Chapter 11

IMPERSONATING USERS

INTRODUCTION

Identity theft is one of the fastest growing crimes in the United States. The loss to consumers was more than $700 million in 2006 [1].

But, what about the loss to enterprises, institutions and government bodies from identity theft that results in unlawful access to buildings that house physical assets and the IT network that house mission-critical, digital assets or the costs associated with trying to secure those buildings and the Internet against intrusion. Simply stated, identity theft is the unlawful acquisition of an individual's personal information by someone who uses that information to assume the identity of his or her victim for personal gain or to cause harm [1].

WHAT'S AT RISK?

For most enterprises, potential threats include:

- Subversive attacks, in which an intruder manipulates the system into non-legitimate activities, like transferring money.
- Disruptive attacks, which compromise business data and/or systems and interrupts activity.
- Privacy attacks, in which outside individuals gain access to private information.
- Physical attacks, in which outsiders gain access to a building and cause harm to property or people or steal assets [1].

Because identity theft has become so pervasive, enterprises and institutions are faced with three major, but separate security issues: physical access control, time & attendance control and logical access control, but all rely upon a common task – identity and access management [1].

IDENTITY AND ACCESS MANAGEMENT

The fire service uses a triangle to explain fire. Heat + Fuel + Oxygen = Fire. Remove any element and the triangle collapses and the fire dies. Security can be described in much the same way. Identity Management + Access Management = Security. Compromise either and security fails [1].

Traditionally, there have been only two methods by which identity and access have been controlled; what one knows and what one has. If you know something that only you are supposed to know, like your mother's maiden name, a four-digit personal identification number (PIN), or a secret password, then you must be who you say your are. If you have something that only you are supposed to possess, like an office key, car key, ATM card, swipe card or token, then you must be the valid owner [1].

IT'S NOT WHAT YOU KNOW THAT COUNTS

As illogical as this seems in today's world, these two methodologies continue to be the methods of choice for many enterprises, though banks have made the process more robust by implementing a two-challenge protocol. Anyone using an ATM card is required to know his or her four-digit PIN and to have his or her ATM card. Yet, as robust as this security challenge appears, it is frequently compromised when an ATM card is lost or stolen. Not only because a four digit PIN is relatively easy to guess, but also because many people write their PIN number on the back of their card or have actually shared their PIN number with the person that has stolen their card [1].

In most security breaches, whether physical or logical, it is the human factor that enables the breach to occur. In fact, according to CERT/CC1 84% of all Internet security breaches result from a password that has been stolen or shared. Passwords are the weakest link! Why? See the following reasons:

- Password weaknesses are well known and easily exploited. Passwords that are based on simple words that users can easily remember are also easy for hackers to guess. Simple password cracking programs can find many whole word passwords quickly.
- As passwords become more complex or increase in number, users tend to write them down.
- Passwords are subject to social engineering attacks. According to industry analysts, four out of five employees give their passwords to someone else within the company if asked. A persuasive outside caller is often able to extract passwords over the phone.
- To avoid remembering many passwords, people often use the same password across many systems, including unsecured websites where passwords may be sent in a clear text format. A single password, once cracked, may open many doors.
- Some e-mail viruses send password information back to the originator of the virus [1].

The main threats to security include outsiders who gain access by impersonating authorized users and legitimate users who impersonate other users with different authorization levels [1].