Chapter 5
Hardware Primitives-Based Security Protocols for the Internet of Things

Muhammad Naveed Aman
National University of Singapore, Singapore

Kee Chaing Chua
National University of Singapore, Singapore

Biplab Sikdar
National University of Singapore, Singapore

ABSTRACT

IoT is the enabling technology for a variety of new exciting services in a wide range of application areas including environmental monitoring, healthcare systems, energy management, transportation, and home and commercial automation. However, the low-cost and straightforward nature of IoT devices producing vast amounts of sensitive data raises many security concerns. Among the cyber threats, hardware-level threats are especially crucial for IoT systems. In particular, IoT devices are not physically protected and can easily be captured by an adversary to launch physical and side-channel attacks. This chapter introduces security protocols for IoT devices based on hardware security primitives called physically unclonable functions (PUFs). The protocols are discussed for the following major security principles: authentication and confidentiality, data provenance, and anonymity. The security analysis shows that security protocols based on hardware security primitives are not only secure against network-level threats but are also resilient against physical and side-channel attacks.

DOI: 10.4018/978-1-5225-5742-5.ch005

INTRODUCTION

The Internet of Things can be included in the list of the most important emerging technologies of the present era. The number of new things or devices being added to the system every day is over five million. The number of IoT devices connected to the Internet in 2016 crossed six billion (Gartner, 2015) and is expected to reach over 20 billion by 2020 (Intel). This considerable number of connected objects presents an excellent opportunity for the use of an extended knowledge base, e.g., healthcare, industrial control, smart cities, transportation systems, and the smart power grid. However, IoT security and privacy are deemed to be the most critical and essential aspect that has to be addressed for the future growth of IoT. A survey report released by HP shows that IoT enabled devices suffer from at least 25 security flaws (HP, 2014).

Virtually any device that is connected to the Internet or other devices poses a threat to the user. For example, an attacker may try to sabotage equipment or even cause human injuries by gaining unauthorized access to the IoT devices monitoring and controlling the manufacturing equipment in a factory. Wearable IoT devices are used to monitor patients, collect vital health data, and wirelessly convey this data to health professionals to make treatment decisions. An attacker may try to eavesdrop or even change this data resulting in wrong treatment. Similarly, IoT sensors onboard vehicles may monitor the engine temperature, and the condition of transmission fluid, brakes, and tire pressure, etc. Moreover, the use of driving aid systems such as ESC (electronic stability control) and ACC (adaptive cruise control) allow even greater control to electronic components. In this case, it is essential to isolate the vehicle's automotive control network from an IoT connected navigation or multimedia system to minimize the risk of cyber-attacks.

Some of the high-profile cases from the hacking of IoT devices include the following. A passenger onboard a commercial airline flight allegedly gained access to the jet's thrust management system by connecting through the in-flight entertainment (IFE) systems (Moyer, 2015). Similarly, two security researchers successfully hacked into a jeep mile away and were able to interfere with the vehicle's entertainment system, engine, and brakes (Greenberg, 2015). In another incident in Germany, attackers used a spear-phishing attack to gain access to a steel mill's control system through the plant's business network causing significant damage (Zetter, 2015). In another high-profile incident in Ukraine in December 2015, attackers were successful in gaining access to the power grid and cutting power to over 200,000 people (Zetter, 2016). Realizing the risk of cyber-attacks on devices in IoT, the US security agency had disabled the wireless capabilities of the monitoring and smart apparatus of his embedded medical device when the former vice president of USA Mr. Dick Cheney was hospitalized (Grau, 2015). These are