Time & Location: March 29, 2019 at 1:30 PM in Engineering 2 202A
Title: Game-Theoretic Frameworks for Defense Against Network Jamming and Collocation Attacks

Networks are becoming increasingly more complex, heterogeneous, and densely connected. While more diverse services are enabled, several important challenges have emerged. For example, densely connected networks are prone to higher levels of interference. The increased reliance on cloud computing services poses formidable security challenges due to the shared nature and virtualization of cloud networks. This thesis studies two types of attacks: jamming attacks on wireless networks and side-channel attacks on cloud networks. The former attacks disrupt the network operation by exploiting the static topology in wireless networks, while the latter attacks seek to gain access to unauthorized data by co-residing with target virtual machines (VMs).

First, in the context of jamming attacks, we analyze a game-theoretic formulation between the adversary and the network defender. In this problem, the attack surface is the network connectivity (the static topology) as the adversary jams a subset of nodes to increase the level of interference in the network. On the other side, the defender continuously adapting the underlying network topology to reduce the impact of the attack. The defender's strategy is based on playing Nash equilibrium strategies securing a worst-case network utility.

In the second problem, we consider multi-tenant clouds, where a number of VMs are collocated on the same physical machine. This increases the risk of a malicious virtual machine performing side-channel attacks and leaking sensitive information from neighboring VMs. We analyze a timing game in which the cloud provider decides when to migrate a VM to a different physical machine to mitigate the risk of being compromised. The adversary decides the rate at which she launches new VMs to collocate with the victim VMs. We establish sufficient conditions for the existence of Nash equilibria for general cost functions, as well as for specific instantiations, and characterize the best response for both players.

Major: Electrical Engineering

Educational Career:
Bachelor's of Electrical Engineering, BS, 2011, Alexandria University
Master's of Wireless Communication and Information Technology, MS, 2013, Nile University

Committee in Charge:
George Atia, Chair, Electrical & Computer Engineering
Marwan Simaan, Electrical & Computer Engineering
Azadeh Vosoughi, Electrical & Computer Engineering
Gita Sukthankar, Computer Science
Mina Guirgis, Texas State University, Computer Science

Approved for distribution by George Atia, Committee Chair, on March 13, 2019.

The public is welcome to attend.