Bennett E. Todd III
bet@rahul.net
bennett.e.todd@gmail.com
(201) 667-2368

Languages and Systems

I am expert in Perl and Bourne Shell. I know the C programming language well. I've studied perl 6 and rust. I've designed and negotiated security policies, built and maintained firewalls and IDS systems, and performed security administration. I support Red Hat Linux regularly, and work occasionally with Solaris. My focus is Unix system administration automation and security.

Papers and Projects

I've published a paper on auditing firewalls, available from
https://bet.github.io/firewall-audit-paper/p5.htm
I've written and maintained several open source projects, including a high-performance POP-before-SMTP authentication daemon for use with Postfix, and a custom Linux distribution based on embedded Linux.
I've written an overview of cryptography,
https://bet.github.io/crypto/index.html

Experience

Google — New York, NY 2019-2020
I worked as a Security Engineer, analyzing internal controls, looking for gaps that might enable internal access to private user data, submitting requests to close them, and confirming that they were closed.
TD Securities — New York, NY 2016-2018
I helped in adding DMARC, DKIM, and SPF records for email security. I helped document and simplify our administration procedures for our multi-factor authentication servers, and enable their use, via RADIUS, for a password archive; and created operations documentation for upgrading them. I helped evaluate Content Distribution Network and Web Application firewall vendors. I wrote and deployed programs to automatically transfer user account lists, with roles, from two different vendor systems to an in-house account re-authorization system.

CNBC — Englewood Cliffs, NJ 2013-2014
I built an IDS sensor, did post-incident forensic analysis, and created our password policy. I built and deployed a tool for forensic session logging, as a companion to the IDS sensor. I designed our configuration collection and tracking system.

Goldman Sachs New York, NY 2008-2010

I helped automate system administration of Linux and Solaris servers, including automated periodic inventory of systems and batch system modification.

Morgan Stanley New York, NY 2003-2008

I was a Unix systems engineer at Morgan Stanley. I created and supported their secure Linux build, for stand alone and security-sensitive applications. I maintained and developed their internal DNS infrastructure. I designed the DNS architecture and servers for a new, highly scalable internal build based on CERN's Quattor.

Société Générale New York, NY 2002-2003

I was a security analyst at Société Générale, in their Information Security and Governance department. I designed and implemented their Perimeter Intrusion Detection System; I created several utilization reporting systems, importing logs of various sorts — web utilization, NT and Unix login activity — and web-based query/reporting tools for viewing the data.

Morgan Stanley New York, NY 2001-2002

I was a security analyst at Morgan Stanley, in their Information Technology Security Engineering department. I designed and implemented their virus-scanning bastion email server. I developed and implemented a remote computing solution for ssh access. I supported many groups, reviewing designs and auditing code, helping ensure that new deployments introduced no security problems.

Oven Digital New York, NY 1999-2000

I was the senior security and systems analyst at Oven Digital.

I wrote their security policy, and designed and implemented their firewalls. I set up their email server and DNS infrastructure, and developed the email content filtering that trapped out any email worms before they are delivered to their users. I provided the architectural design and implementation for scalable, high-performance, high-security, high-availability web server farms.

Lehman Brothers, Inc. Jersey City, NJ 1998-1999

I was a Senior Systems Administrator and Systems Analyst at Lehman Brothers.

I developed a full-text index search engine companion to the in-house trouble ticket database; I developed a data mining application for systems management, that collected information both from direct probes of systems, and from various administrative tables in management databases, and allowed report generation queries through a web interface against the collected data. This was instrumental in planning and managing upgrades.

Fuji Capital Markets Corp. New York, NY 1995-1998

I was a Senior Systems Analyst at Fuji Capital Markets.

I worked as a Systems Administrator, with a team that supported 200 users. I was also the security administrator, charged with internal and external computer systems security planning, maintenance, testing, and reporting. I designed the Jumpstart configuration for Solaris, along with the packaging standard and automounter architecture we used for installing and accessing software.

Salomon Brothers, Inc. New York, NY 1991-1995
I worked as a Senior Systems Analyst for SBI.
I set up an in-house WWW server, designed our web documents, and put the Perl 5 manual up for access via WWW, with an automatically-maintained index of all the documentation for libraries.
I headed up the design and implementation of facilities for automating the installation, restoration (e.g. after disk failure), and maintenance of several hundred workstations. I produced a software suite for automated network load of SunOS 4.x, much in the style of Jumpstart. The group I worked with provided second-tier support for some seventy System Administrators, who were in turn responsible for machines serving roughly a thousand end-users, including traders, researchers, and application developers.
I brought in, built, and supported substantial free software packages, including TeXand LaTeX, Xfig and Transfig, X11R5, Perl, TCL/Tk, and all the GNU software. I wrote software and performed delivery testing in support of deploying software into production. I dramatically enhanced the local software distribution process, both by writing software and by establishing standards for packaging and delivery.
I tested and packaged many security-related facilities, including net-distributed security challenge programs like Crack, COPS, and SATAN, as well as security fixes like Sun's ypserv patch and new versions of sendmail.

Radiology Department, Duke University Medical Center Durham, NC 1988-1991
My responsibilities included system administration, user support, system programming, and application programming on a network of Sun workstations and other systems, used for medical image processing. I completed two substantial tasks connecting non-standard peripherals to our system, requiring system programming. I performed security auditing, and improved the network's security substantially.

Computation Center, Duke University Durham, NC 1984-1988
I supported System V UNIX on AT&T 3B5, IBM OS/MVS and VM on various mainframes, and MS-DOS on PCs. In this job I answered questions from users all over the University, performed minor contract programming tasks, and served as system administrator for the UNIX facility offered by the Computation Center.

Education

Department of Electrical Engineering, School of Engineering, Durham, NC 1980-1984
Duke University
I earned a Bachelor of Science in Electrical Engineering, Magna Cum Laude, and completed departmental requirements for a Bachelor of Science in Computer Science.