Title: Real-time IRC Threat Detection Framework

Speaker: Sicong Shao

Abstract: Most of the social media platforms generate a massive amount of raw data that is slow-paced. On the other hand, Internet Relay Chat (IRC) protocol, which has been extensively used by hacker community to discuss and share their knowledge, facilitates fast-paced and real-time text communications. Previous studies of malicious IRC behavior analysis were mostly either offline or batch processing. This results in a long response time for data collection, pre- processing, and threat detection. However, since the threats can use the latest vulnerabilities to exploit systems (e.g. zero- day attack) and which can spread fast using IRC channels. Current IRC channel monitoring techniques cannot provide the required fast detection and alerting. In this paper, we present an alternative approach to overcome this limitation by providing real-time and autonomic threat detection in IRC channels. We demonstrate the capabilities of our approach using as an example the shadow brokers' leak exploit (the exploit leveraged by WannaCry ransomware attack) that was captured and detected by our framework.