The Evolution of Cyber Security with the Emergence of Internet of Things

Sanjay Goel

University at Albany, State University of New York

The Internet of Things (IoT) is definitely here. There will be 200 million IoT devices by 2020. The range of possible benefits of IoT is expanding with greater efficiency, streamlined processes, and reduced costs being top benefits realized by all manner of business enterprises as adoption increases. Imagine for a moment smart farming, and the advances in production and prediction that will be realized when sensors can deliver fine-tuned information about temperatures and humidity, soil ph and nutrient levels, to streamline farming practices and increase crop yields. Or the remarkable potential in medicine and biomedical informatics…of insulin pumps that can monitor blood sugar levels and adjust insulin levels in real-time, or IBM's Medical Sieve, which, driven by smart algorithms and advanced AI sorts through a patient's complete medical history, looking for clues to inform its analysis of the patient's images; learning everything there is to know about the individual in seconds for a smarter diagnosis and an infinitely more personal treatment plan. Imagine recapturing the time you currently spend fighting traffic on your daily commute, for reading or even daydreaming, in your self-driving vehicle. We are working on a project at UAlbany where traffic signals can communicate with each other, making adjustments to increase traffic flow. Imagine sensors that can predict earthquakes before they happen; and the improvements that could be made with greater real-time energy consumption and environmental performance monitoring.

With this unlimited promise comes tremendous risk in terms of security and privacy losses, system breaches and hacking. When critical infrastructure like power stations, water supplies, airports, and hospitals are governed by IoT systems, the potential for loss of life—from failures and cybercriminal activity--rises exponentially. Securing the Internet of Things is no simple task. It is not a matter of 'redoubling our current security efforts," because IoT systems do not have well-defined perimeters, are highly dynamic, and with mobility, continuously change. Traditional "host–centric" and perimeter-based security approaches (antivirus, software patches, firewalls) are fundamentally at odds with IoT realities, with multiple devices and vendors and great variation in security practices. This talk discusses the challenges in IoT security and how the security paradigm is evolving to suit the IoT world.