Chapter 7

The Access of Things: Spatial Access Control for the Internet of Things

ABSTRACT

Access to resources, both physical and cyber, must be controlled to maintain security. The increasingly connected nature of our world makes access control a paramount issue. The expansion of the Internet of Things into everyday life has created numerous opportunities to share information and resources with other people and other devices. The Internet of Things will contain numerous wireless devices. The level of access each user (human or device) is given must be controlled. Most conventional access control schemes are rigid in that they do not account for environmental context. This solution is not sufficient for the Internet of Things. What is needed is a more granular control of access rights and a gradual degradation or expansion of access based on observed facts. This chapter presents an access control system termed the Access of Things, which employs a gradual degradation of privilege philosophy. The Access of Things concept is applicable to the dynamic security environment present in the Internet of Things.

INTRODUCTION

Today, access to buildings and facilities is often controlled by electronic systems; gone are the days of large key rings. Magnetic stripe technology is one such technology that encodes an identifier linked to a person or employee on their identification card. A scanner at the door reads the identifier and sends it back to a centralized system. The centralized system replies with a message granting access (opening the door) or denying it (keeping the door locked). Wireless versions of this system are available and widely used, with most based on radio frequency identification (RFID)
technology. Both systems rely on the person keeping control of their identification card and preventing it from being copied. This has led to binary security policies for access control systems providing either complete access to all authorized areas or no access at all, and does not function well in the case of copied or “cloned” RFID tags or identification cards. The binary security policy often fails to prevent the cloned RFID tag from gaining entry or locks out the legitimate RFID tag preventing the employee from accomplishing their tasks. The wireless nature of RFID makes cloning possible without physical contact with the legitimate user. A security policy and supporting technology is needed to enable access rights to be gradually and gracefully reduced to allow the legitimate user to complete most of their tasks, while preventing significant damage caused by the malicious user. This chapter will present a framework for such a system for RFID and will discuss the integration of other data sources into this system, yielding a truly Internet of Things approach to spatial access control.

The chapter will begin with an overview of the Internet of Things and the need for access control in this environment. Next, current access control systems and policies, the difficulties introduced by the traditional binary access policy, and the requirements for access control within the Internet of Things will be presented. The graceful degradation of privilege policy will then be introduced and the RFID implementation of this policy will be described. Security measures available to RFID technology to prevent cloning will be highlighted. The extension of the graceful degradation of privilege model to the Internet of Things will be presented. This extension is termed “the Access of Things,” and provides robust access control policies and options for the Internet of Things. The Access of Things concept integrates information from a variety of sources to achieve multi-point identification and authentication of the user. The chapter will conclude with a discussion of future research areas, issues facing access control systems, and how the system presented in this chapter begins to address those concerns.

INTERNET OF THINGS CONCEPT

The Internet of Things (IOT) concept envisions an environment where devices automatically connect together to solve problems or better monitor the environment. The problems that can be addressed in the IOT framework are larger than a single device could solve on its own. This may be due to lack of computing power or lack of access to input data. The concept of the IOT is not necessarily one of human-centric applications, but one that will include more machine-to-machine (M2M) applications facilitated by massive M2M networks supported by the IOT’s infrastructure. The differentiator between the IOT and a generic Internet capable device is the increased degree of autonomy of the device and reliance on M2M communication. In fact, most IOT applications are based around the M2M communication with the human user being a consumer of information or service rather than the initiator of operations.

The initial idea was to provide every device with an IP address for routing data (traffic) between devices to facilitate M2M communication. While IP is a widely used protocol, it may not be the best protocol for all applications and other protocols are available to supplement IP. This is true for IOT applications because many IOT devices have limited computational and communication resources, especially remote sensor nodes.

IOT applications include smart health, remote healthcare (You, Liu, & Tong, 2011; Revere, Black, & Zalila, 2010; Chen, Gonzalez, Leung, Zhang, & Li, 2010; Wicks, Visich, & Li, 2006), home management, traffic management (Foschini, Taleb, Corradi, & Bottazzi, 2011), smart grid, and