

**Hacker Vulnerability: A Major New Complication in Crystallographic Computing.** Carroll K. Johnson, *Chemical Sciences Division, Oak Ridge National Laboratory\**, and *Mathematics Department, University of Tennessee, Knoxville.* ([johnsonck@ornl.gov](mailto:johnsonck@ornl.gov))

At the 2002 ACA session on computer security, a surprisingly large fraction of the audience had been hacked either at home or the laboratory. On the internet, there are frequent bug fixes by major system-software vendors in response to security breaches and long lists of newly discovered vulnerabilities without fixes or workarounds. Most crystallographic programs were written with little thought given to malicious user action. Current and future generation computing must respond to this development with better software engineering and network security.

It is tempting to rationalize that no one would want to hack you at home, and I started my retirement in 1996 with that mindset. Through online auctions, I assembled a computer laboratory with a local area network interfacing the internet. It uses a half dozen different operating systems on a dozen IBM and Apple computers. The plan was to leisurely solve the associated problems and use the system to do something credible in computational crystallographic topology. The hardware, system software, and mathematical theory are in reasonable shape, but the title topic has stymied (but also fascinated) me for over a year.

Firewalls on a hardware gateway router and all computers provide the default home-office defense. My current system has a Cisco enterprise-level router and a Cisco cable modem, each using Cisco IOS IP-control commands\*\*. Less capable firewalls did not deter the more proficient of the heckling hackers. Pending projects include database logging and analysis for intrusion detection and forensics, and tripwire-triggered replacement of compromised components from a segmented backup.

\*\**Router Security Configuration Guide*; National Security Agency, Ft. Meade, MD. <http://nsa1.www.conxion.com/cisco/download.htm>

\*Oak Ridge National Lab. is managed and operated by UT-Battelle, LLC, for the U.S. Department. of Energy under contract DE-AC05-00OR22725.