HOW CAN WE PREVENT DENIALS OF SERVICE?

Peter G. Neumann, Computer Science Lab, SRI International, Chair
Steve Bellovin, AT&T Labs
Virgil Gligor, University of Maryland
J.F. Mergen, Genuity
Marv Schaefer, ARCA

PREVENTING DENIALS OF SERVICE

Peter G. Neumann, Computer Science Lab, SRI International
Menlo Park, California 94025-3493
1-650-494-1433 Neumann@CSL.sri.com

Subsequent to earlier denial-of-service (DoS) flooding attacks (such as smurf, syn, ping-of-death), the flurry of distributed denial-of-service attacks in February 2000 (affecting Yahoo, Amazon, eBay, CNN.com, Buy.com, ZDNet, E*Trade, and Excite.com, among others) has intensified the realization that the problems we face lie deep in our information infrastructures—inadequate protection and integrity in operating systems, networking, protocols, mailer environments and many other applications, and operational practice.

Many of these attacks typically target systems without needing any authorized access, although the distributed DoS attacks additionally benefitted from their ability to penetrate unsuspecting intermediate host systems (zombies). Actually, given the penetrability of the systems around the Internet, the consequences in the future could be vastly more devastating than we have seen thus far. Thus, it is essential that we rethink our system and network architectures and our overall approaches to using the Internet.

This panel explores what (if anything) can be done to combat denials of service from a total systems/network perspective, hopefully without too seriously compromising the performance that everyone has come to expect. A wide range of topics must be considered within scope of the discussion, such as radically different system and network architectures, defensive protocols, pervasive use of cryptography (for example, for authentication, integrity, and confidentiality), automated tools for early detection of and response to attacks, and many operational considerations. One of the biggest challenges we face is developing, configuring, and operating systems and networks with stringent requirements for survivability (with subrequirements for security, reliability, and real-time performance). Some relevant background may be found in [1].

1. Peter G. Neumann, Practical Architectures for Survivable Systems and Networks, Final report for the U.S. Army Research Laboratory, 30 June 2000. http://www.csl.sri.com/neumann/arl-two.html and .ps and .pdf

Denials of Service and Economic Risks

JF Mergen
VP Product Development & Technology
Chief Engineer, Global Networks
GENUiTY
<Jfmergen@genuity.com>

The ability of the industrialized world to continue to improve its standard of living is becoming increasingly dependent to the access to complete, accurate and reliable information. Much of the wealth creation of the last two decades is predicated on the movement and use of information rather than on the increasing consumption of physical resources. In addition, the best hope for improving the quality of life for the non-industrialized world lies in the expansion of access to information and the ability to disseminate homegrown knowledge for commercial purposes.

All of the growth of the information economy is based on a collection of competing, dissimilar networks and organizations providing a reliable, ubiquitous and low cost infrastructure. This is all done without a central authority, command structure or (at least it seams) a willingness to cooperate.

Given the above, and the number of interests which wish to upset the status quo there is an increasing risk to the global economy from perturbations to the communications environment. The result is an environment where the communications systems operation cannot be predicated upon the cooperation and support of all the other elements in the network. The result will be the emergence of a class of systems, which can operate under duress and can adapt to the loads and pressures placed upon them. How these systems evolve and the decision models for their operation are key questions to the creation and expansion of the growing global communications grid. Providing systems, which have a natural propensity to return to a stable and viable state when disturbed in any manner, is a central challenge to the designer today.

Speakers' Bios

Peter G. Neumann <neumann@csl.sri.com> is a Principal Scientist in the Computer Science Laboratory at SRI (where he has been since 1971), concerned with computer system survivability, security, reliability, human safety, and high assurance. He is the author of *Computer-Related Risks*, Moderator of the ACM Risks Forum (comp.risks), Chairman of the ACM Committee on Computers and Public Policy, and Associate Editor of the CACM for the Inside Risks column. He is a member of the U.S. General Accounting Office Executive Council on Information Management and Technology. See http://www.CSL.sri.com/neumann/ for Senate and House testimonies, reports, RISKS, papers, slides, etc. Neumann is a Fellow of the American Association for the Advancement of Science, the ACM, and the Institute of Electrical and Electronics Engineers (of which he is also a member of the Computer Society). He has received the ACM Outstanding Contribution Award for 1992, the first SRI Exceptional Performance Award for Leadership in Community Service in 1992, the Electronic Frontier Foundation Pioneer Award in 1996, the ACM SIGSOFT Distinguished Service Award in 1997, and the CPSR Norbert Wiener Award for in October 1997, for "deep commitment to the socially responsible use of computing technology."

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.

Virgil D. Gligor received his B.Sc., M.Sc., and Ph.D. degrees in EECS from the University of California at Berkeley in 1972, 1973, and 1976 respectively. He joined the University of Maryland in 1976, where he is a Professor of Electrical and Computer Engineering. Virgil's interests have been in the areas of: (1) network and distributed system security, and (2) cryptographic schemes, protocols and infrastructures. He has done some of the early work on denial of service, and some of that work was reported at the IEEE Symposium on Security and Privacy, 1983 -- 1988.

John-Francis Mergen received a BSEE in Electrical Engineering and Administrative Science from Yale in 1978, and an M.S. in Management, with a concentration in Information Systems, Sloan School, MIT, Cambridge, MA, 1981. He is a staff member in the Center for Information Sciences Research (CISR) and the Digital System Laboratory. His thesis title was "An Examination of Joint U.S./Japanese Ventures in the Computer Industry". Since 1995, he has been at GENUiTY (formerly BBN Planet), now as VP of Product Development & Technology Chief Engineer, Global Networks. He is responsible for technology planning efforts, including next generation photonic networks, IP/DWDM, and advanced technology initiatives for the network. He is also responsible for all aspects of GENUiTY global network. Responsibilities include architecture of international systems; development of business and operational relationships to extend the network; support of activities to assure efficient markets in Europe; development of the GENUiTY fully routed photonic backbone; implementation of the non-US portions of the GENUiTY network.

Marv Schaefer is VP & Chief Scientist at Arca (since 1994). He was the first Chief Scientist of the NSA/National Computer Security Center 1982-84. He is a contributing author to TCSEC, and chaired the NAS/AFSB Summer Study on Multilevel Database Management Security. Involved in computer security since 1965 (modified disk swapping algorithm and central tables on Q32-TSS as user while system was running and while not logged in); learned system design flaws technology while on tiger teams through mid 1970s. Played hand at doing it right starting with writing ADEPT-50 security model (1967); Hinke-Schaefer Multilevel Relational DBMS security model (1973-4); Kernelized VM/370 (1976-82). Information Security, including network security and covert channel theory, formal methods (including InaJo/FDM). Other professional interests: language/compiler design, Petri Nets, algebraic number theory. Worked for SDC, Cie Internationale pour l’Informatique, TIS, CTA. Other interests: antiquarian books, zither, go.