Ajou University, South Korea, June 2010

INVITED TALKS

Conferences/Workshops:

I-1: **[ACSAC ICSS].** "Programmable Logic Controller Forensics", In 3^{rd} Annual Industrial Control System Security Workshop (ICSS'17), In conjunction with 33^{rd} Annual Computer Security Applications Conference (ACSAC'17), December 2017, Orlando, FL USA.

I-2: **[ACSAC MMF].** "Reliable In-Memory Code Identification Using Relocatable Pointers", In Malware Memory Forensics Workshop (MMF), In conjunction with 30th Annual Computer Security Applications Conference (ACSAC'14), December 2014, New Orleans, LA, USA.

I-3: **[ACSAC NGMAD].** "Integrity Checking of Function Pointers in Kernel Pools – A Virtual Machine Introspection based Approach", In the Next Generation Malware Attacks and Defense Workshop (NGMAD), In conjunction with 29th Annual Computer Security Applications Conference (ACSAC'13), December 2013, New Orleans, LA, USA.

I-4: **[BIDM].** "Computer Forensics with Data Mining: File-Type Identification", In the Business Intelligence and Data Mining Conference (BIDM 2010), pp. 110-123, April, 2010, Seoul, South Korea.

Universities/Research Centers/Institutes:

I-4: **[Sacred Heart University].** "Modern Critical Infrastructure at the Risk of Cyberattacks", Sacred Heart University, `http://www.sacredheart.edu`, Oct 2017, Fairfield, CT, USA. *(Duration: 90 minutes)*

I-5: **[NSRI].** "Digital Forensics of Industrial Control System: An Academia Viewpoint", National Security Research Institute (NSRI), `http://www.nst.re.kr/nst_en/member/03_12.jsp`, August 2017, Yuseong-gu, Daejeon, South Korea. *(Duration: 2 hours)*

I-6: **[Soonchunhyang University].** "Digital Forensics of Industrial Control System: An Academia Viewpoint", Soonchunhyang University, `http://sgee.sch.ac.kr/`, August 2017, Chungcheongnam-do, South Korea. *(Duration: 60 minutes)*

I-7: **[Ajou University].** "Digital Forensics of Industrial Control System: An Academia Viewpoint", Ajou University, `https://www.ajou.ac.kr/en/`, August 2017, Suwon, Gyeonggi-do, South Korea. *(Duration: 60 minutes)*

TEACHING

University of New Orleans, New Orleans, USA Jan 2013 - To-date

Term	Course Number	Course Name	Student Population	Student Evaluation
Spring 2013	CSCI 4621/5621	Introduction to Computer Security	21	4.64 / 5.00
Fall 2013	CSCI 4311/5311	Computer Networks	26	4.13 / 5.00
Spring 2014	CSCI 4311/5311	Computer Networks	23	
Fall 2014	CSCI 4401/5401	Operating System	37	4.71 / 5.00
Fall 2014	CSCI 4621/5621	Introduction to Computer Security	33	4.88 / 5.00
Spring 2015	CSCI 4311/5311	Computer Networks	45	
Spring 2015	CSCI 4621/5621	Introduction to Computer Security	34	
Fall 2015	CSCI 6627	Industrial Control System Security	38	4.91 / 5.00
Fall 2015	CSCI 4621/5621	Introduction to Computer Security	26	4.95 / 5.00
Spring 2016	CSCI 6627	Industrial Control System Security	19	4.45 / 5.00
Spring 2016	CSCI 6621	Topics in Network Security and Forensics	20	4.56 / 5.00
Fall 2016	CSCI 4623/5623	Introduction to Computer Forensics	15	4.89 / 5.00
Fall 2016	CSCI 4621/5621	Introduction to Computer Security	25	4.42 / 5.00
Spring 2017	CSCI 6627	Industrial Control System Security	14	4.72 / 5.00
Spring 2017	CSCI 6621	Topics in Network Security and Forensics	10	4.71 / 5.00
Fall 2017	CSCI 4621/5621	Introduction to Computer Security	35	-

WORKSHOP/TUTORIALS/GUEST LECTURES

W-1: "Supervisory Control and Data Acquisition (SCADA) System Security", Workshop (Duration: 4 hours), Fordham University, New York, USA, Jun 2016

W-2: "Network Forensics", Guest Lecture (Duration: 1 hour), Queensland University of Technology, Brisbane, Australia, Jun 2011

THESIS/RESEARCH ADVISOR

University of New Orleans, New Orleans, USA

Postdocs

- Hyunguk Yoo — Aug 2017 - to-date
  PhD from Ajou University, South Korea

PhD Students:

- Syed Ali Qasim — Aug 2017 - to-date
- Manish Bhatt — June 2017 - to-date
- Aisha Ibrahim Ali-Gombe — August 2013 - May 2017
  Malware Analysis and Privacy Policy Enforcement Techniques for Android Applications (co-supervised with Dr. Golden G. Richard III)
  First employment: Assistant Professor at Towson University, MD

Master Students:

- Majde Bilal Judeh — Oct 2017 - to-date
- Sushma Kalle — Aug 2017 - to-date

- Pranita Deshpande — May 2017 - to-date
- Sharon Elizabeth Blake — August 2016 - to-date
- Jonathan Grimm — Sept 2015 - to-date
- Saranyan Senthivel — June 2016 - July 2017
  Automatic Forensic Analysis of PCCC Network Traffic Log
- William Eldon Johnson — July 2015 - May 2017
  Development of Peer Instruction Material for a Cybersecurity Curriculum
- Anjila Tamrakar — Summer 2014 - April 2016
  SPICE: A Software Tool for Studying End-user's Insecure Cyber Behavior and Personality-traits
- Dalbir Kaur Chhabra — Jan 2014 - Aug 2014
  Feature selection and clustering for malicious and benign software characterization

Undergraduate Students:

- Jose Rene Berlioz Rivera — Aug 2017 - to-date
- Shrey Dhungana — May 2017 - to-date
- Manish Bhatt — Dec 2016 - May 2017
- Banan Ibrahim — Oct 2016 - Jun 2017
- Phillip Bradley Reason — Feb 2016 - Jul 2016
- Philip Schwartz — May 2014 - Aug 2014

Queensland University of Technology, Brisbane, Australia

PhD Students:

- Eesa Alsolami - co-supervised with Dr. Colin Boyd — Mar 2011-Aug 2012
  Continuous Biometric Authentication: Keystroke Dynamics
- Nishchal Kush - co-supervised with Dr. Ernest Foo — Mar 2011-Sept 2011
  Smart Grid Security

THESIS COMMITTEE MEMBER

University of New Orleans, New Orleans, USA

PhD Students:

- Joseph T. Sylve — May 2017
  Towards Real-Time Volatile Memory Forensics: Frameworks, Methods, and Analysis

Master Students:

- Shane McCulley — May 2017
  Forensic Analysis of G-Suite Collaborative Services
- Vivek Oliparambil Shanmughan — May 2017
  Lightweight Environment for Cyber Security Education
- Andrew Case — June 2016
  Detecting Objective-C Malware through Memory Forensics
- Elyse Bond — June 2015
  Creating Volatility Support for FreeBSD
- Andres E. Barreto — June 2015
  API-Based Acquisition of Evidence from Cloud Storage Providers
- Robert Strickland — June 2015
  GPU Keystroke Logging and Detection on Microsoft Windows with Kernel Mode Drivers

- Salman Javaid Aug 2014
  Analysis and Detection of Heap-base Malware Using Introspection in a Virtualized Environment
- Christopher Stelly Nov 2013
  Dynamic User Defined Permissions for Android Devices
- Deekshit Kura Nov 2013
  Categorization of Large Corpora of Malicious Software

ACADEMIC SERVICES

Conference/Workshop Program Chair

- *Industrial Control System Security (ICSS) Workshop*, In conjunction with 33^{rd} Annual Computer Security Applications Conference (ACSAC'17), December 2017, San Juan, Puerto Rico, USA.
  `https://www.acsac.org/2017/workshops/icss/`
- *Industrial Control System Security (ICSS) Workshop*, In conjunction with 32^{nd} Annual Computer Security Applications Conference (ACSAC'16), December 2016, Los Angeles, California.
  `http://acsac.org/2016/workshops/icss/`
- *Industrial Control System Security (ICSS) Workshop*, In conjunction with 31^{st} Annual Computer Security Applications Conference (ACSAC'15), December 2015, Los Angeles, California.
  `http://acsac.org/2015/workshops/icss/`
- *Malware Memory Forensics Workshop (MMF)*, In conjunction with 30^{th} Annual Computer Security Applications Conference (ACSAC'14), December 2014, New Orleans, LA, USA.
  `https://www.acsac.org/2014/workshops/mmf/`
- Track Chair of *Intrusion Detection and Forensics Track*
  IEEE World Congress on Information and Communication Technologies (WICT 2011), 11-14 December 2011, Mumbai, India
  `http://www.mirlabs.net/wict11/`

Technical Program Committee Member

- ACM Technical Symposium on Computer Science Education (SIGCSE) – 2017
- Digital Forensics Research Conference (DFRWS) – 2015, 2016
- International Conference on Digital Forensics & Cyber Crime (ICDF2C) – 2013, 2014, 2015, 2016, 2017
- International Conference on High Performance Computing and Communications (HPCC) – 2014
- International Conference on Emerging Technologies (ICET) – 2012, 2013, 2017
- Annual Cyber and Information Security Research Conference (CISRC), held at Oak Ridge National Laboratory – 2018

Panel/Session Moderator and Panelist

- Panelist on "Infrastructure Cybersecurity: Industry, Government, and Academia Viewpoints", University of New Orleans Engineering Forum, and Southeast Symposium on Contemporary Engineering Topics (SSCET), New Orleans LA, Sept 2017.
- Moderator of a panel on "SCADA System Security: Challenges and Future Directions", Annual Computer Security Applications Conference (ACSAC), New Orleans LA, Dec 2014

Journal Guest Editor

- *Special Issue on SCADA and Control System Security*, In International Journal of Information Security (IJIS), Springer, Vol. 11, No. 4, August 2012
- *Special Issue on Applications of Machine Learning Techniques on Intrusion Detection and Digital Forensics*, In Security and Communication Networks Journal, Wiley
  `http://onlinelibrary.wiley.com/doi/10.1002/sec.344/full`

Journal Reviewer

- IEEE Security & Privacy www.computer.org/security-and-privacy
- IEEE Computer www.computer.org/computer
- Computers & Security, Elsevier www.journals.elsevier.com/computers-and-security
- ACM Transactions on Cyber-Physical Systems http://tcps.acm.org
- IEEE Transactions on Computers http://www.computer.org/web/tc
- Journal of Network and Computer Application, Elsevier http://www.journals.elsevier.com/journal-of-network-and-computer-applications/
- IETE Technical Review Journal http://tr.ietejournals.org
- International Journal of Network Security http://ijns.femto.com.tw
- Security and Communication Networks, Wiley http://onlinelibrary.wiley.com/journal/10.1002/(ISSN)1939-0122
- Journal of Applied Mathematics, Hindawi http://www.hindawi.com/journals/jam/