# The Cuckoo’s Egg Exercise

In the 1980’s Clifford Stoll provided one of the first true and detailed accounts of a real-life computer hacker in his book, *The Cuckoo’s Egg*. Stoll first suspected that something was not right with the computing systems in his astronomy lab at Lawrence Berkeley Lab when he discovered a 75-cent discrepancy between the time-sharing system logs and the accounting logs. Was somebody using computer time somehow without running up charges? Stoll began an investigation that provided him a close-up view of the underground world of computer hacking. Fortunately for us, he wrote it down in a book, and it provides an engaging read and a glimpse into the world of computing and computer hacking in the 1980s.

In the book, Stoll describes how the hacker was deeply familiar with various operating systems and with how computer networks were configured. The hacker was skilled and knowledgeable on the level of a professional systems and network administrator. The hacker was also adept at cracking passwords by using a forward search attack that started with dictionary words and then computed hashes for later comparison to known hashes. The hacker also wrote scripts and even modified operating system utilities to act as Trojan horses. He modified the login program to secretly record all login attempts in plaintext in a hidden file.

Stoll also describes how the hacker was able to escalate his privileges on systems from a regular user to root level by using Gnu-Emacs, a popular text editor with a built-in mail feature which enabled users to communicate with one another by writing files into each other’s home directories. The hacker had the key insight that it was also possible to use the mail utility to write files into the systems directory. So, the hacker wrote a “message” to the systems directory that was actually a simple shell script programmed to change his login’s permissions to root-level access. Since the script was in the system’s directory, it was able to be executed by Cron – a program that runs in the background on Unix systems and executes scripts on a schedule.

This possibility likely never occurred to the Gnu-Emacs developers because there was no legitimate reason to send messages to the systems folder. In fact, this attack is why Stoll titled the book, *The Cuckoo’s Egg*. Stoll thought of the attack as the hacker “laying an egg” in “the system’s nest” that would later “hatch,” and when it did hatch, that would take over the entire computer system! This is similar to how a cuckoo bird lays its egg in a different bird species’ nest, and when it hatches, the baby cuckoo bird kicks the mother’s actual baby birds out of the nest so that it will be raised by the mother!

Stoll also describes how the hacker installed backdoors so that he could gain access to systems even after they had been patched, how he modified logs and audit trails to avoid detection, how he hid information in the compromised computer systems for later retrieval, how we tunneled through several intermediary computers to make it difficult to trace his whereabouts, and how he employed many shrewd tactics for identifying new login credentials, including keyword searches in emails and files, installing Trojan horses to capture login attempts, and password cracking and guessing. Many of these tactics allowed the hacker to pivot from the initially compromised machine so that he could attack additional systems. By searching through email messages, the hacker was also able to monitor whether or not the victim organization was suspicious of the possibility that they had been hacked.

**Q1: Identify the hacker’s actions that illustrate each of the three components of adversarial thinking (technological capabilities, unconventional perspectives, and strategic reasoning). Defend your choices based on the three types of intelligence in Sternberg’s triarchic theory (analytical, creative, and practical).**