Smart Binary-level Vulnerability Assessment for Cyber-attack Prevention (Cybersecurity, by A/P Liu Yang)

The concept of vulnerability refers to a weakness in a binary executable, which allows an attacker to compromise a system’s information assurance. Specifically, a vulnerability is an exploitable bug in the software and/or hardware components of an IT system. Vulnerabilities are difficult to detect and can cause severe damage if exploited, making them a significant security threat for IT infrastructure and systems. In an era where cities and nations are transitioning into ‘smart cities’ and ‘smart nations’, multiple systems are integrated into an increasingly complex IT infrastructure that creates a holistic, smart-city system. As can be envisioned, the vulnerability of a single component or sub-system can endanger the whole system. For example, the vulnerability of WIFI routers of the subway system may give attackers access or the internal networking and endanger the whole controlling system. In addition, for those smart device like smart TV has been reported to contain vulnerability that allows the remote attackers to surveillance the watchers (the smart TV is also watching you). Even for today’s pilotless automobile, the autodriving and auto-navigation system may contain vulnerability and endanger the passengers. As in normal daily life, cell phone may explode due to the vulnerability. Previously, researchers have exploited the vulnerability of iOS and remotely controlled the battery statues, which can make iPhone as a weapon of explosive.

Hence, to effectively protect the IT infrastructure and related systems, there exists the need for a vulnerability detection and analysis framework that is platform agnostic, efficient and minimizes the amount of manual intervention required. The objective of this project is to develop such a framework which detects unknown vulnerabilities (and its causes) in any given binary executable in a time-bound manner.