The University of Texas at San Antonio
UTSA Global Initiatives

Cyber Security Research at UTSA

Project Interest Form

Visiting TUDa PhD students will come to San Antonio in late August 2022 for a 3-month stay during UTSA's Fall semester (August-December) at UTSA. Each will be matched to Cybersecurity research projects spearheaded across different disciplines, institutes, and departments at UTSA, including Computer Science, Electrical and Computer Engineering, and Business Information Systems.

UTSA will cover program fees and basic living costs (housing, utilities, some meals) of participants who are nominated and matched to projects. Other associated costs (travel, insurance, visa fees, personal expenses, etc.) will be the responsibility of the participant.

Nominated students should submit:

1) This form, with basic information and departmental approval for nomination.
2) A short letter of interest, outlining scope of research and specific areas of expertise/interest.
3) A short letter of support/recommendation from research supervisor at TU Darmstadt.
4) A CV or resume.

Applicant Information

Last/Family Name:
First Name & Middle Name:

Indicate What Projects You're Interested In:

☐ New Security and Privacy Challenges in Modern Mobile and IoT Systems (Murtuza Jadliwala)
☐ Adversarial Attacks on Protein Folding Networks (Sumit Kumar Jha)
☐ Tools to Assist Communities in Developing Cybersecurity Programs (Greg B. White)
☐ Misinformation, Disinformation, and Malinformation in Cyber Operations (Greg B. White)
☐ Human-in-the-Loop XAI-enabled Vulnerability Detection, Investigation, and Mitigation (Kim-Kwang Raymond Choo)
☐ Automatic VR Testing with Deep Reinforcement Learning (Xiaoyin Wang)

☐ I would like to be considered for additional projects based on my application materials.

Project Interest Form, continued

Approval by International Relations and Mobility at TU Darmstadt

Name and Title: Julia Fitzthum, Head of unit Overseas
Department: International Relations and Mobility
Email: julia.fitzthum@tu-darmstadt.de

I herewith approve the applicant's participation in a Research Exchange with University of Texas at San Antonio. I understand that this program runs under the auspices of the Cooperation and Affiliation Agreements between our institutions. I understand that the participant will engage in full-time research, and not be enrolled for academic credit at UTSA.

______________________________	______________________________
Approver's Signature	Date (Month/day/year)

Applicant's Acknowledgement

By completing and signing this application, I understand that:

1. I am being considered for participation as a full-time visiting research scholar at University of Texas at San Antonio, with the expectation that, if selected, I will engage in full-time, in-person research in San Antonio for three months August – December 2022.

2. Participation as a full-time research exchange scholar is subject to terms of the Cooperation and Affiliation Agreements between Technische Universität Darmstadt and UTSA.

I certify that the information provided is correct and complete

______________________________	______________________________
Applicant Signature	Date (Month/day/year)

Please attach a letter of interest, letter of recommendation, and CV/resume to this application for consideration.

These materials will be collected by TU Darmstadt's International Office and forwarded to UTSA's Global Initiatives unit for project matching. Upon successful nomination and matching, candidates will need to submit additional materials for the visa process.

UTSA PROJECT #1

Full Name & Title of Project Lead (printed): Murtuza Jadliwala, Associate Professor

UTSA Department: Computer Science

Project Title: New Security and Privacy Challenges in Modern Mobile and IoT Systems.

Project Description:
Modern ubiquitous sensing and computing technologies such as smartphones, wearables, smart home systems and other Internet-of-Things (IoT) devices enable exciting new applications, but they also expose an additional threat surface which can be exploited to infer users' private information or to compromise their safety and (cyber) security. Continued progress in hardware, sensor and software (including, machine learning and cloud) technology have caused new threats to emerge which current access-control models and protection mechanisms are unable to address. This project's goal will be to discover and evaluate new security and privacy risks in modern ubiquitous sensing and computing environments comprising of functionally heterogeneous and isolated sensors and applications. Specifically, the newly exposed threats should show how different types of sensors on these devices can be employed by applications as information side-channels to leak sensitive user-information and how data sensed by some of these sensors can be surreptitiously modified to compromise (the functionality of) applications relying on it. Students can refer to the following publications to get an idea of the nature and scope of the problems to be solved in this project.

1. Soundarya Ramesh, Xiao Rui, Anindya Maiti, Jong Taek Lee, Harini Ramprasad, Ananda Kumar, Murtuza Jadliwala, Jun Han, "Acoustics to the Rescue: Physical Key Inference Attack Revisited", USENIX Security, 2021.
2. Mohd Sabra, Anindya Maiti, and Murtuza Jadliwala, "Zoom on the Keystrokes: Exploiting Video Calls for Keystroke Inference Attacks", NDSS, 2021.
3. Anindya Maiti, and Murtuza Jadliwala, "Light Ears: Information Leakage via Smart Lights", ACM IMWUT (UbiComp), 2019.

Ideal Qualifications for Applicants/Pre-requisite Skills:
This opportunity is for PhD students from TU Darmstadt. Please elaborate on specific skills, experience, or qualifications applicants should have in order to be matched to this project.

- Extremely strong systems and programming background is required. Experience with mobile programming environments such as Android, iOS, Unity is a plus.
- Prior experience in empirical evaluation of mobile and networked systems and collecting data from human subject participants would be very useful.
- Knowledge in statistical analysis tools and methodologies is also required.
- Finally, student should be extremely motivated to learn about new mobile and IoT systems and vulnerabilities. It is expected that project outcomes and results should be publishable in top-4 security/mobile computing venues (IEEE S&P, ACM CCS, NDSS, USENIX Security, ACM MobiSys, ACM MobiCom, ACM IMWUT, etc.)

UTSA PROJECT #2

Full Name & Title of Project Lead (printed): Sumit Kumar Jha, Professor

UTSA Department: Computer Science

Project Title: Adversarial Attacks on Protein Folding Networks

Project Description:

Protein folding networks like AlphaFold and RoseTTAFold promise solutions to a long-standing fundamental problem in biology: can we predict the structure of a protein from its sequence? In recent work, Jha and others have shown that RoseTTAFold is not robust to adversarial attacks. In this project, we will investigate if a low-resource protein analysis network suffers from adversarial robustness.

Deliverables: Code for adversarial attack on a low-resource biological neural network, adversarial examples on 100 protein sequences.

Ideal Qualifications for Applicants/Pre-requisite Skills:

The student should have excellent implementation skills. Pytorch, Python and past work in neural networks is required. High school knowledge of biology is needed.

UTSA PROJECT #3

Full Name & Title of Project Lead (printed): Greg B White, Professor

UTSA Department: Computer Science

Project Title: Tools to Assist Communities in Developing Cybersecurity Programs

Project Description:

1) Increasingly we are seeing cities and other municipalities targeted by cyberattacks. While state and national governments are developing some level of assistance, there simply are not enough resources at either of these levels to provide the needed support for communities. In a large-scale cyberattack, communities will be on their own for some period of time while attempting to maintain critical infrastructures. This is especially true for smaller, rural communities which frequently do not have any cybersecurity personnel and in some cases don't even have full-time IT personnel.
2) In the environment described, what documents and tools can be provided or created to help with community intrusion detection, information sharing, creation of needed policies and procedures, and training? How can a "Culture of Cybersecurity" be created in a community that can help maintain a level of cybersecurity across the community? What can be done in grades K-12 to encourage more interest in Cybersecurity to ensure the needed professionals are "in the pipeline"?

Ideal Qualifications for Applicants/Pre-requisite Skills: N/A

UTSA PROJECT #4

Full Name & Title of Project Lead (printed): Greg B. White, Professor

UTSA Department: Computer Science

Project Title: Misinformation, Disinformation, and Malinformation in Cyber Operations

Project Description:

1) Recent events (including the 2016 and 2020 presidential elections in the U.S.) have shown the problems that misinformation, disinformation, and malinformation in social media and news organizations can cause. A proper, coordinated cyber operation utilizing all three types of information could potentially have a significant impact and could possibly result in the election of a candidate the attackers prefer.
2) Research and development of plans for a coordinated cyber operation should be developed that could provide a taxonomy of attacks that could occur and what is involved in each. Research and tools are needed to be able to more readily identify all three types of information. Additionally, resources are needed to train the public to introduce a level of understanding of these types of operations and how to spot the different types of information.

Ideal Qualifications for Applicants/Pre-requisite Skills: N/A

UTSA PROJECT #5

Full Name & Title of Project Lead (printed): Kim-Kwang Raymond Choo, Professor and Cloud Technology Endowed Professorship

UTSA Department: Department of Information Systems and Cyber Security

Project Title: Human-in-the-Loop XAI-enabled Vulnerability Detection, Investigation, and Mitigation

Project Description:
In our proposed 'Human-in-the-Loop Explainable-AI-Enabled Vulnerability Detection, Investigation, and Mitigation' (HXAI-VDIM) system, instead of resolving complex scenario of security vulnerabilities as an output of an AI/ML model (e.g., a definitive outcome of yes or no, or a likelihood score for vulnerability degree), we integrate the security analyst or forensic investigator into the man-machine loop and leverage explainable AI (XAI) to combine AI and Intelligence Assistant (IA) in amplifying human intelligence in both proactive and reactive processes. Our ultimate goal is that the proposed HXAI-VDIM system will amplify the human intelligence in resolving and investigating complex security vulnerabilities. In other words, HXAI-VDIM integrates both human and machine in an interactive and iterative loop that utilizes human intelligence to guide the XAI-enabled system and generate refined outputs.

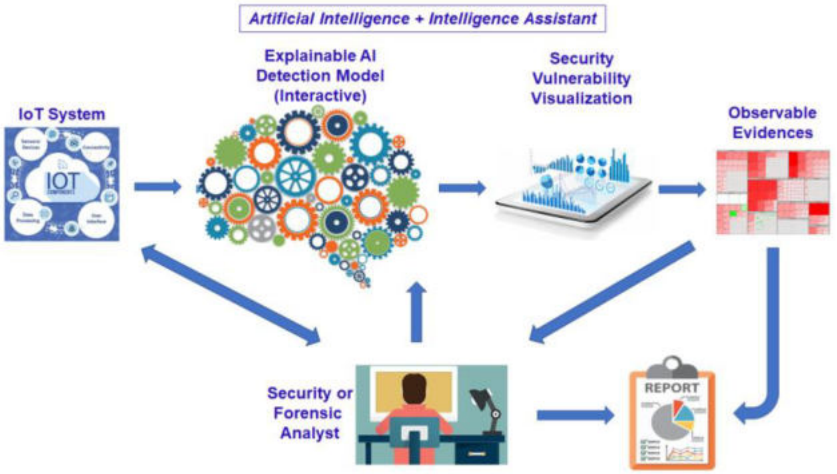
Artificial Intelligence + Intelligence Assistant
Explainable AI Detection Model (Interactive)
Security Vulnerability Visualization
IoT System
IOT
Observable Evidences
Security or Forensic Analyst
REPORT

Figure 1: Human-in-the-Loop XAI-enabled Vulnerability Detection, Investigation, and Mitigation[1]

Ideal Qualifications for Applicants/Pre-requisite Skills:

The applicant should ideally have the following skills: AI and security (more specifically, vulnerability detection in systems and/or source code).

[1] Tien N. Nguyen and Raymond Choo, "Human-in-the-Loop XAI-enabled Vulnerability Detection, Investigation, and Mitigation", in Proceedings of the 36th IEEE/ACM International Conference on Automated Software Engineering (IEEE/ACM ASE 2021), November 15-19, 2021. IEEE CS, 2021.

UTSA PROJECT #6

Full Name & Title of Project Lead (printed): Xiaoyin Wang, Associate Professor

UTSA Department: Computer Science

Project Title: Automatic VR Testing with Deep Reinforcement Learning

Project Description:
We are working on a project to perform automatic testing of VR scenes using deep reinforcement learning techniques. Our lab has developed VRTest, an automatic testing framework for experimenting various testing strategies. We have currently implemented various testing strategies including the random, greedy-algorithm-based, hot-area-based ones. We are currently developing a testing strategy based on deep reinforcement learning. In particular, a virtual avatar (agent) will be trained with data (bounding boxes, positions, and interaction patterns of virtual objects) from randomly created virtual scenes and evaluated on testing tasks of real-world VR projects. We will experiment with deep reinforcement algorithms such as Deep Q Learning, and various reward functions. We will also work on inverse reinforcement learning based on manual tests.

Ideal Qualifications for Applicants/Pre-requisite Skills: N/A