Distributed Denial of Service Attacks - Can We Survive This New Threat?

Chair -

Jon David
Lehman Brothers

Panelists -

Steve Bellovin
AT&T Labs Research

Bill Cheswick
Lucent Technologies

Paul Ferguson
Cisco

DDoS attacks have recently made headlines by taking down major networks and services. The sharing of attack "enhancements" and the providing of attack tools via the web makes these attacks a growing threat. This session investigates the nature and elements of DDoS attacks, and presents things to be done by users, sys admins, ISPs, router vendors and the like to best treat this threat. Key areas it will treat are:

What is a DDoS attack?

How is DDoS different from other threats?

Can they be detected in time?

What security/network practices need be in place?

What user preparation is necessary for DDoS hits?

What industry preparation is necessary for DDoS?

Directions in DDoS attacks.

Jon David

Jon David is an officer in the Security Engineering group at Lehman Brothers. With over 30 years in security, he was a pioneer in both computer and network security. Prior to Lehman Brothers, he was Director of Network Security for an ISP, and spent a depressingly long time as a security consultant. He is a frequent author and speaker, and has repeatedly been in the van of security technology. Well past his prime and clearly at the pre-dotage stage of life, he lives off of the knowledge and abilities of friends these days. In an attempt to disguise his street kid tendencies, he did his undergraduate work at Queens College and his graduate work at Columbia University.

Steve Bellovin

Steven M. Bellovin received a B.A. degree from Columbia University, and an M.S. and Ph.D. in Computer Science from the University of North Carolina at Chapel Hill. While a graduate student, he helped create netnews; for this, he and the other perpetrators were award the 1995 Usenix Lifetime Achievement Award. He joined AT&T Bell Laboratories in 1982. Despite the

fact that he has not changed jobs, he is now at AT&T Labs Research, working on networks, security, and why the two don't get along. He was named an AT&T Fellow in 1998.

Bellovin is the co-author of the recent book "Firewalls and Internet Security: Repelling the Wily Hacker," and holds several patents on cryptographic and network protocols. He served on a National Research Council study committee on information systems trustworthiness is a member of the Internet Architecture Board, and is currently focusing on how to write systems that are inherently more secure.

Bill Cheswick

Bill Cheswick logged into his first computer in 1969. Six years later, he was graduated from Lehigh University with a degree that looked like Computer Science.

Cheswick has worked on (and against) operating system security for nearly 30 years. He contracted for several years at Lehigh and the Naval Air Development Center working on systems programming and communications. In 1978 he worked at the American Newspaper Publishers Association/Research Institute, where he shared a patent for a hardware-based spelling checker, a device clearly after its time.

For the next nine years he worked for Systems and Computer Technology Corporation at a variety of universities including Temple University, LaSalle College, Harvard Business School, Manhattan College, NJIT, and several others. Duties included system management, consulting, software development, communications design and installation, PC evaluations, etc.

In 1987 (Morris minus 1) he joined Bell Laboratories as a Member of the Technical Staff. Since then he has worked on firewalls, network security, PC viruses, mailers, interactive science exhibits, and trash-picking in the physics building. He co-authored the first full book on Internet security in 1994, and has since toured the world giving talks and supplying the media with sound bites. Infoweek called him "the sweet but feral hacker-in-residence at Bell Labs."

Ches has been working on Internet mapping problems, and has produced some really smashing posters. He has now turned these tools towards the control and understanding of large intranets, which are always out of control. He is now working on perimeter scans that can find breaches in a network defense perimeter.

In his spare time he launches rockets with his wife, tries to fly RC aircraft, works on exhibits for science museums, and automates his home.

Paul Ferguson

Paul Ferguson is a consulting engineer on Internet architecture in the Office of the CTO at Cisco Systems, Inc., and is based in the Washington, D.C., area. His principal disciplines are large-scale design and global routing, Internet security, and Internet service provider architectural issues in general. He is an active participant in the Internet Engineering Task Force (IETF), as well as the North American Network Operators Group (NANOG), and has authored several books, articles for various trade journals, and successfully submitted several articles to publications on data networking issues. Mr. Ferguson has been with Cisco for 5 years—prior to that, he has worked for Sprint, Computer Sciences Corporation (CSC), NASA, and AT&T.