Chapter 9
Network Manageability Security
Salvador Mandujano
Intel Corporation, USA

ABSTRACT
As the number of devices connected to computer networks increases, so does the need for algorithms, protocols, and tools to manage these devices and their communications infrastructure. Manageability solutions allow Information Technology administrators to keep control over such resources in order to identify, configure, and repair network devices remotely in a way that reduces desk visits and maximizes service availability for customers. This chapter studies the security and privacy aspects of different manageability technologies. It describes the protection mechanisms built into standard protocols and highlights some of the basic risks they face when deployed in an enterprise environment. Solutions for desktop, laptop, server, and cell phone platforms are discussed and compared in the context of common threats to managed devices, as well as the control consoles that monitor them. Secure enablement and configuration guidelines are provided for implementers and designers to develop effective threat models when integrating manageability software and hardware inside a computer network. The analysis presented in this chapter will help the reader understand how network manageability solutions work and what their strengths and weaknesses are from the security standpoint.

INTRODUCTION
Network manageability encompasses a wide range of remote administration activities that help minimize downtime and accelerate the control and repair of devices connected to a network, from multi-core servers and laptop computers, to PDAs and cell phones. IT shops as well as Manageability Service Providers (MSPs) use these solutions to remotely access a variety of systems connected to enterprise and home networks in order to reconfigure software, apply patches, and monitor performance and security. Manageability technologies can decrease cost of ownership by...
limiting the number of systems that need to be taken to the shop for repair and by reducing the number of desk visits an IT shop needs to cover to support its users.

One of the most powerful capabilities that manageability systems offer is access to a device regardless of health level or power state. That is, even though applications or the operating system may not be operational, an out-of-band channel implemented on the manageability framework is available to remotely troubleshoot the computer, printer, or whatever the device may be. Similarly, if the system is executing in power-saving mode (e.g., standby, hibernate), manageability solutions often support discovery and wakeup functionality that will allow administrators to locate the device on the network, reboot it, and take a look at it, for instance, by establishing a keyboard-video-mouse (KVM) session.

Due to the nature of manageability tasks, access to administration consoles must be carefully controlled, and failure to do so could result in significant network disruption, privacy violations and other security breaches. As we will see, the interfaces made available by the device for administration consoles to connect to them must be secured with strong authentication, and the traffic encrypted in order to prevent unauthorized parties from abusing secondary interfaces. For instance, if the firmware update function on a managed device is not properly protected, an attacker could try to corrupt the firmware on multiple PCs or servers inside the enterprise and prevent them from booting – a costly problem to repair, especially if physical access to the system is necessary.

This chapter analyzes a number of frameworks and protocols that have been developed to support network manageability. New as well as proven technologies that combine hardware, firmware and software components are available today to make manageability more effective, scalable and secure. Protecting this support infrastructure, however, requires clear separation of duties, sound implementations, as well as comprehensive audit ing that allow network administrators to preserve their control over the managed devices at all times. Depending on the type of device, the implications of having insufficient protection coverage may vary. For instance, if a manageability protocol is deployed to troubleshoot laptop systems in the enterprise but the protocol standard does not offer a security bar that is high enough to adequately match the value of the information stored on those systems, the manageability solution may in fact add risk and reduce the security of the network.

Recent research (Bojinov, 2009; Wojtczuk, 2009) has shown an increased interest in the security of manageability products, in part, due to the OS-agnostic nature of some solutions and their privileges over platform resources. We will discuss the protection properties of a number of well known network manageability technologies for servers, desktop computers, laptops and mobile devices. These solutions will be analyzed and compared highlighting their security strengths, limitations as well as their applicability to different classes of networks and devices.

**BASIC MANAGEABILITY FUNCTIONS**

Manageability technologies support a number of fundamental functions that allow administrators to anticipate potential problems and maintain devices operating as expected. From the analysis of different solutions (Campbell, 2007; Sheldon, 2001; Kumar, 2009; Blair, 2007; Berlin, 2009), we can identify some common capabilities offered by them:

- **Discovery.** Ability to find and identify devices connected to the network.
- **Inventory collection.** Software, firmware and hardware on the device can be inventoried for tracking and update purposes.
- **Eventing.** Manageability solutions offer a number of notification mechanisms