Chapter XXXVI
Hacking and Eavesdropping

Kevin Curran
University of Ulster, UK

Peter Breslin
University of Ulster, UK

Kevin McLaughlin
University of Ulster, UK

Gary Tracey
University of Ulster, UK

ABSTRACT

Many self-proclaimed hackers would actually consider themselves to be performing a service to businesses as they claim they are simply showing businesses the flaws within their systems so that they can implement ways to prevent future attacks. They state that if it was not for hacking, then security software would not be where it is today. An ethical hacker will tell you that someone who hacks into a system for purposes of self benefit would be best known as a cracker, rather than a hacker, for it is the latter that gives cause for security software in the first place. This chapter reviews the tools, methods, and rationale of hackers.

INTRODUCTION

"Access" is defined in Section 2(1)(a) of the Information Technology Act[1] as "gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network." Unauthorized access, therefore, would mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system, or computer network. Thus not only would accessing a server by cracking its password authentication system be unauthorized access, switching on a computer system without the permission of the person in charge of such a computer system would also be unauthorized access. Raymond (1996), compiler of *The New Hacker's Dictionary,* defines a hacker as a clever programmer. According to Raymond, a *good hack* is a clever solution

to a programming problem and *hacking* is the act of doing it. Raymond lists five possible characteristics that qualify one as a hacker:

1. A person who enjoys learning details of a programming language or system
2. A person who enjoys actually doing the programming, rather than just theorizing about it
3. A person capable of appreciating someone else's hacking
4. A person who picks up programming quickly
5. A person who is an expert at a particular programming language or system, as in "Unix hacker"

Raymond, like a lot of hackers, condemns someone who attempts to crack someone else's system or otherwise uses programming or expert knowledge to act maliciously. This type of person, according to most hackers would better be described as a *cracker*. A cracker is someone who illegally breaks into someone else's computer or network by bypassing passwords, licences, and so forth. A cracker could be doing this for purposes of maliciously making a profit. On the other hand, a hacker (according to a hacker) would break into a system to supposedly point out the site's security problems. Therefore, we must carefully distinguish between a hacker and a cracker. Although hacking, according to a lot of hackers themselves is beneficial to the development of systems security, it is still known as a crime under the Computer Misuse Act. Categories of misuse under this act, include: computer fraud—unauthorized access to information; computer hacking; eavesdropping; unauthorized use for personal benefit; unauthorized alteration or destruction of data; denying access to authorized user; and unauthorized removal of data (Harris, Harper, Eagle, Ness, & Lester, 2005).

The law does not distinguish between a hacker and a cracker. In relation to this, reformed hacker John Draper states that:

Hackers are very important for the Internet community as a whole because they are the ones who will be buttoning up the holes in the system. Governments should be a little more tolerant of what is going on and hackers should be willing to contact a company and say "I found bugs in your system." (Machlis, 2000)

He believes that without hackers, security would not be where it is today. He believes that hackers are playing a valuable part in the development of highly effective security systems, and that the government and the law should recognize this. They should try to distinguish more carefully between a hacker with intent of displaying security flaws for the company and a cracker whose intent is truly malicious.

Crackers use various methods to maliciously attack a computer system's security, one such method is a "virus." A virus is defined as a piece of programming code usually disguised as something else that causes some unexpected and usually undesirable event. A *computer virus* attaches itself to a program or file, so it can spread from one computer to another, leaving infections as it travels. The severity and effects of a computer virus can range much the same as a human virus. Some viruses have only mild affects simply annoying the host, but more severe viruses can cause serious damage to both hardware and software. Almost all viruses are attached to an executable file, which means the virus may exist on your computer, but it cannot infect your computer unless you run or open the malicious program. It is important to note that a virus cannot be spread without a human action (such as running an infected program) to keep it going. People continue the spread of a computer virus, mostly unknowingly, by sharing infecting files or sending e-mails with viruses as attachments in the e-mail.

Another method is to use a "worm." A worm is similar to a virus in both design and in the damage it can cause. Like a virus, worms spread from system to system, but unlike a virus, it has the ability to travel without any help from the user. It does this by taking advantage of the files and information already present on the computer. The biggest danger with a worm is its ability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect. For example,