Department of Mathematics and Computer Science

Friday, February 8, 2019, 4:10 pm

SPECIAL COLLOQUIUM TALK

Speaker: Ghaith Husari–University of North Carolina, Charlotte

Old Main 2210

TTP Mining Fom The Unstructured Text of Cyber Threat Intelligence

Abstract:

With the rapid growth of the cyber-attacks, the sharing of cyber threat intelligence (CTI) becomes essential to identify and respond to a cyber-attack in a timely and cost-effective manner. However, with the lack of standard languages and automated analytics of cyber threat information, analyzing the complex and unstructured text of CTI reports is extremely time- and labor-consuming. Without addressing this challenge, CTI sharing will be highly impractical, and attack uncertainty and time-to-defend will continue to increase. Considering the high volume and speed of CTI sharing, my research aims to develop automated and context-aware analytics of cyber threat intelligence to accurately learn attack pattern (TTPs) from commonly available CTI sources in order to timely implement cyber defense actions. My research has three key contributions. First, it presents a novel threat-action ontology that is sufficiently rich to understand the specifications and context of malicious actions. Second, I developed a novel text mining approach that combines enhanced techniques of Natural Language Processing (NLP), Information retrieval (IR), Word Embedding (WE) to extract threat actions based on semantic (rather than syntactic) relationship. Third, my approach?s CTI analysis can construct a complete attack pattern by mapping each threat action to the appropriate techniques, tactics and kill chain phases, and translating it any threat sharing standards, such as STIX 2.

SNACKS IN FACULTY LOUNGE AT 3:30 PM.
EVERYONE WELCOME (EVEN IF YOU ARE UNABLE TO ATTEND THE TALK)
MR. HUSARI IS A CANDIDATE FOR OUR COMPUTER SCIENCE POSITION