SHAGUFTA MEHNAZ

Assistant Professor, Department of Computer Science, Dartmouth College
https://smehnaz.github.io
Shagufta.Mehnaz@Dartmouth.edu (765)-409-7410

RESEARCH INTEREST

My broad research interest is at the intersection of information security, privacy, and machine learning, more specifically, *security and privacy of machine learning*, *privacy-preserving analytics*, and *machine learning for security*. I am particularly passionate about building practical data-driven systems that take into account both data security and privacy while also keeping the intended functionality of the system unimpaired.

PROFESSIONAL EXPERIENCE

- **Assistant Professor** **Winter 2021 - Present**
  Department of Computer Science, Dartmouth College.
- **Research and Teaching Assistant, Purdue University.** **2014 - 2020**
  Advisor: Elisa Bertino
  Topics: Privacy-preserving machine learning techniques and intrusion detection systems.
- **Research Associate Intern, Edge/IoT Lab, Hewlett Packard Enterprise Labs.** **Summer 2017**
  Mentor: Dr. Amip Shah
  Topic: Privacy-preserving anomaly detection for Internet of Things (IoT).
  – Research results published in a conference paper [8].
- **Research Associate Intern, Analytics Lab, Hewlett Packard Enterprise.** **Summer 2016**
  Mentors: Dr. Gowtham Bellala and Dr. Amip Shah
  Topic: Privacy-preserving distributed data analytics.
  – Research results published in three patents and two conference papers [3, 4].
- **Graduate Technical Intern, Binary Translation Group, Intel Corporation.** **Summer 2015**
  Mentor: Dr. Koichi Yamada
  Topic: Identifying and defending against VM evasion techniques used by malware.

EDUCATION

Purdue University

- **Ph.D. in Computer Science** **Summer 2020**
  Advisor: Elisa Bertino
  Advisory Committee: Mike Atallah, Chris Clifton, and Ninghui Li.
  Thesis: Fine-Grained Anomaly Detection for in Depth Data Protection
- **M.S. in Computer Science**, GPA: 3.93 **Spring 2016**

Bangladesh University of Engineering and Technology

- **B.Sc. in Computer Science and Engineering**, GPA: 3.97 **Spring 2013**
  Class Rank: 1st among 142 students (summa cum laude)
  Advisor: Md. Sohel Rahman
  Thesis: A study and some new results on Pairwise Compatibility Graphs

Last updated on January 21, 2022

GRANTS

- Title: **"Secure and Privacy-Preserving Machine Learning".**
  Sponsor: Walter and Constance Burke Research Initiation Award.
  Amount: $30K.
  Single PI.

SELECTED PUBLICATIONS

Conferences:

[12] S. DIBBO, D. CHUNG, S. MEHNAZ, "An In-depth Analysis of Disparate Vulnerability in Model Inversion Attacks", under submission, 2022.

[11] B. MCNUTT*, A. DOCENA*, S. MEHNAZ, "Mitigating Targeted Label Flipping Attacks in Federated Learning under Non-IID Settings", under submission, 2022. (* Equal contribution)

[10] C. GAO*, K. GU*, S. VOSOUGHI, S. MEHNAZ, "Reinforce Attack: Adversarial Example Attack against BERT with Reinforcement Learning", under submission, 2022. (* Equal contribution)

[9] S. MEHNAZ, S. DIBBO, E. KABIR, N. LI, E. BERTINO, "Are Your Sensitive Attributes Private?: Novel Model Inversion Attribute Inference Attacks on Classification Models", 31st USENIX Security Symposium (**USENIX Security**), 2022.

[8] S. MEHNAZ, E. BERTINO, "Privacy-preserving Real-time Anomaly Detection Using Edge Computing", 36th IEEE International Conference on Data Engineering (**ICDE**), 2020. Acceptance rate: 22.7% [129/568].

[7] S. MEHNAZ, A. MUDGERIKAR, E. BERTINO, "RWGuard: A Real-Time Detection System Against Cryptographic Ransomware", International Symposium on Research in Attacks, Intrusions, and Defenses (**RAID**), 2018. Acceptance rate: 22.8% [33/145].

[6] S.R. HUSSAIN, O. CHOWDHURY, S. MEHNAZ, E. BERTINO, "LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE". 25th Network and Distributed System Security (**NDSS**), 2018. Acceptance rate: 21.5% [71/331].

[5] S. MEHNAZ, E. BERTINO, "Ghostbuster: A Fine-grained Approach for Anomaly Detection in File System Accesses", 7th ACM Conference on Data and Applications Security and Privacy (**CODASPY**), 2017. Acceptance rate: 16% [21/134]. 🏆 **Best Paper Award**.

[4] S. MEHNAZ, G. BELLALA, E. BERTINO, "A Secure Sum Protocol and Its Application to Privacy-preserving Multi-party Analytics", ACM Symposium on Access Control Models and Technologies (**SACMAT**), 2017. Acceptance rate: 28% [14/50].

[3] S. MEHNAZ, E. BERTINO, "Privacy-preserving Multi-party Analytics over Arbitrarily Partitioned Data", 10th IEEE International Conference on Cloud Computing (**IEEE CLOUD**), 2017. Acceptance rate: 18%.

[2] S. R. HUSSAIN, S. MEHNAZ, S. NIRJON, AND E. BERTINO, "SeamBlue : Seamless Bluetooth Low Energy Connection Migration for Unmodified IoT Devices", International Conference on Embedded Wireless Systems and Networks (**EWSN**), 2017. ★ **Best Paper Award Nomination**.

[1] S. MEHNAZ, E. BERTINO, "Building Robust Temporal User Profiles for Anomaly Detection in File System Accesses", IEEE International Conference on Privacy, Security and Trust (**PST**), 2016.

Journals:

[2] S. MEHNAZ, E. BERTINO, "A Fine-grained Approach for Anomaly Detection in File System Accesses with Enhanced Temporal User Profiles", IEEE Transactions on Dependable and Secure Computing (**TDSC**), vol 18(6): pages 2535-2550, 2021.

[1] S. R. HUSSAIN, S. MEHNAZ, S. NIRJON, AND E. BERTINO, "Secure Seamless Bluetooth Low Energy Connection Migration for Unmodified IoT Devices", IEEE Transactions on Mobile Computing (**TMC**), vol 17(4), pages 927-944, 2018.

Patents:

[3] S. MEHNAZ, G. BELLALA, "Performing Privacy-Preserving Multi-Party Analytics on Vertically Partitioned Local Data", US Patent App. 15/421,041.

[2] S. MEHNAZ, G. BELLALA, "Performing Privacy-Preserving Multi-Party Analytics on Horizontally Partitioned Local Data", US Patent App. 15/421,144.

[1] S. MEHNAZ, G. BELLALA, "Computing a Global Sum that Preserves Privacy of Parties in a Multi-party Environment", US Patent App. 15/410,714.

Pre-prints:

[1] S. MEHNAZ, N. LI, E. BERTINO, "Black-box Model Inversion Attribute Inference Attacks on Classification Models", arXiv preprint arXiv:2012.03404, 2020.

Posters:

[3] S. R. HUSSAIN, S. MEHNAZ, S. NIRJON, AND E. BERTINO, "Seamless and Secure Bluetooth LE Connection Migration", ACM Conference on Data and Applications Security and Privacy (**CODASPY**), 2017.

[2] S. MEHNAZ, E. BERTINO, "iSONG - Intrusion into SOcial Network Groups", Network and Distributed System Security (**NDSS**), 2016.

[1] S. MEHNAZ, E. BERTINO, "Hey, I Am In: Intrusion into Online Social Network Groups", Grace Hopper Celebration (**GHC**), 2014.

OPEN SOURCE TOOLS

- Privacy-preserving Real-time Anomaly Detection Using Edge Computing.
  https://github.com/smehnaz/PPAD
- A Secure Sum Protocol and Its Application to Privacy-preserving Multi-party Analytics over Horizontally, Vertically, and Arbitrarily Partitioned Data.
  https://github.com/smehnaz/Priv-Pres-Analytics

TEACHING EXPERIENCE

- **Assistant Professor**, Dartmouth College.
  Course: Security and Privacy (COSC 55) **Fall 2021**
  – This course provides an introduction to the theory and application of computer security and privacy.

Course: Security and Privacy of Machine Learning (COSC 89/189) **Winter, Fall 2021**
– This course explores recent academic research at the intersection of machine learning, security, and data privacy that demonstrates the risks adversaries pose to machine learning systems.

- **Graduate Teaching Assistant**, Purdue University. **Fall 2014 - Spring 2015**
  Course: Problem Solving And Object-Oriented Programming Lab (CS180)
  – Designed homework problems, set exam questions, graded assignments, and supervised group projects with 3-4 students in each group.

- **Guest Lecturer**, Purdue University.
  Course: Data Security & Privacy (CS590) **Spring 2019**
  – Lecture on RWGuard, a real-time cryptographic ransomware detection system.
  Course: Database Management (CS541) **Spring 2018**
  – Lecture on Ghostbuster, a fine-grained approach for anomaly detection in file system accesses.

- **Lecturer**, Bangladesh University of Engineering and Technology. **Spring 2013 - Fall 2013**
  Courses: Structured Programming Language, Compilers, Systems Design, Assembly Language
  – Designed lab problems, quiz and final exam questions, and supervised projects.

- **Lecturer**, Ahsanullah University of Science and Technology. **Summer 2013 - Fall 2013**
  Courses: Computer Fundamentals, Computer Graphics
  – Designed lab problems, quiz and final exam questions, and supervised projects.

AWARDS & HONORS

2022	Walter and Constance Burke Research Initiation Award.
2019-2020	Bilsland Dissertation Fellowship, sponsored by Purdue University.
2015-2019	Faculty For The Future (FFTF) Fellowship, Schlumberger Foundation.
2019	Grace Hopper Celebration (GHC) Invited Speaker and Travel Scholarship.
2018	Network and Distributed System Security (NDSS) Symposium Travel Grant Award.
2018	Selected as one of the 200 Young Researchers to attend Heidelberg Laureate Forum (HLF) along with Travel Scholarship.
2017	Best Paper Award, ACM Conference on Data and Applications Security (CODASPY).
2015	Facebook Travel Grant Award to attend the WiCyS conference.
2014	Grace Hopper Celebration (GHC) Student Scholarship.
2009-2013	Bangladesh University of Engineering & Technology Dean's List Award for all academic years and Merit Scholarship.

ADVISING

- **PhD Students**
  – Ehsanul Kabir Fall 2021 - Now
  – Kang Gu Fall 2021 - Now
  – Sayanton Dibbo Summer 2021 - Now
  – Amel Docena Summer 2021 - Now

- **MS Students**
  – Brody McNutt Winter 2021 - Now

- **Undergraduate Students**
  - Ziray Hao — Winter 2022 - Now
  - Neha Ramsurrun — Winter 2022 - Now
  - Dae Lim Chung — Fall 2021 - Now

THESIS COMMITTEE MEMBER

- **PhD Students**
  - Prashant Anantharaman — 2021 - Now
  - Peter Brady — 2021 - Now
  - Sameed Ali (RPE) — 2021
- **Undergraduate Students**
  - Sydney Lister — 2021

TALKS

- **Secure and Privacy-preserving Data-driven Systems**
  Invited talk at NSF RESET Conference, 2021
- **Security and Privacy Risks of Machine Learning**
  Invited talk at NSysS Conference, 2020
- **Privacy-preserving Real-time Anomaly Detection Using Edge Computing**
  Conference talk at ICDE, 2020
- **RWGuard: A Real-Time Detection System Against Cryptographic Ransomware**
  Conference talk at RAID, Greece, 2018
- **Ghostbuster: A Fine-grained Approach for Anomaly Detection in File System Accesses**
  Conference talk at CODASPY, Arizona, US, 2017
  Invited talk at Award Winning Research Session, Grace Hopper Celebration (GHC), 2019
  Invited talk at Product Lifecycle Management (PLM) Center, Purdue University, 2016
- **A Secure Sum Protocol and Its Application to Privacy-preserving Multi-party Analytics**
  Conference talk at SACMAT, Indiana, US, 2017
- **Privacy-preserving Multi-party Analytics over Arbitrarily Partitioned Data**
  Conference talk at IEEE CLOUD, Hawaii, US, 2017

DEPARTMENT SERVICES

- Dartmouth College CS Faculty Hiring Committee, 2022.
- Computer Science Ph.D. Admissions Committee, 2020-21.
- Webmaster, Dartmouth College Computer Science, 2021-2022.

ACADEMIC SERVICE

Program Committee Member:

- ACM Conference on Computer and Communications Security (CCS), 2022.
- USENIX Security Symposium, 2022.
- Privacy Enhancing Technologies Symposium (PETS), 2022.

- Annual Computer Security Applications Conference (ACSAC), 2021.
- Web Conference (formerly known as WWW conference), 2021.
- ACM Conference on Data and Applications Security and Privacy (CODASPY), 2021.
- ACM Symposium on Access Control Models and Technologies (SACMAT), 2021.

External Reviewer (Selected):

- Conference on Information and Knowledge Management (CIKM), 2019.
- Web Conference (formerly known as WWW conference), 2019.
- IEEE International Conference on Distributed Computing Systems (ICDCS), 2018 and 2019.
- ACM Conference on Data and Applications Security and Privacy (CODASPY), 2018 and 2019.
- European Symposium on Research in Computer Security (ESORICS), 2017.
- ACM Asia Conference on Information, Computer & Communications Security (AsiaCCS), 2017.
- Transactions on Dependable and Secure Computing.
- Transactions on Services Computing.

SELECTED MEDIA

- **RWGuard:** Research Outreach
- **LTEInspector:** ACM Tech News, New York Times, Forbes, ZDNet