**Paper review**

*An Evening with Berferd In Which a Cracker is Lured, Endured and Studied*

*by Bill Cheswick*

This article documents a system administrator’s attempts to lure hackers (crackers) into a controlled environment, study the various attacks attempted by the hackers, and trace the origins of the attacks. The events occurred in 1991, and may not reflect the current state of the Internet and its vulnerabilities. However, it has taught us some important lessons that we have yet to solve.

**Development of automated tools to track suspicious activities.** The author of the article (at that time) had to review the logs manually to find suspected attempts to break into the system. Now we have various tools to scan for suspicious activities. I believe this is the right approach to take, since breaking into a system usually involves unnatural behavior (such as port scanning, unusual inputs to services, etc.).

**Using “honey pots” to study possible attacks.** This is precisely what the author of the article is doing. He sets up a restricted environment, and lets the hacker play around in it. This gives useful information on what kind of attacks a hacker might attempt.

**Complicated programs running with root privilege.** The main problem in most systems is that most services must run under the root privilege. These services often involve large and complicated components, entailing multiple vulnerabilities. To avoid this problem, many services are suggested to be run under more restricted privilege. Moreover, much work has been put into designing a small “secure” kernel which can be verified of correctness, and is trusted to perform privileged system calls. Also the kernel will be able to verify other processes whether they have been tampered with or not. This reduces the risk of a hacker gaining complete control of the system.

**Working as a community and international cooperation.** The paper shows the importance of working as a community to prevent and track down hackers. Information obtained from the honey pot should be shared among system administrators to help prevent possible attacks. Also, hackers usually use stolen identities to launch the attack so that their attacks cannot be easily tracked. Thus, tracking an attack requires cooperation of all the system administrators’ involved. Moreover, since the Internet has no boundaries international cooperation is also critical. In the article, the hacker was in the Netherlands, where hacking was legal, and thus no legal action could be pursued.

I am strongly against the U.S. policy in limiting export of cryptographic technology. This makes machines with inferior cryptographic tools a weaker link, and thus hackers may compromise these machines to launch attacks on machines in the U.S. Again, I repeat that the Internet has no boundaries, and securing only a portion of the Internet is not the solution (unless you are not going to interact with the rest of the world).