CYBERSECURITY
RESEARCH LAB

CRL 101 Series

IoT Security and Privacy Gaps

By Annegret Henninger & Dr. Atefeh Mashatan

The internet-of-things (IoTs), dubbed industry 4.0, allows us to connect everyday objects which communicate with each other autonomously. This global network of smart devices provides us with ubiquitous computing. The IoT revolution is characterized by two distinct factors, the fast growing size and density of IoT networks, and shrinking size of the connected devices. While the devices are getting smaller and smaller, the development, adoption and range of use cases for smart devices is growing steadily with tens of millions of IoT devices already in existence. These two characteristics are desirable to consumers and producers of smart devices, but are also the primary points of weakness in the security and privacy of the IoT implementations.

The IoT is spread across core networks which are each made up of smart objects and embedded systems, which consist of sensors and actuators (devices which cause other machines to operate). Sensors often collect privacy sensitive information (data). As technologies improve, the devices become 'smarter' and proceed to carry even more privacy sensitive information about us. These end points of receiving and transmitting information are the most vulnerable part of an IoT. Consequently, they are attractive targets to attackers for gaining unauthorized access.

Secure communication largely relies on classical cryptographic protocols to transmit information between devices. User authentication as well as message authentication and integrity are typically achieved through the use of standardized cryptographic algorithms and the management of cryptographic keys and credentials. Most implementations heavily rely on asymmetric-key cryptography and is managed with public key infrastructure (PKI).

This becomes an issue with the miniaturization of smart devices. Asymmetric-key cryptography used in secure communication is computationally expensive and not scalable for many IoT use cases. As smart devices get smaller and more convenient, the miniature devices cannot support the complex algorithms used in asymmetric-key cryptography and thus resort to lightweight alternatives which are not adequately secure. New protocols that provide adequate security, but which are also lightweight enough to be used for the small IoT sensors need to be developed. At the CRL, we are developing effective solutions for IoTs that meet post-quantum privacy and security specifications, without burdening devices with unnecessary security measures which increase costs and reduce efficiency and applicability.

There is also a security issue related to the increasing size and density of IoT core networks. With IoTs covering an increasingly vast array of use cases, the data handled by smart devices widely varies in its level of sensitivity. There is also an increase in range with regards to the required hardware and software capabilities to meet the different technology needs. For example, a smart phone handles more sensitive data and can support more robust security mechanisms than

a wearable fitness monitor. The multi-part communication and cryptographic protocols suffer from an increasing number of cyber-attacks, and every sensor in the IoT network represents a risk. Therefore, one challenge is that there is no one-size-fits-all security solution. Furthermore, it is important to remember that the devices are linked on a network, and thus a weak sensor can pose a risk to the data stored elsewhere in the system. The CRL is examining ways to design multitiered solutions that can be applied to the complex architecture of the IoT network.

Another security issue lies in the network architecture. The network architecture for IoTs is a standard centralized architecture. This presents a single point of failure making the system vulnerable to a denial of service attack, which is a risk to information availability. Using blockchain in IoT devices would help with decentralizing the IoT network.

As with all computing, the longevity of security mechanisms, and length of time that the data is valuable, needs to be considered. IoT devices are typically deployed with a useful-life expectancy of over ten years, and store information that is intended to stay confidential for decades. Those devices that do use asymmetric-key schemes, they are still at risk. Quantum computing poses a serious threat whereby the asymmetric-key encryption could be broken during the valuable lifespan of the data. While existing quantum resistant algorithms are being reviewed and tested, they have not yet been standardized and are definitely not light-weight enough for many IoT use cases. More efficient quantum cryptographic protocols are needed for protecting against the quantum threat. At the CRL, we are developing classical/quantum hybrid solutions for present use, which can both protect against quantum attacks, and maintain current security guarantees.

July 22, 2019
CRL 101 Series

The CRL 101 series is a knowledge transfer project designed to give readers an overview of trending security-related technologies that we are working on at the Cybersecurity Research Lab.