SIES Graduate School of Technology
RISE WITH EDUCATION

Techscience
IT Magazine

Editors
Ms. Seema Redekar
Ms. Stuti Ahuja

DEPARTMENT OF IT Jan – June 2017

Security in the Internet of Things:

The Internet of Things (IoT) is envisioned to grow rapidly due the proliferation of communication technology, the availability of the devices, and computational systems. Hence, IoT security is an area of concern in order to safeguard the hardware and the networks in the IoT system. However, since the idea of networking appliances is still relatively new, security has not been considered in the production of these appliances.

Some examples of existing IoT systems are self-driving vehicles (SDV) for automated vehicular systems, microgrids for distributed energy resources systems, and Smart City Drones for surveillance systems. A microgrid system represents a good example of a cyber-physical system: it links all distributed energy resources (DER) together to provide a comprehensive energy solution for a local geographical region. However, a microgrid IoT system still relies on traditional Supervisory Control and Data Acquisition (SCADA). The integration of the physical and cyber domains actually increases the exposure to attacks: cyber attacks may target the SCADA supervisory control and paralyse the physical domain or the physical devices may be tampered or compromised, affecting the supervisory control system. On the other hand, the drone market is moving quickly to adopt automation techniques and can be integrated into fire fighting, police, smart city surveillance, and emergency response. As municipalities and citizens begin to rely on such a system, it will become critical to keep the system secure and reliable.

In recent years, it has been observed that academic research to address the privacy and security issues for IoT systems has attained positive developments. Currently, the techniques and security methods which have been proposed are essentially based on conventional network security methods. However, applying security mechanisms in an IoT system is more challenging than with a traditional network, due to the heterogeneity of the devices and protocols as well as the scale or the number of nodes in the system. The challenges in applying IoT security mitigation which are due to physical coupling, heterogeneity, resource constraints, privacy, the large scale, trust management and unpreparedness for security are extensively explained in .

The surveys evaluate the possible threats to IoT systems according to the layers and the available countermeasures. Kouicem et al. stated that in recent years, there has been a lot of research to address issues such as key management, confidentiality, integrity, privacy, and policy enforcement for IoT systems, hence suggested traditional cryptography methods and new technologies such as Software Defined Network (SDN) and Blockchain to be implemented to solve current IoT security issues.

One of the key enablers of the rapid progress of academic IoT security research is the availability of a tool for IoT or sensor network simulation and modelling. A comprehensive list of the simulators used in current research is presented by Chernyshev et al. . An open source network simulator, such as NS 3, is the most used simulator for IoT security research. However, since many new security protocols are being proposed, there is an urgent need for a security protocol evaluator, such as Automated Validation of Internet Security Protocols and Applications, AVISPA.

Challenges in applying security mechanisms in IoT and its attack vectors will also be evaluated. Simulators or IoT modellers that may be used by new researchers to further develop the IoT security field will be highlighted. The credibility of the published work surveyed here has been ensured by using the reputable Web of Knowledge search engine by using the keyword “IoT security simulation” . The contribution of is highlighted by comparing several aspects of other surveys, such as techniques for IoT security mechanisms, simulation tools, and current research. Table 1 compares the present survey with the other surveys in IoT security published from 2017 to 2018. As compared to these other surveys, the present survey presents findings on the current IoT security mechanisms, including authentication, encryption, trust management, secure routing protocols, and new technologies applied to IoT security, along with the related tools and simulators involved in the research.

Due to the diversity of the devices and multitude of communication protocols in an IoT systems, and also various interfaces and services offered, it is not suitable to implement security mitigation based on the traditional IT network solutions. In fact, the current security measures which are applied in a conventional network may not be sufficient. Attack vectors as listed by Open Web Application Security Project (OWASP) concern the three layers of an IoT system, which are hardware, communication link and interfaces/services. Hence, the implementation of IoT security mitigation should encompass the security architecture at all IoT layers, as presented in Fig. 1. Radio Frequency Identification (RFID) and Wireless Sensor Network (WSN) are considered as part of an IoT network. Thus, possible attacks on these two systems are presented in Table .

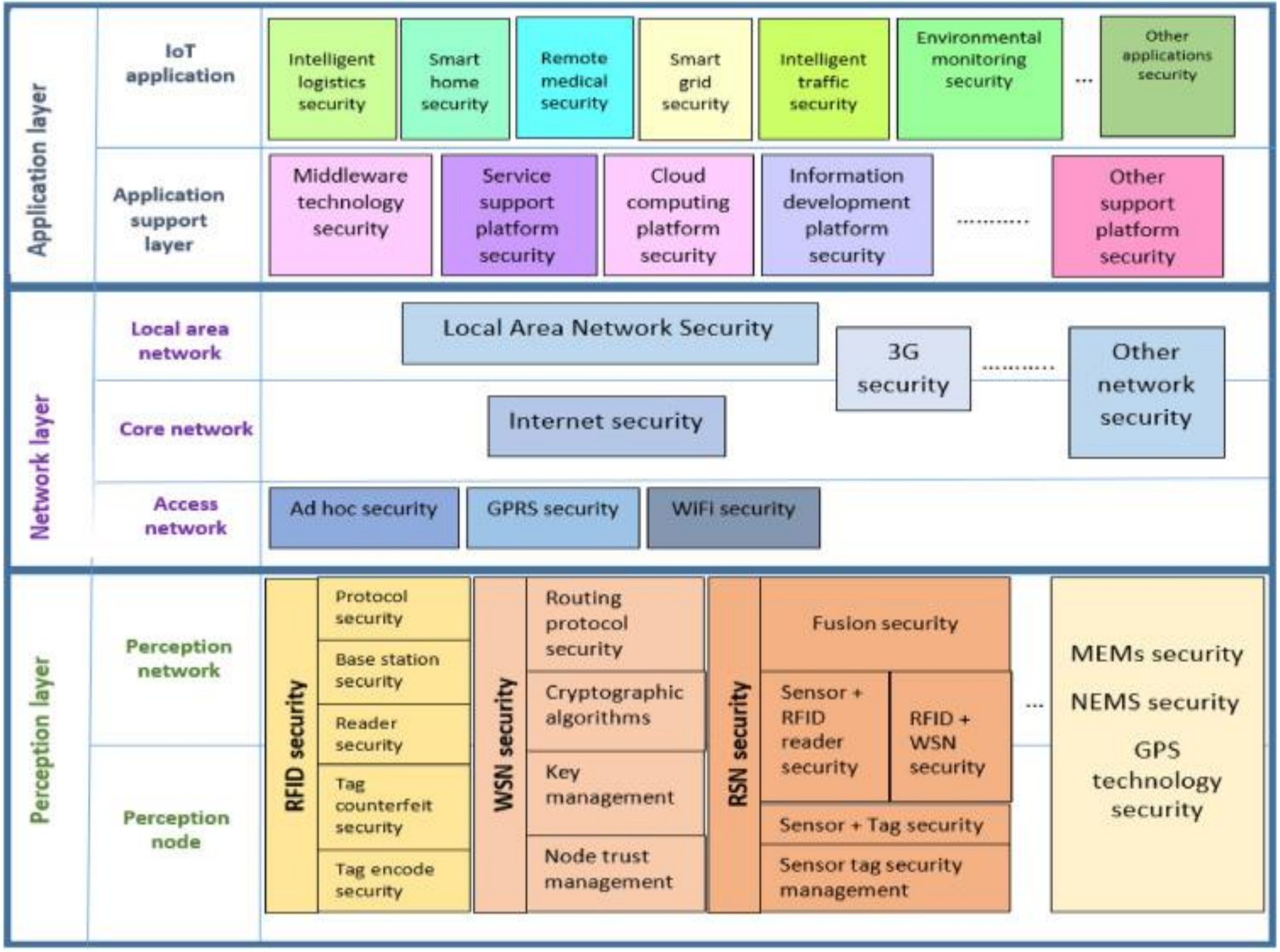
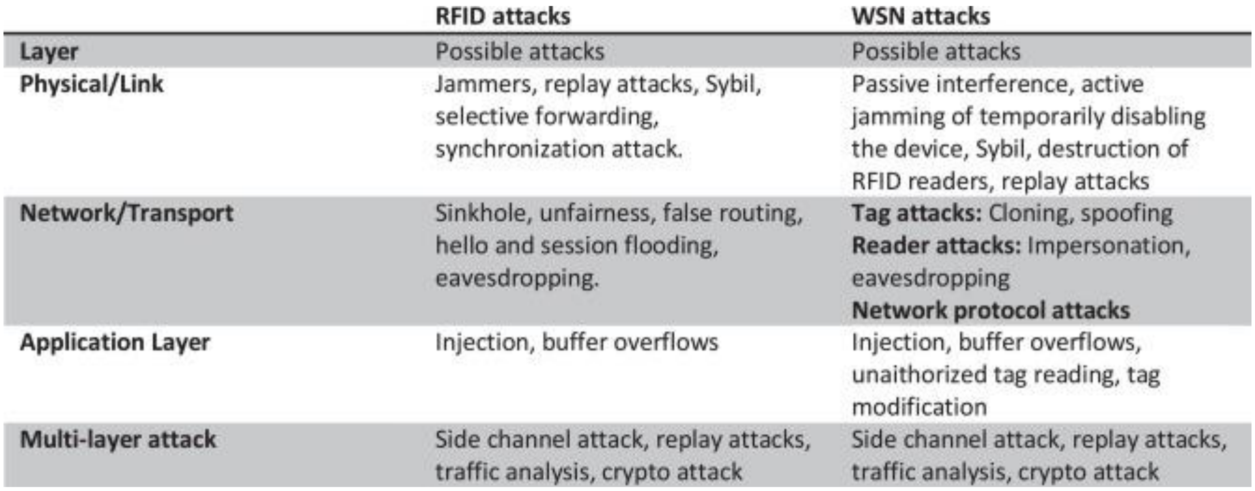


Fig. 1. Typical IoT security architecture



	RFID attacks	WSN attacks
Layer	Possible attacks	Possible attacks
Physical/Link	Jammers, replay attacks, Sybil, selective forwarding, synchronization attack.	Passive interference, active jamming of temporarily disabling the device, Sybil, destruction of RFID readers, replay attacks
Network/Transport	Sinkhole, unfairness, false routing, hello and session flooding, eavesdropping.	**Tag attacks:** Cloning, spoofing **Reader attacks:** Impersonation, eavesdropping **Network protocol attacks**
Application Layer	Injection, buffer overflows	Injection, buffer overflows, unaithorized tag reading, tag modification
Multi-layer attack	Side channel attack, replay attacks, traffic analysis, crypto attack	Side channel attack, replay attacks, traffic analysis, crypto attack

Table1: Possible Attacks on WSN and RFID.

White Box Testing Technique for SOA Application

SOA application, using online book sales application event exposure, has been implemented. This approach to whiten the testing of service compositions is based on events exposed by services.To assure the quality of an SOA application, service consumers usually conduct integration testing to verify whether all the involved services work correctly when composed in the SOA application. Service-oriented architecture (SOA) is a software design and software architecture design pattern based on distinct pieces of software providing application functionality as services to other applications. This is known as service-orientation. It is independent of any vendor, product or technology. SOA is the architectural style that supports loosely coupled services to enable business flexibility in an interoperable technology in an agnostic manner.

2. SOA TESTING CHALLENGES

Testing SOA is somehow an intricate and a challenging computing problem, and that is due to several reasons, some of which are outlined below and figure.1 illustrates the SOA Components.

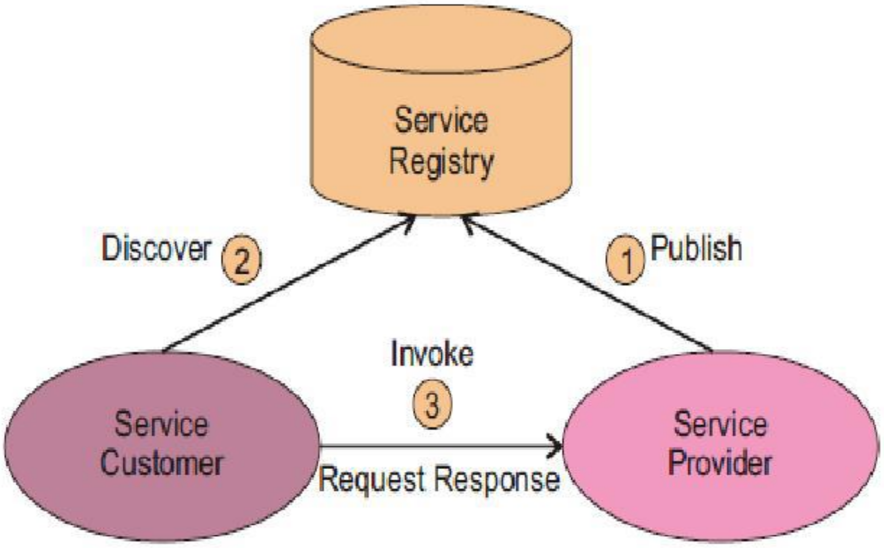


Figure 1. SOA Components

1. SOA is distributed in which they are composed of web service components dispersed over different hardware and operating system platforms; thus, testing must cover the different deployment configurations (Bartolini et al 2009).

2. SOA are dynamic in which they implement adaptive behaviors such as adding new services, integrating new services, and removing old ones; consequently, performing an effective regression testing can be a challenging task.

3. SOA are complex in which they can be seen as a mesh of interacting services, each having specific functionalities and capable of different operations; thus, designing test cases for test automation can be a complicated and a demanding task.

4. SOA are closed in which they are made out of closed services that run on the provider's side and clients have no control over their implementations;

5. SOA are remote in which their services are commonly located on the provider's server; and therefore, testing SOA can be costly, especially, if services are charged on a per-use basis. Moreover, service providers could suffer from denial-of-service (DoS) in case of massive testing.

6. SOA are heterogeneous in which their services deliver no standard interfaces for inter-communication as they are built using incompatible technologies, platforms, and programming languages; thus, it would be necessary to build multiple types of test engines each pertaining to a particular service platform.