Cyber–Physical Security of a Smart Grid Infrastructure

Name: Viraj Kamat **SBU-ID:** 112818603

The electric grid being a vital piece of infrastructure to human beings is being designed to be “smart”. The electrical grids today incorporate electrical power from renewable sources and from fossil fuels. The generation of power from renewable sources is varying and as a result the output of power generated changes. With the use of complex energy prediction algorithms (energy from renewable sources) and predictive analysis we now know the power output available from power generation units at different timesteps in the future. Since power-generation is variable and so is their pricing, we need to employ smart methods to let consumers be aware of energy pricing at different times. This will enable consumers to manage how appliances use this energy at different times to keep the electricity bill low. This could also benefit power generation companies as load demand could be reduced and the need for expensive power generation units required during peak load times will be unnecessary. This requires a complex smart infrastructure that would relay electrical pricing information to consumers on a smart electrical grid network using smart metering systems. However, it also leaves this electrical grid network vulnerable to both physical attacks on the systems and cyber-attacks on the electrical network.

In smart-energy grid system two types of vulnerabilities originate – physical & cyber. Since electrical metering devices are connected over a network using traditional TCP/IP protocol they can be hacked and metering data within them be accessed, which can yield usage activities in home. D.O.S attacks can also be carried out over the network that would render the systems incapacitated. Likewise, the system that enables transmission of electrical pricing data can be physically compromised as well; metering systems, power delivery units, etc can be physically altered for reasons such as pranks to outright terrorism. Multiple entry points exist with which the systems can be compromised either through physical or non-physical means (cyber/software or hardware). It is then imperative that a smart electrical grid be both physically and cyber secure. In the case of addressing cyber based vulnerabilities we can use shared-keys for encrypted traffic, use a robust network architecture impermeable to attacks or use code-attestation techniques that verify the metering data is indeed transmitted from an un-compromised software on the system. In the case of addressing physical vulnerabilities we can check if the system is operating in the expected range and detect abnormalities or changes (via attacks) so that we could take action to mitigate the effects.

One attack that involved corrupting system measurements was a malware named Stuxnet that deployed onto computer systems at a Nuclear Facility in Iran and played black pre-recorded measurements in real time to centrifuges thus damaging them – this sort of an attack is known as “Replay attack”. In order to prevent this, we could develop a system with an estimator, controller and a detector which could allow a system to detect replay attacks as measurements with high probability. Similarly, we can also have tamper resistant secure devices such that the sensors can detect corrupted measurements. Thus, we employ both system theoretic secure models and cyber-secure models in order to protect the system overall in a hybrid approach. We thus conclude that cyber–physical system security demands additional security requirements, such as continuity of power delivery and accuracy of dynamic pricing, introduced by the physical system. Therefore, both information security and system-theory-based security are essential to securing cyber–physical systems.