Title: Proactive Security Techniques for Social Engineering Attacks and More

Speaker: Prof. Rakesh Verma, University of Houston

Abstract:

Security, so far, has been largely a reactive ?eld wherein attackers expose new vulnerabilities, which are then patched by defenders. Another problem has been that the solutions have been to a large extent one-size-?ts-all. For example, in the case of spam, phishing and malware-containing emails, organizations have installed email ?lters, which are typically based on machine learning techniques. The problem with machine learning techniques is well-known. They work well when the instance in question is similar to the historical data on which they have been trained. Knowing this, the attackers constantly change the attack, so that the attacks escape the email ?lters. These new attacks, when they reach the inboxes of unsuspecting users, cause havoc, which periodically makes it into the news headlines, but most often is kept under wraps by companies worried about their reputations. This talk will discuss how to change the playing field. We take a multipronged approach that is proactive rather than reactive. We conclude with other cybersecurity topics being researched in the ReDAS Laboratory at the university of Houston.

Bio:

Rakesh Verma is currently a Visiting Professor at Shiv Nadar University at the invitation of Professor S. Sen, Director of SNU's School of Engineering. Rakesh is also a Professor of computer science with the University of Houston (UH), where he is leading a research group that applies reasoning and data science to cybersecurity challenges. He is the coauthor of Cybersecurity Analytics (Chapman and Hall/CRC Press, 2019), which discusses key data analysis techniques for cybersecurity challenges. He has co-organized the 1st Anti-phishing Shared Task, in 2018, with proceedings in the CEUR workshop series. Since 2015, he has been co-organizing and editing the proceedings of the ACM International Workshop on Security and Privacy Analytics. He is an Editor of Frontiers of Big Data in the Cybersecurity Area, an ACM Distinguished Speaker, from 2011 to 2018, and the winner of two Best Paper Awards. He received the 2013 Lifetime Mentoring Award from UH for involving undergraduates in research. He is a Fulbright Senior Specialist in computer science. He received his BTech. in Electronics & Communication Engg. from IIT (BHU) Varanasi, and his MS, PhD from SUNY Stony Brook in Computer Science.