Co-Organizer

Dr. Cliff Wang

Affiliation/Position

National Science Foundation /

Program Director and Co-lead for NSF SaTC Program

Biography

Dr. Cliff Wang graduated from North Carolina State University with a PhD in computer engineering in 1996. He has been carrying out research in the area of computer vision, medical imaging, high speed networks, and most recently cyber security. He has authored many technical papers and 3 Internet standards RFCs. Dr. Wang authored/edited more than 20 books in the area of information security and holds 4 US patents on information security system development.

Since 2003, Dr. Wang has been managing extramural research portfolio and leading cyber security research at ARO and now at NSF. He currently serve as the program director and co-lead of SaTC program at NSF Dr. Wang also holds appointment at both Department of Computer Science and Department of Electrical and Computer Engineering at North Carolina State University. Dr. Wang is a Fellow of IEEE and AAAS.

Co-Organizer

Dr. Selçuk Uluağaç

Affiliation/Position

National Science Foundation /

Director, SaTC Program

Biography

Dr. Selcuk Uluagac is currently a Program Director in Secure and Trustworthy Cyberspace (SaTC) Program at US National Science Foundation (NSF)'s Directorate for Computer and Information Science and Engineering (CISE) from Florida International University (FIU) (Miami, Florida). At FIU, he is an Eminent Scholar Chaired Professor in the Knight Foundation School of Computing and Information Science, leading the Cyber-Physical Systems Security Lab with an additional courtesy appointment in the Department of Electrical & Computer Engineering. Before, he was a Senior Researcher at Georgia Tech. He holds a PhD from Georgia Tech and MS from Carnegie Mellon University in cybersecurity. His research is in cybersecurity and privacy with emphasis on their practical aspects (focusing on systems security topics, malware, ransomware, forensics, IoT, CPS, smart systems). He has hundreds of research papers, including the most reputable venues such as NDSS, USENIX Security, IEEE TIFS. He has served on the PC of top-tier security conferences such as NDSS, USENIX Security, ACM CCS, IEEE SP. In 2023, he was the TPC Chair of Security & ML Track of ACM CCS 2023, IEEE CNS in 2022, and was the General Chair of ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec) in 2019. He currently serves as the deputy editor in-chief of IEEE TIFS and associate editors of IEEE TMC and Elsevier COMNET journals. More information can be obtained from https://users.cs.fiu.edu/~suluagac/.

Keynote

Prof. Chun-I Fan

Affiliation/Position

Dept. of Computer Science and Engineering,
National Sun Yat-sen University /
Distinguished Professor

Title:

Secure Electronic Health Record Mechanism Supporting Privacy-Preserving Cloud Outsourcing

Abstract

With the rapid development of health information technology, most hospitals have implemented Electronic Medical Record (EMR) into their medical environment. Simultaneously, these hospitals also joined in the EMR exchange center and followed the EMR transmission standard proposed by the Ministry of Health and Welfare in Taiwan. It helps hospitals exchange EMRs under the same protocol and simplifies the procedure when patients are referred to another hospital by doctors. However, although the exchange standard is robust under the National Health Insurance information virtual private network in Taiwan, the medical data are restricted into the enclosed environment. It results in medical data being difficult to be opened to industry and academia and causes some privacy and security issues. Therefore, the research team cooperated with Kaohsiung Veterans General Hospital based on the international Fast Healthcare Interoperability Resources standard designed a privacy-preserving medical data warehouse system supporting secure data mining and realized the proposed standard focusing on the collection search, storage, data mining, and applications. Furthermore, the research team also shared the designed mechanism and results with the Ministry of Health and Welfare in Taiwan. We built a privacy-preserving digital medical data environment based on cryptographic technologies. It can provide a secure environment for hospitals to securely upload medical data to a public cloud and open the medical data. We expect this system to be a foundation for intelligent and precision medicine. This

work won the "Brightest Achievement Award" from the Office of Technology Promotion Program in Advanced Cybersecurity Research of the National Science and Technology Council (NSTC), the 2023 "FutureTech Award", and the 20th "National Innovation Award" in Taiwan.

Biography

Chun-I Fan received the M.S. degree in computer science and information engineering from National Yang Ming Chiao Tung University, Hsinchu, Taiwan, in 1993, and the Ph.D. degree in electrical engineering from National Taiwan University, Taipei, Taiwan, in 1998. From 1999 to 2003, he was an Associate Researcher and a Project Leader with Telecommunication Laboratories, Chunghwa Telecom Company, Ltd., Taoyuan, Taiwan. In 2003, he joined the faculty of the Department of Computer Science and Engineering, National Sun Yat-sen University (NSYSU), Kaohsiung, Taiwan. He has been a Full Professor since 2010 and a Distinguished Professor since 2019. His current research interests include applied cryptology, information security, network security, and AI security. Prof. Fan was the Dean of the College of Engineering and is the Director of Information Security Research Center at National Sun Yat-sen University. He also is the Chairman of Chinese Cryptology and Information Security Association (CCISA), Taiwan, and was the Chief Executive Officer (CEO) of Telecom Technology Center (TTC), Taiwan. Prof. Fan was the recipient of the Best Student Paper Awards from the National Conference on Information Security in 1998, the Dragon Ph.D. Thesis Award from Acer Foundation, and the Best Ph.D. Thesis Award from the Institute of Information and Computing Machinery in 1999. Prof. Fan won the Engineering Professors Award from Chinese Institute of Engineers - Kaohsiung Chapter in 2016, the 18th Y. Z. Hsu Science Paper Award from Far Eastern Y. Z. Hsu Science and Technology Memorial Foundation in 2020, the Outstanding Technical Achievement Award from IEEE Tainan Section in 2020, the Best Journal Paper Award from Taiwan Association of Cloud Computing in 2022, and the FutureTech Award from National Science and Technology Council of Taiwan in 2023. He also is an Outstanding Faculty in Academic Research in NSYSU and one of the World's Top 2% Scientists.

Keynote

Prof. Somesh Jha

Affiliation/Position

University of Wisconsin, Madison/

Lubar Professor

Computer Sciences Department

Title:

Publicly-Detectable Watermarking for Language Models

Abstract

We present a highly detectable, trustless watermarking scheme for LLMs: the detection algorithm contains no secret information, and it is executable by anyone. We embed a publicly-verifiable cryptographic signature into LLM output using rejection sampling. We prove that our scheme is cryptographically correct, sound, and distortion-free. We make novel uses of error-correction techniques to overcome periods of low entropy, a barrier for all prior watermarking schemes. We implement our scheme and make empirical measurements over open models in the 2.7B to 70B parameter range. Our experiments suggest that our formal claims are met in practice.

Biography

Somesh Jha is a Lubar Professor of Computer Science in the Department of Computer Sciences at the University of Wisconsin-Madison. Jha studies security and formal methods, particularly adversarial machine learning and privacy. More specifically, his work focuses on analysis of security protocols, survivability analysis, intrusion detection, formal methods for security, and analyzing malicious code. Recently he has focused his interests on topics related to trustworthy ML. He is an ACM Fellow and Distinguished Scientist, an IEEE Fellow, an AAAS Fellow, and is the recipient of an NSF Career Award.

Keynote

Prof. Wenjing Lou

Affiliation/Position

Virginia Tech/ W.C. English Endowed Professor

Title:

Security and Privacy in 5G and Beyond Networks

Abstract

While softwarization, cloudification, and advanced radio access network (RAN) technologies have been key enablers for 5G, the focus of next-generation mobile networks is likely to shift. Integrating AI/ML into networks, adopting open-RAN architecture, and enhancing security will likely be the key differentiators.

This talk will address various security and privacy challenges in 5G and beyond networks. We will cover the O-RAN initiative and zero-trust architecture, as well as introduce our recent research on building a secure framework to prevent mobile tracking, block unwanted calls, and implement a blockchain-based spectrum management system.

Biography

Wenjing Lou is the W. C. English Endowed Professor of Computer Science at Virginia Tech and a Fellow of the IEEE and ACM. Her research interests cover many topics in the cybersecurity field, with her current research interest focusing on wireless networks, blockchain systems, trustworthy machine learning systems, and security and privacy problems in the Internet of Things (IoT) systems. Prof. Lou is a highly cited researcher by the Web of Science Group. She received the Virginia Tech Alumni Award for Research Excellence in 2018, the highest university-level faculty research award. She received the INFOCOM Test-of-Time paper award in 2020. She is the TPC chair for IEEE INFOCOM 2019 and ACM WiSec 2020. She was the Steering Committee Chair for IEEE CNS conference from 2013 to 2020. She is currently a steering committee member of IEEE INFOCOM and IEEE CNS. She served as a program director at US National Science Foundation (NSF) from 2014 to 2017.

Keynote

Prof. Ying-Dar Lin

Affiliation/Position

IEEE / Fellow

Dept. of Computer Science,

National Yang Ming Chiao Tung University /

Chair Professor

National Institute of Cyber Security / Vice President

Title:

AI for cybersecurity & cybersecurity for AI

Abstract

AI has stepped into cybersecurity to better recognize the footprints of attack techniques, lifecycles (kill chains), and even disinformation and scam on social networks. AI itself also becomes the target of adversarial attacks as it is heavily used in various classification and generative applications. In this talk, I highlight research works done in National Institute of Cyber Security (NICS) and in my own lab at National Yang Ming Chiao Tung University (NYCU). At NICS, there are related research on (1) correlating sighting data and intelligence data for recognizing kill chains, (2) analyzing social network behaviors for anti-disinformation and anti-scam, (3) testing generative AI and classification AI for product certification. We also select a few research works done at NYCU: (1) network and host sighting to recognize attack techniques and kill chains, (2) cyber threat intelligence to trace attack path, (3) adversarial attack and defense when AI itself is used in intrusion detection.

Biography

Ying-Dar Lin is Vice President of National Institute of Cyber Security (NICS), and also a Chair Professor of computer science at National Yang Ming Chiao Tung University (NYCU), Taiwan. He received his Ph.D. in computer science from the University of California at Los Angeles (UCLA) in 1993. He was a visiting scholar at Cisco Systems in San Jose during 2007–2008, CEO at Telecom Technology Center, Taiwan, during 2010-2011, and Vice President of National Applied Research Labs (NARLabs), Taiwan, during 2017-2018. He cofounded L7 Networks Inc. in 2002, later acquired by D-Link Corp. He also founded and directed Network Benchmarking Lab (NBL) from 2002, which reviewed network products with real traffic and automated tools, also an approved test lab of the Open Networking Foundation (ONF), and spun-off O'Prueba Inc. in 2018. His recent research interests include machine learning for cybersecurity, wireless communications, network softwarization, and mobile edge computing. His work on multi-hop cellular was the first along this line, and has been cited over 1000 times and standardized into IEEE 802.11s, IEEE 802.15.5, IEEE 802.16j, and 3GPP LTE-Advanced. He is an IEEE Fellow (class of 2013), IEEE Distinguished Lecturer (2014–2017), ONF Research Associate (2014-2018), and received K. T. Li Breakthrough Award in 2017 and Research Excellence Award in 2017 and 2020. He has served or is serving on the editorial boards of many IEEE journals and magazines, including Editor-in-Chief of IEEE Communications Surveys and Tutorials (COMST) with impact factor increased from 9.22 to 25.3 during his term (2017-2020). He published a textbook, Computer Networks: An Open Source Approach, with Ren-Hung Hwang and Fred Baker (McGraw-Hill, 2011).

Lightning Talks

Prof. **Tsungnan Lin**

Affiliation:

Dept. of Electrical Engineering, National Taiwan University

Biography:

https://www.ee.ntu.edu.tw/profile2.php?teacher_id=901147&p=3

Speech Title:

Resilient Networks and Systems

Prof. **Yanchao Zhang**

Affiliation: Arizona State University

Biography:

https://search.asu.edu/profile/1620062

Speech Title:

Security and Privacy Challenges in FutureG Wireless Networks

Prof. **Jun-Cheng Chen**

Affiliation:

Research Center for Information Technology Innovation,

Academia Sinica

Biography:

https://www.citi.sinica.edu.tw/pages/pullpull/index_en.html

Speech Title:

Towards More General Deepfake Detection Foundation Model Adaptation

Lightning Talks

Prof. **Yi-Ting Huang**

Affiliation:

Dept. of Electrical Engineering,

National Taiwan University of Science and Technology

Biography:

https://antslabtw.github.io/faculty/

Speech Title:

The Future of Cybersecurity: Exploring AI-Driven

Prof. **Ruei-Hau Hsu**

Affiliation:

Dept. of Computer Science and Engineering,

National Sun Yat-sen University

Biography:

https://sites.google.com/site/drrueihauhsu/

Speech Title:

Security and Privacy for Intelligent Computing in Next Generation Communications

Prof. **Chinyang Henry Tseng**

Affiliation:

Dept. of Computer Science and Information Engineering,

National Taipei University

Biography:

https://web.ntpu.edu.tw/~tsengcyt/english.html

Speech Title:

Feature Value Classification Tendency

Lightning Talks

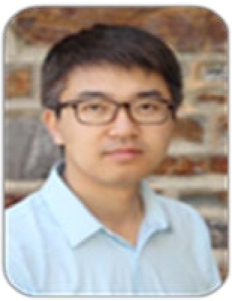
Prof. **Neil Gong**

Affiliation: Duke University

Biography:

https://people.duke.edu/~zg70/

Speech Title: Safe and Robust Generative AI



Prof. **Amir Houmansadr**

Affiliation: University of Massachusetts Amherst

Biography:

https://people.cs.umass.edu/~amir/index.php

Speech Title:

Injecting Bias in Text-To-Image Models via Composite-Trigger Backdoors

Prof. **Ruzica Piskac**

Affiliation: Yale University

Biography:

http://www.cs.yale.edu/homes/piskac/

Speech Title: Formal Privacy-Preserving Verification

Lightning Talks

Prof. **David Wu**

Affiliation: The University of Texas at Austin

Biography:

https://www.cs.utexas.edu/~dwu4/

Speech Title:
Private Information Retrieval: Recent Advances and Challenges

Prof. **Dongyan Xu**

Affiliation: Purdue University

Biography:

https://www.cs.purdue.edu/homes/dxu/
Speech Title:
Computer Systems Security in a Cyber-Physical World

Prof. **Tsui Peng**

Affiliation:

Department of Information and Financial Management,

National Taipei University of Technology

Biography:
https://tipeng.wixsite.com/school/about

Speech Title:

End-to-end resilience in MLOps

Lightning Talks

Prof. **Wen-Huang Cheng**

Affiliation:

Dept. of Computer Science and Information Engineering,
National Taiwan University

Biography: https://www.csie.ntu.edu.tw/~wenhuang/

Speech Title:

Artificial Intelligence Security:
Adversarial Attacks and Hallucinations in AI Model

Prof. **Cho-Jui Hsieh**

Affiliation: University of California, Los Angeles

Biography:

https://web.cs.ucla.edu/~chohsieh/

Speech Title: Are Large Language Models Oversensitive?

Prof. **Suman Jana**

Affiliation: Columbia University

Biography:

https://www.cs.columbia.edu/~suman/

Speech Title:

Secure and Trustworthy Machine Learning: How far are we?

Lightning Talks

Prof. **Sneha Kumar Kasera**

Affiliation: University of Utah

Biography:

https://www.cs.utah.edu/~kasera

Speech Title: A Real-time System for Detection, Classification, and Analysis of Aviation Signals

Prof. **Sanmi Koyejo**

Affiliation: Stanford University

Biography:

https://cs.stanford.edu/~sanmi/

Speech Title:

DecodingTrust: A Comprehensive Assessment of Trustworthiness in GPT Models

Prof. **Zhuo Lu**

Affiliation: University of South Florida

Biography:

https://csalab.site/

Speech Title:

Security for Machine Learning in Wireless Networking

Lightning Talks

Prof. **Gang Wang**

Affiliation: University of Illinois Urbana-Champaign

Biography:

http://gangw.cs.illinois.edu/

Speech Title:

Machine Learning Enabled Abuse and Security Defense

Prof. **Ning Zhang**

Affiliation: Washington University in St. Louis

Biography:

https://engineering.wustl.edu/faculty/Ning-Zhang.html

Speech Title:

Security Protection for the Cyber-physical World

Prof. **Jung-Shian Li**

Affiliation:

Dept. of Electrical Engineering,

National Cheng Kung University

Biography:

https://www.ee.ncku.edu.tw/en/teacher/index2.php?teacher_id=22

Speech Title:

Critical Water Infrastructure Cybersecurity Testbed

Lightning Talks

Prof. **Mao-Hsiu Hsu**

Affiliation:

Dept. of Electro-Optical Engineering,

National Formosa University

Biography:

http://nfueo-e.nfu.edu.tw/files/11-1100-8196-1.php

Speech Title:

Deepfake Tiny Fingerprint Detection with Data Center

Prof. **Arijit Karati**

Affiliation:

Dept. of Computer Science and Engineering,

National Sun Yat-sen University

Biography:

https://www.ak.canseclab.com/

Speech Title:

Security Enhancement of Smart Card Authentication

Distinguished Prof. **Jyh-Ching Juang**

Affiliation:

Dept. of Electrical Engineering,

National Cheng Kung University

Biography:

https://www.ee.ncku.edu.tw/en/teacher/index2.php?teacher_id=58

Speech Title:

Lean Satellite and Cybersecurity

Lightning Talks

Prof. **Yu-Chi Chen**

Affiliation:

Dept. of Computer Science and Information Engineering,

National Taipei University of Technology

Biography:

https://wycchen.github.io/

Speech Title:

Privacy-preserving Verification with Compression Techniques

Prof. **Shun-Wen Hsiao**

Affiliation:

Dept. of Management Information Systems,

National Chengchi University

Biography:

https://sites.google.com/view/mikehsiao/

https://mis2.nccu.edu.tw/en/Faculty/Faculty_01/Shun-Wen-Hsiao-19738494

Speech Title:

Cyber Attack Analysis with Packet Payload Embedding