Article Review

Stalking the Wily Hacker*

In August 1986, a computer intruder attacked the Lawrence Berkeley Laboratory (LBL). The intruder was not as popularly expected, a "whiz–kid" but a competent, patient programmer experienced in several operating systems.

LBL's first response was to disable the security hole and change all passwords. However the LBL is a research institute and it was decided to take the novel approach of allowing the intruder access in an attempt to determine who was breaking into the system and to reveal its apparent weaknesses. This project was to last some 10 months and to cost the University over $US100,000 in computing and network time.

The break–in was first detected when one of the LBL's computers reported an accounting error; namely an account name was found with no billing address. Not long after, a message from the National Computer Security Center arrived, reporting that someone from LBL had attempted to break in to one of their computers through MILNET (Military Network) connection.

It was decided initially, that to successfully monitor and trace the intruder would require a well organised effort. A detailed logbook was kept, summarizing the intruder's traffic, the traces, the suspicions of staff at LBL and interactions with law enforcement people.

Monitors and alarms were set up so that computer personnel could be notified instantly the intruder entered the system.

Printouts provided details of the intruder's keystrokes, targets, keywords, chosen passwords and methods.

The intruder attempted to access various computers through different networks using common account names and passwords. The passwords he guessed were English words, common names or place names. He was decrypting password files on his local computer by successively encrypting dictionary words and comparing the results to password file entries.

Did the intruder cause damage? He tried not to erase files and killed only a few processes. However he wasted systems staff time, computing resources and network connection time and ran up a large bill in long distance telephone calls and international network charges.

The attack raises many interesting legal questions, perhaps most importantly should the laboratory have remained open? By remaining open the intruder was able to attack other sites, in particular various military installations. The author argues that whether LBL closed up or not, the intruder may still have been able to access MILNET. By disabling him, the laboratory could neither monitor him nor trace his connections in real time.

And what about the legal responses.? The author states that police agencies were relatively uninterested until monetary loss could be quantified and damages demonstrated. As the case was international in scope, it was necessary to work closely with law enforcement organizations of many different countries. There was confusion as to responsibility. Most organizations recognized the seriousness of the break–ins, yet no one agency had clear responsibility to solve it! Further problems raised concerned the scope of the duties and responsibilities of common carriers such as Tymnet and German Bundespost?

Passwords are at the heart of computer security. The following requirements should not be forgotten;

–non guessable
–not in a dictionary
–frequently changed
–easily remembered

This disturbing article reminds the reader about the problems of security particularly in networked systems. Although not providing any ready answers it raises interesting legal problems requiring detailed research and greater legislative consideration.

* *By Clifford Stoll, Communications of the ACM May 1988, Volume 31 No 5*

[Editor's note: It was decided not to prosecute the "hacker".]