Keynote Address

Visual Tools for Security: Is there a there there?

Bill Cheswick

AT&T Research

Abstract

It seems obvious: networks, software, authentication, and people have important and often complicated relationships and interactions. There's far too much going on to keep track of all of it, but we know there are important devils down in the details. We know they are there.

Though many have been chasing this dream of security visualization for a couple of decades, we don't have that much to show for our efforts. We use NOCs and tools widely for managing large networks, but they get complicated fast. And most of the anomalous activity is weird but benign, leaving us awash in a sea of false positives. And those people in the NOCs seem totally resistant to 3D displays, data gloves, and other cool tools of our trade.

What can we do? How can we help, really?

Bio

Bill Cheswick logged into his first computer in 1968. Seven years later, he was graduated from Lehigh University in 1975 with a degree resembling Computer Science.

Cheswick has worked on (and against) operating system security for over 35 years. He has worked at Lehigh University and the Naval Air Development Center in system software and communications. At the American Newspaper Publishers Association/Research Institute he shared his first patent for a hardware-based spelling checker, a device clearly after its time.

For several years he consulted at a variety of universities doing system management, software development, communications design and installation, PC evaluations, etc.

Ches joined Bell Labs in December 1987, where he became postmaster and firewall administrator and designer. In 1990 he published a paper on firewall design that coined the word "proxy" in its current meaning. He followed this with "An Evening With Berferd", and then the publication of "Firewalls and Internet Security; Repelling the Wily Hacker", co-authored with Steve Bellovin. This book taught Internet security to a generation of administrators. In 1998, Ches started the Internet Mapping Project with Hal Burch. This work became to core technology of a Bell Labs spin-off, Lumeta Corporation. Ches has pinged a US nuclear attack submarine (distance, 66ms).

During his sabbatical over the winter of 2007 he worked on science museum including an upgrade for the Liberty Science Center's digital darkroom.

He joined AT&T Research in Florham Park in April 2007 and is working in security, visualization, user interfaces, and a variety of other things. He is a frequent keynote speaker at securty conferences.

Ches has a wide interest in science and medicine. In his spare time he reads technical journals, hacks on Mythtv and his home, and develops exhibit software for science museums. He eats very plain food---boring by even American standards.