*IDEA GROUP PUBLISHING* ITB11413

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This chapter appears in the book, *Managerial Guide for Handling Cyber-Terrorism and Information Warfare* by Lech J. Janczewski and Andrew Colarik © 2005, Idea Group Inc.

## Chapter 10

# Identification, Authentication, and Access Control

It is a known fact that terrorists are developing a keen set of technology skills to further their agendas. As previously stated, they use IT for their operational purposes as well as for launching attacks. In the IT domain, identification/ authentication of a user is the first step in gaining access to system resources. Identity theft attacks are the simplest way to accomplish this objective, as was discussed in the preceding chapter.

In these times of increased security awareness, IT managers must examine very carefully their identification and authentication subsystems to prevent the disabling or bypassing of the system by an unauthorized party. In this section, we will discuss identification, authentication methods, access control, and how to strengthen these methods for added resistance against possible attacks.

## A Question of Proper Identification

We will start this chapter with two cases that identify the need for authenticating a party's identification in a terrorism environment.

### *Case 10.1: Al Qaeda announcement*

> *On August 12, 2003, CNN made the following announcement*:
>
> JAKARTA, Indonesia (CNN) – The al Qaeda terrorist network has claimed responsibility for last week's bombing of the Marriott Hotel in the Indonesian capital of Jakarta, terror experts have confirmed for CNN. The claim comes amid reports the Marriott bomber may have been a member of a new 15-strong suicide strike brigade, which is preparing more attacks. Bomber Asmar Latin San was a member of Laskar Khos, a group whose members were prepared to die in their attacks, Indonesian police told the *Sydney Morning Herald* newspaper. Laskar Khos is an Arabic phrase which means "special force," they said. The new group is reported to have formed inside the al Qaeda-linked Jemaah Islamiyah group which is believed responsible for the Marriott blast and the Bali attacks of October 12th which killed more than 200 people. The al Qaeda claim of responsibility was released to Arab media sites over the weekend in an unsigned statement.

It is worth examining this announcement from the information security specialist's point of view. Objectively, a non-disputable fact that we can draw from this story is that the world's mass media network received a message about the activities in the above case. No more, no less. The identification and authentication of the message from al Qaeda was weak, based on the content of the original message. The attack was carried out using methods implemented previously by al Qaeda units, and, more importantly, the public was waiting for such an announcement. It is obvious that anyone could have generated such a

### *Case 10.2: IRA communication channel*

> It is not a widely known fact that during the period of the highest IRA attacks in Northern Ireland, the British government established a sort of communication channel with the IRA command. At that time, the typical IRA policy was to plant a bomb and inform the authorities shortly before the timed explosion about the bomb's location. Both sides of the conflict wanted to be sure that the warning message was genuine. Because blind terror was not the IRA's primary objective, and the British government was unable to respond to every bomb alert, both sides accepted a specific delivery method of a warning to assure its authenticity.