Revere Security Abstract for

CETA Workshop on Cryptography for Emerging Technologies and Applications

Recent advancements in ASIC circuitry and low power memory have produced a plethora of devices in RFID systems, remote sensors, mesh networks, advanced industrial control systems, smart cards and many more. Operating on the "edge" of the internet, these devices enable unprecedented improvements in secure access, supply chain management, weapons tracking and monitoring, remote sensing and other force management/intelligence gathering capabilities. Micro-processor applications are also growing in commercial markets. Over the next decade, billions of devices to will be installed in power grids, houses, buildings and factories to monitor and control critical flows, pressures, temperatures, household events and numerous other functions in our critical infrastructure.

Unfortunately these devices are vulnerable to malicious attacks that compromise operations and threaten networks. Robust security is essential to safeguard enterprises and protect individual privacy. However, because of the limited speed, power and code-space of the devices, the burdensome overhead of encryption complicates security implementations.

Revere Security is developing light weight encryption algorithms to address this problem. Our Chief Cryptographer, Dr. Whitfield Diffie, will discuss recent advancements in symmetric and asymmetric algorithms that are designed for these "low resource" devices. Dr. Daniel Engels, our CTO, will discuss our efforts to integrate these ciphers into communication security systems.