Chapter XXXIX
Survivability of Sensors with Key and Trust Management

Jean-Marc Seigneur
University of Genev, Switzerland

Luminita Moraru
University of Genev, Switzerland

Olivier Powell
University of Patras, Greece

ABSTRACT

Weiser (1991) envisioned ubiquitous computing with computing and communicating entities woven into the fabrics of every day life. This chapter deals with the survivability of ambient resource-constrained wireless computing nodes, from fixed sensor network nodes to small devices carried out by roaming entities, for example, as part of a personal area network of a moving person. First, we review the assets that need to be protected, especially the energy of these unplugged devices. There are also a number of specific attacks that are described, for example, direct physical attacks are facilitated by the disappearing security perimeter. Finally, we survey the protection mechanisms that have been proposed with an emphasis on cryptographic keying material and trust management.

INTRODUCTION

Weiser (1991) envisioned a ubiquitous computing world where intelligent computing and communicating devices are pervasive and woven into the fabrics of every day artifacts. His vision is being materialised: the market of large scale sensors and hand-held devices networks has been gaining momentum. However, one may question whether or not these computing and communicating entities will be able to survive in an open environment. These computing entities are no more protected by a physical security perimeter; foreign, potentially malicious, entities can tamper with them. Another challenge for the real deployment of these networks of sensors and portable devices is to provide them

with enough energy for long term functioning because it is assumed that they are unplugged from the main electrical power supply and can rarely recharge themselves by this means. Any action carried out by these entities depletes their energy. In addition to being resource-constrained in terms of energy, these entities are resource-constrained in terms of memory and processing, which limit what they can do, especially when these entities are small, such as the sensors deployed in sensors networks.

Usually, sensors are performing two important types of actions or tasks: they have to sense the environment and to send information to a specific target entity, sometimes called sink. For example, the sink may be an Internet gateway that will propagate the information for persistent storage and analysis. Security problems exist both when messages are generated and when they are relayed. Working most of the time in an unattended environment without tamper-proof hardware makes the sensors very vulnerable to attacks.

Generally, mobile ad hoc networks (MANETs) are thought to be composed of nodes bigger than the sensors of sensors networks. Also, whereas sensors are considered (after their deployment) rather fixed concerning their location, MANETs imply that the nodes move. If we assume that the MANET nodes are also unplugged from the main power supply, the nodes have also limited energy. Another difference between sensors and MANET nodes is that instead of just having to sense and forward simple information, MANET nodes are expected to run much more complicated operations that surely require more energy than simple tasks. In this chapter, we consider all ad hoc networks where the wireless nodes are resource-constrained, especially in terms of energy. Thus, as introduced above, the nodes may go from the tiny fixed deployed sensor to the mobile unplugged mobile device.

In this chapter, we first survey the different assets of these entities and then delve into specific attacks on these assets. We present further two main protection mechanisms: cryptographic keying material and evidence-based trust management. Finally, we discuss future trends and draw our conclusion.

BACKGROUND ASPECTS OF NODES SURVIVABILITY

In this section, we first discuss what we mean by nodes survivability, their assets, and especially their energy. Then, we focus on the routing asset, which is an important asset that enables the nodes to communicate beyond their own wireless communication range. It shows that the routing has been initially engineered without attackers in mind, which is also the case for most of the other enabling mechanisms and assets. However, there are a number of attacks that can be carried out on these assets. We survey them at the end of the section.

Node(s) Survivability

First, it is important to note we use the plural in the heading of this section, *nodes survivability,* because it emphasises that the scope of the node's mission may span more than one node. On one hand, it may be a scenario where the survivability of the node itself is more important than the survivability of the other nodes. For example, a user who carries a mobile phone in the mountains may be selfish and would not bother forwarding the messages of other users as they are met on the way to the top of the mountain. The forwarding of a message from another user would deplete the energy of the mobile phone and endanger the survivability of the device and its mission lifetime. On the other hand, the mission may be that the majority of the nodes survive at the expense of the survival of one specific node. It is usually the case in sensors networks where the goal is to sense and monitor a region thanks to the collaboration of many nodes. If a part of the monitored region is quite active, it is possible that the nodes in this active region take over the work of another node, for example, to forward the sensed information in order to maximise the lifetime of the monitoring of the whole region. That type of scenario requires that there is some sort of control on the nodes; an authority is needed to guarantee that the nodes will collaborate and follow the rules. For example, in a military environment, the nodes that are deployed