|  |  |
| --- | --- |
| **Presenter** | **Terence Leong** |
| **Title** | **Classification and quantification of Security Attack and Defences** |
|  |  |
| **Abstract** | In recent decades, modern vehicles have been rapidly increasing their number of in-vehicle electronic devices and ever-increasing complexity of in-vehicle systems. Therefore, it has been imperative to rely upon external network systems for efficient communication services. However, this development in technology has exposed them to new types of internal and external threats. As a result, cyber security has become one of the most significant challenges in connected vehicular systems. One of the most vulnerable of which is the electronic controller units (ECUs), which allows vehicle components to communicate with each other via a controller area network (CAN) serial bus.  Researchers, have tackled the problems present from many angles, resulting in a variety of solutions for a large number of vulnerabilities. Despite that, the attacks and defences present have not been compiled and quantified in such a way that would provide a greater insight for taking the next step in vehicular security. For that purpose, this thesis focuses on researching widely abused vulnerabilities that targets the ECU and existing methods to counter them. In addition, suggestions were made to systematically quantify these attacks and defences through existing security metrics. This method quantifies security risk based on methods of performing attack (ie. Attack restriction, attack preconditions) and affected component (ie. Consequence on them, acquired privileges). The idea is to present a method of capturing the relationship between attack and defence, whilst providing a greater insight into potential cost benefits. Finally, I present the above and describe my approach via a set of potential attacks independent of each other. |
| **Degree** | Master of Professional Engineering (Software) |
| **Supervisor** | Dr. Jin Hong, School of Engineering and Mathematical Science |
| **Work Experience** | - |