Writeup for the talks of Dr. Peng Gao 11/5

Submitted by: Provakar Mondal

Dr. Peng Gao is an Assistant Professor in the Department of Computer Science at Virginia Tech. He received his PhD in Electrical Engineering at Princeton University. His research interest lies in the fields of security, privacy, and systems.

In the seminar, Dr. Gao talked about **Building Trustworthy Systems for Fighting Modern Threats.** Desktop computers, laptops, smartphones, enterprise systems, social networks, blockchain he mentioned about complex computing systems. He provided statistics of the biggest data breaches of the 21st Century that cost 3.86 million and it took 207 days to identify.

Then Dr. Gao described the threats to security and privacy. Malware, Spam/phishing, Advanced persistent threats (APT) are threats to security. Unauthorized data access and Identify theft are threats to privacy. Dr. Gao visualized a hierarchy of his group's research including **Secure & Trustworthy Cyberspace, Defending Computing Systems, Making Computing Transparent, Securing Emerging Systems, Understanding Threat Landscape.**

Later he provided a flow diagram for Attack behind the data braches. He pointed out why APT is challenging. Guarding the border, e.g. firewall can be considered as Perimeter defense but too many security holes inside. Another challenge is the ocean of activities in modern enterprise systems due to the existence of **big data**. After that Dr. Gao talked about Transparent Computing through Ubiquitous System Auditing. Ubiquitous systems auditing monitors every host and monitors system activities through selective system call like file access, process creation, network access. He described **AIQL: Domain specific Query System for Efficient Attack Investigation.** The task associated with this technique are i) Attack investigation via iterative querying ii) A domain-specific query system.

He then pointed out the AIQL Query Execution Pipeline which includes Lexing/Parsing, Semantic Analysis, Query Rewriting, Query Planner: Compiling to Data Queries, and Data Query Scheduling. He also talked about DepImpact: High Fidelity Provenance Tracking. To make it more clear, he explained Backtracking on systems t answer how did something happen. DepImpact is intended to identify critical dependencies and attack entries. Furthermore, Dr. Gao talked about ThreatRaptor: Using threat intelligence for automated threat hunting which has rich knowledge about threats.

In the seminar, Dr. Gao described Sources of Open Source Cyber Threat Intelligence (OSCTI) also. It has some limitations as its primary focus is on isolated, low-level indicators. It also ignores higher-level concepts and ignores relationships. Dr. Gao then mentioned SecurityKG which is an automated high-fidelity OSCTI gathering and management. It is an ai powered security knowledge graph. De. Gao presented his group's current research projects consisting of Threat Intelligence, Threat Protection, Blockchain, and Programmable networks+security.

The seminar conducted by Dr. Gao was very nice and informative. He described many topics regarding security and privacy and enriched our knowledge about these fields. He also mentioned at the end of the seminar that he has openings for PhD, Masters, and Undergraduate research and suggested interested ones apply.