Popular summary in English

Connected digital computing devices have spread to virtually all aspects of society. As of 2021, there are more connected *things*, i.e. small computers, on the internet than people. These small computers power a wide variety of things in our society, from household appliances and vehicles, to power plants. One important sector that is becoming increasingly connected to the internet is manufacturing.

Industry 4.0, for example, predicts and outlines a more flexible future of manufacturing. Smaller series of custom products can be produced efficiently with distributed connected control systems without requiring complex and time-consuming retooling. Such trends in manufacturing point to a more connected, decentralized, and *agile* future.

The future of connected devices is scale and decentralization. Since devices are deployed at scale, they must be cheap to manufacture, deploy, and run. Wireless and battery-powered devices can decrease the cost of installation by 30-60%. Many of the devices being added to networks today are *constrained devices*, that is, devices with limited computational power, memory, and network bandwidth. Many constrained devices are also battery-powered and need to preserve energy.

Often the public is only made aware that a device is connected when a cyber attack is disrupting that device's operation. The move from connected computers, servers, and networking equipment to connected Smart Manufacturing, Smart Grid, and other cyber-physical systems has moved the risks of cyber attacks from loss of capability and data to the risk of physical harm, loss of property or even life. Technologies exist that mitigate the risk of connected IT infrastructures. These technologies might not, however, be suited to deployment in connected constrained devices. The limited performance of the constrained device can make such technologies too resource-intensive to be feasible. The number of sensors and actuators in a factory or a wireless sensor network can be thousands of devices. Solutions must be able to handle a large number of deployed devices. This thesis addresses the lack of efficient security protocols for new decentralized connected systems.

We have studied the efficiency of the protocols OSCORE and Group OSCORE. These protocols have been proposed to enable secure communication for constrained devices with untrusted intermediaries. We show that the protocols can be implemented efficiently, and that they are suitable for use in constrained connected devices.

Next, we used formal verification to evaluate the security properties of the WirelessHART protocol. WirelessHART has been adopted and deployed for industrial control systems. We have found that WirelessHART is secure as long as no device in a network is compromised. Furthermore, we found that a single compromised device can be used to cause further damage to a WirelessHART network. This analysis can inform WirelessHART users of the security properties of the protocol.

Furthermore, we have studied how the concept of Digital Twins can be used to create a security architecture for industrial control systems. A Digital Twin can be seen as a digital replica of a physical entity.

Next, we identified the problem of *ownership transfer* for constrained connected devices. We have designed and evaluated a protocol that enable one owner of a constrained-device network to transfer the network to another entity. This can allow a network of constrained devices to be shared between operators, without anyone having to reprogram each device that can be inaccessible.

Finally, we have proposed a novel protocol for privacy-preserving data collection and analytics. Our proposed protocol allows values, such as measurements, to be sent encrypted to an aggregator. The aggregator can then compute the sum of the encrypted values, learning the sum, but not the individual values. Our protocol allow measurements while preserving privacy.

The main finding of this thesis is that it is possible to implement and deploy secure and efficient protocols in the setting of constrained devices.