CSC 6222：Project Assignment

Due on 12/3/2018, 12:30pm

The goal of the project is to study the emerging research problems related to Cyber Security through exploring new research ideas/solutions/directions. All the submitted materials such as the abstract and report must use word or latex following the IEEE template (single space, 11 pt font size, https://www.ieee.org/conferences/publishing/templates.html). No copy and paste are allowed in the report. A student can work on this individually or team up with another graduate student to carry out the course project. You will be responsible for completing the work if some members drop the class.

Option 1: A Survey of Cyber Security Techniques

Project Background: Today, the constant progress of IT infrastructure connectivity and the unending innovations in digital technologies make systems more and more complex. As a system gets more complex, it gets less secure. This complication in digital systems has led to a change in the cyber-attacks forms, functions, and sophistications from just a few years ago targeting individual end users, businesses and government agencies.

Requirement for this Project:

1. Students need to complete a survey towards the state-of-art cyber attacks/defense techniques. The survey needs to contain following sections: 1) **Introduction**, 2) **Background**, 3) **Related Work**, 4) **3 Specific topics about the cyber security** (e.g., Cyber Security in smart grid, technical threat intelligence and so on.), 5) **Discussion** (e.g., A discussion about several comparisons between the state-of-art techniques with the traditional methods) and 6) **Conclusion**.
2. Other than the aforementioned sections, the survey needs to have **at least 9 pages** without counting the references. Students need to describe the major idea of each paper **in their own words instead of copying sentences or paragraphs** from the original paper or other surveys.
3. In the final presentation, each student in the team needs to report one state-of-art technique. **At least one student needs to give a demo of a state-of-art technique in the presentation.**

Option 2: Cyber Security Defense Strategy in Smart Grid (Network Security)

Project Background: Smart grid uses the power of information technology to intelligently deliver energy by using a two-way communication and wisely meet the environmental requirements by facilitating the integration of green technologies. The inherent weakness of communication technology has exposed the system to numerous security threats.

Requirement for this Project:

1. Students need to firstly figure out the **attack strategies** in the Smart Grid (e.g., Man-in-the-middle, Denial of Service and so on). According to each attack strategy, students need to find **the corresponding defense strategy** and analyze the pros and cons of the defense strategy.
2. Students need to **improve** the defense strategy based on the proposed cons of that defense strategy and **implement** **three strategies** to make comparisons of the improved version with the original version.
3. Report needs to be more than 6 pages and described **in own words instead of copying sentences or paragraphs** from the existing papers.

Reference: El Mrabet, Z., Kaabouch, N., El Ghazi, H., & El Ghazi, H. (2018). Cyber-security in smart grid: Survey and challenges. Computers & Electrical Engineering, 67, 469-482.

Option 3: Machine Learning (ML) and Data Mining (DM) Methods for Cyber Security Intrusion Detection (Machine Learning & Data Mining)

Project Background: Cyber security is the set of technologies and processes designed to protect computers, networks, programs, and data from attack, unauthorized access, change, or destruction. Cyber security systems are composed of network security systems and computer (host) security systems. Each of these has, at a minimum, a firewall, antivirus software, and an intrusion detection system (IDS). IDSs help discover, determine, and identify unauthorized use, duplication, alteration, and destruction of information systems.

There are three major types of cyber analytics in support of IDSs: misuse-based (also known as signature-based), anomaly-based and hybrid-based methods.

Misuse-based methods: detect known attacks by using signatures of those attacks

Anomaly-based techniques: model the normal network and system behavior and identify anomalies as deviations from normal behavior.

Hybrid techniques: combine misuse and anomaly detection.

An in-depth review of the literature did not discover many pure anomaly detection methods; most of the methods were really hybrid. Therefore, in the descriptions of ML and DM methods, the anomaly detection and hybrid methods are described together.

Requirement for this Project:

1. Students firstly need to figure out the applications of the **aforementioned three cyber analytics** supporting the IDSs. Then, students need to investigate which **DM or ML techniques** (e.g., decision tree, Bayesian network and so on) can be applied to realize the detection of intrusion in cyber security.
2. The final project needs to be at least 6 pages and described **in own words instead of copying sentences or paragraphs** from the existing papers.
3. Also, the report needs to include necessary descriptions towards how to create such a DM/ML based detection for intrusion in cyber security (**application-oriented**).
4. At least **one simulation of the DM/ML based method** should be implemented and demoed in the final presentation.

Reference: A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," in IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153-1176, Secondquarter 2016.

Option 4: Cyber Cloud Security (Cloud Computing)

Project Background: Cyber space is affecting all areas of our life. Cloud computing is the cutting-edge technology of this cyber space and has established itself as one of the most important resources sharing technologies for future on-demand services and infrastructures that support Internet of Things (IOTs), big data platforms and software-defined systems/services. More than ever, security is vital for cloud environment. There exist several cloud security models and standards dealing with emerging cloud security threats. However, these models are mostly reactive rather than proactive and they do not provide adequate measures to assess the overall security status of a cloud system.

Requirement for this Project:

1. Students firstly need to investigate the **concepts of the cyber cloud security** and **the weaknesses of traditional cloud security models**. It's better to understand the **cyber security metrics** before going to next step.
2. Then, students need to conclude the reasons causing those weaknesses and also propose novel models to overcome current weaknesses.
3. The final project needs to be at least 6 pages and described **in own words instead of copying sentences or paragraphs** from the existing papers.
4. At least one model needs to be simulated and demoed in the presentation.

Reference: Le, N. T., & Hoang, D. B. (2017). Capability Maturity Model and Metrics Framework for Cyber Cloud Security. Scalable Computing: Practice and Experience, 18(4), 277-290.

Option 5: Cyber Security in Internet of Things (IoT & Cyber-Physical System)

Project Background: In recent years, we have witnessed an exponential growth in the development and deployment of various types of cyber-physical systems (CPSs). They have brought impacts to almost all aspects of our daily life, for instance, in electrical power grids, oil and natural gas distribution, transportation systems, health-care devices, household appliances, and many more. Many of such systems are deployed in the critical infrastructure (CI), life support devices, or are essential to our daily lives. Therefore, they are expected to be free of vulnerabilities and immune to all types of attacks, which, unfortunately, is practically impossible for all real-world systems.

CPS are composed of various components in many ways. There are different hardware components such as sensors, actuators, and embedded systems. There are also different collections of software products, proprietary and commercial, for control and monitoring. As a result, every component, as well as their integration, can be a contributing factor to a CPS attack.

Requirement for this Project:

1. Students firstly need to investigate **the weakness of the CPS or IoT in security aspect**. With the understanding of the weakness of the security for CPS or IoT, students need to figure out the CPS/IoT security threats. Besides, students also need to understand the traditional strategies towards some security threats.
2. Then, students need to **provide improved strategies** to solve the remaining problems in the traditional strategies and simulate the proposed strategies.
3. The final project needs to be at least 6 pages and described **in own words instead of copying sentences or paragraphs** from the existing papers.
4. At least one model needs to be simulated and demoed in the presentation.

Reference:

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal*, *4*(6), 1802-1831.