Announcing the Final Examination of Sharif Hassan for the degree of Doctor of Philosophy

Time & Location: March 27, 2019 at 11:00 AM in HEC 438
Title: Framework for Modeling Attacker Capabilities with Deception

In this research we built a custom experimental range using opensource emulated and custom pure honeypots designed to detect or capture attacker activity. The focus is to test the effectiveness of a deception in its ability to evade detection coupled with attacker skill levels. The range consists of three zones accessible via virtual private networking. The first zone houses varying configurations of opensource emulated honeypots, custom built pure honeypots, and real SSH servers. The second zone acts as a point of presence for attackers. The third zone is for administration and monitoring. Using the range, both a control and participant-based experiment were conducted.

We conducted control experiments to baseline and empirically explore honeypot detectability amongst other systems through adversarial testing. We executed a series of tests such as network service sweep, enumeration scanning, and finally manual execution. We also selected participants to serve as cyber attackers against the experiment range of varying skills having unique tactics, techniques and procedures in attempting to detect the honeypots.

We have concluded the experiments and performed data analysis. We measure the anticipated threat by presenting the Attacker Bias Perception Profile model. Using this model, each participant is ranked based on their overall threat classification and impact. This model is applied to the results of the participants which helps align the threat to likelihood and impact of a honeypot being detected. The results indicate the pure honeypots are significantly difficult to detect. Emulated honeypots are grouped in different categories based on the detection and skills of the attackers.

We developed a framework abstracting the deceptive process, the interaction with system elements, the use of intelligence, and the relationship with attackers. The framework is illustrated by our experiment case studies and the attacker actions, the effects on the system, and impact to the success.

Major: Computer Science

Educational Career:
Bachelor's of Management Information Systems, BS, 2000, University of Central Florida
Master's of Computer Science, MS, 2008, Florida Institute of Technology

Committee in Charge:
Ratan Guha, Chair, Computer Science
Mostafa Bassioune, Computer Science
Mainak Chatterjee, Computer Science
Ronald Demara, Electrical and Computer Engineering

Approved for distribution by Ratan Guha, Committee Chair, on March 10, 2018.

The public is welcome to attend.