

# Cybersleuthing: Means, Motive, and Opportunity

Larry Rogers

Editor's Note: This column originally appeared in the June 2000 issue of InfoSec Outlook, a joint publication of the Information Technology Association of America (<http://www.ita.org>) and the CERT<sup>®</sup> Coordination Center (<http://www.cert.org>) at the Software Engineering Institute.

We've all seen television police dramas where the detectives nab the criminal by determining who has the means, a motive, and the opportunity to commit a crime. They ask questions such as "Did the suspect have the means to commit the crime? Did they have something to gain? Did they have the opportunity to carry out the crime?" We can view trends in cyber attacks using the same three categories: means, motive, and opportunity.

## Means

To commit an Internet-based crime, intruders need either personal expertise or the tools that are freely available through the Internet. It is the sum of the two that defines the means to do the job at hand.

The means for attacking computer systems has changed over the years. Ten years ago, intruders attacked computer systems primarily "by hand." For example, they tried to guess passwords by brute force techniques such as repeatedly trying to login to an account by using a dictionary of passwords. They also used social engineering methods to trick people into revealing passwords. Today, there are tools that encrypt dictionary words and their variations (such as replacing the letter "o" with the digit "0") and compare them to the encrypted password.

The level of sophistication of intrusion tools has become high and is getting higher. Intruders have harnessed the power of the Internet itself, building automated tools to coordinate large-scale attacks involving hundreds of hosts aimed at Internet sites. These tools are well documented and freely available on the Internet. Members of the intruder community share programs and improve on each other's work.

Sophisticated tools have given birth to a class of script kiddies, intruders who use tools to break into computer systems although they lack the knowledge to craft the tools themselves or to even understand the nuances of their inner workings. There have been reports of break-ins where the script kiddies used a sophisticated tool to gain access to one operating system but then typed commands that work only on another operating system.

## **Motive**

Motives for computer attacks have evolved just as the means have. In the early years of the Internet (then called the ARPAnet), there were no .com sites, only government and university research information. In 1981 only 213 computers were connected to the Internet. The small network made it easy for researchers at diverse locations to cooperate on work to their mutual benefit. There was a collegial atmosphere of sharing among people who either knew each other or knew of each other.

Contrast that to today's Internet. The January 2000 Internet Domain Survey reports that .com sites make up more than one-third of the Internet, which has now passed the 72-million computers mark. You can find nearly everything on the Internet today: proprietary information about companies and people, corporate strategic plans, access to financial resources, and most commercial products.

Computer power has increased from the days of the VAX-11/780 with its 1 MIPS (million instructions per second) processing power, to 1Ghz (gigahertz) Pentium III processors, an increase of more than 800%. As a result, attackers can steal computer cycles without the knowledge of the computer owner.

Long gone are the days of users and administrators knowing and trusting each other. Users on the Internet are anonymous, and their number grows daily. The atmosphere is not collegial, and trust is neither automatic nor always warranted.

## **Opportunities**

Opportunities for computer attacks are readily available for two reasons: the number of vulnerable systems on the Internet and the ease of connecting to the Internet. Ten years ago, there were about 300,000 hosts on what was then the ARPAnet; today there are more than 72 million. Even if the same percentage of vulnerable hosts exists, that's nearly 25,000% more vulnerable hosts today.

The number of computers on the Internet and the difficulty of configuring them securely means that attackers have more chances of finding a way into systems than they did a decade ago. Along with low-cost Internet access, computers are inexpensive and the price is dropping. This means that more attackers can afford both the computer and the Internet access needed for an attack.

Also, there are many more opportunities for computer access. Some libraries provide free Internet access. My children's school invites family members to use its computing facilities one evening a week. These Internet access points are a convenience and a helpful service, but they are also an opportunity to commit a crime, and are readily available to anyone so inclined.

## Who Wants to be a Millionaire?

Whatever the motive—money, curiosity, politics, power—this is all it takes to commit a crime on the Internet:

- Means—the tools are there, nicely catalogued and ready to go.
- Motives—with so much on the Internet, motives are there.
- Opportunity—there are many, many access points to the Internet. Most are inexpensive, some are free.

Intrusions are going to happen; it's inevitable. Administrators, their managers, and senior executives all need to know what they're up against so that they are better equipped to deal with attacks and be aware of what intruders are doing. Because attack techniques and tools are constantly changing, we must maintain constant vigilance.

## About the Author

**Larry Rogers** is a senior member of the technical staff in the Networked Systems Survivability Program at the Software Engineering Institute. The CERT<sup>®</sup> Coordination Center is a part of this program. Rogers' primary focus is analyzing system and network vulnerabilities and helping to transition security technology into production use. His professional interests are in the areas of the administering systems in a secure fashion and software tools and techniques for creating new systems being deployed on the Internet. Before joining the SEI, Rogers worked for ten years at Princeton University, first in the Department of Computer Science on the Massive Memory Machine project, and later at the Department of Computing and Information Technology (CIT). Rogers co-authored the *Advanced Programmer's Guide to UNIX Systems V* with Rebecca Thomas and Jean Yates. He received a BS in systems analysis from Miami University in 1976 and an MA in computer engineering in 1978 from Case Western Reserve University.

---

Copyright 2000 Carnegie Mellon University

The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

<sup>®</sup> Capability Maturity Model, Capability Maturity Modeling, CERT, CERT Coordination Center, and CMM are registered in the U.S. Patent and Trademark Office.

<sup>SM</sup> Architecture Tradeoff Analysis Method; ATAM; CMM Integration; CMMI; CURE; IDEAL; Interim Profile; OCTAVE; Operationally Critical Threat, Asset, and Vulnerability Evaluation;

Personal Software Process; PSP; SCE; Simplex; Team Software Process; and TSP are service marks of Carnegie Mellon University.

™ Simplex is a trademark of Carnegie Mellon University.