

FINAL REPORT

Second Workshop on Ultra Large Networks: New Research Directions in Modeling and Simulation-based Security

Sponsor

National Science Foundation
Advanced Networking and Infrastructure Research Division

Organizers

Arizona Center for Integrative Modeling & Simulation (ACIMS)
Stevens Institute of Technology
Society for Modeling and Simulation International (SCS)

Held during May 29-31, 2003 at Stevens Institute of Technology, New Jersey, USA

Table of Content

1. Sponsor and Organizers	3
1.1 List of Participants	3
2. Purpose.....	3
3. Outcome	3
4. Background	4
5. Final Agenda	5
6. Summary of Findings.....	6
6.1 Keynotes and Discussions:	6
6.2 GroupSystems Session.....	7
6.2.1 Recommendations Resulting from GroupSystems Session:.....	7
7. New Research Directions.....	8
8. Summary of Recommendations	8
9. Bibliography.....	9
Appendix 1. Keynote presentations and keynoters' biographies	10
Appendix 2. Key Findings and Recommendations of the Participants (GroupSystems).....	16

Overview

The Second Workshop on Ultra Large Networks: New Directions in Modeling and Simulation-based Security, May 29-31, Stevens Institute of Technology, was hosted by the Arizona Center for Integrative Modeling & Simulation (ACIMS), the Secure Network Systems Design Laboratory (SENDLAB), and the Society for Modeling and Simulation International (SCS) under sponsorship of the National Science Foundation Advanced Networking Infrastructure Research Program (ANIR, NSF).

1. Sponsor and Organizers

Dr. Taieb Znati, Program Manager, ANIR, NSF
Prof. Sumit Ghosh, Stevens Institute of Technology
Prof. Hessam Sarjoughian, Arizona State University
Prof. Bernard Zeigler, University of Arizona
Steven Branch, Society for Modeling and Simulation, International (SCS)

1.1 List of Participants

Alan Boulanger, IBM Research
Steve Branch, SCS
Bill Cheswick, Lumeta Corp.
Sung-Do Chi, Hangkong University, Korea
Jerry M. Couretas, Lockheed Martin Corp.
Richard Fujimoto, Georgia Tech.
Erol Gelenbe, University of Central Florida
Sumit Ghosh, Stevens Institute of Technology
Jim Lee, University of Arizona
Lyndon Pierson, Sandia National Labs
Hessam Sarjoughian, Arizona State University
Tom Tarman, Sandia National Labs
Elliot Turrini, Elliot Turrini, MDM
Gabriel Wainer, Carleton University
Bill Way, Bytex Corp.
Bernard Zeigler, University of Arizona

2. Purpose

The workshop brought together users of cyberspace networks and researchers in networking, modeling, and simulation. Their task included identifying key user requirements for network security, and to translate these requirements into definitive simulation-based design approaches for future robust and secure ultra-large networks.

3. Outcome

As planned, the workshop shed light on some of the key unknowns of cyberspace security. Participants formulated new research directions that addressed such unknowns using modeling and simulation technologies. The results of this workshop include a set of specific findings of gaps in our knowledge of security issues in Cyberspace and recommendations for how to employ modeling and simulation to improve our understanding in these areas. The thinking is that increased understanding will foster the development of new paradigms for design of infrastructure elements for management, and control.

The workshop participants proposed the goal of developing "inherently secure architecture" that scales to large networks and does not depend on the ever more frequent patches and security updates. Consider an example of simulation-based approach to cyberspace security. Network security can be described

comprehensively within a Fundamental Security Framework (see Ghosh [1]) thus enabling security to be viewed as a design parameter in the development of any networked system, and threat scenarios to be designed and assessed through modeling and simulation. In such a framework, network security transcends the traditional end-to-end encryption paradigm and assumes the form of an engineering concept that lends itself to systematic design, scientific measurement, and quantitative assessment. The workshop participants concluded that modeling and simulation is a must-use tool needed to incorporate security as a network design parameter and measure its impact on the network performance. Beyond this, modeling and simulation is needed to develop and test a logical set of principles to help design and validate networks with desired attributes such as security and high performance. Further, it is needed to understand and make the difficult tradeoffs between increased security and reduced privacy. Moreover, modeling and simulation may supply agile tools that are able to rapidly analyze new scenarios and phenomena as they appear in order to defend against increasingly quick, sophisticated, and powerful intrusions and virus attacks.

4. Background

There are many issues that arise in the emergence of ultra-large communication networks, such as the Internet, with billions of highly decentralized interacting parts. The greatly increased connectivity and capability creates new kinds of complexities and dynamics that we are only on the verge of appreciating. The requirements of robustness and security often conflict with each other and those of performance and thus imply formidable challenges. Difficulties in dealing with large-scale software systems are well documented in a recent report by the National Research Council (*Making IT Better, see Bibliography*). Techniques that work for small software systems fail when the scale is increased by hundred- to million-fold. In the context of ultra-large communication networks, current software limitations are manifest in a key finding that virtually all IP-based networks, used to control the national power grid, financial systems, and other critical infrastructure suffer from lack of robustness and are vulnerable to complete failure of communications and control under stress such as occurred during 9/11/01. Furthermore, failure to overcome current technological limitations such as inability to trace IP packets may ultimately severely impact the Constitutional right to privacy.

The plan underlying ULN'03 was to build on the findings from the first workshop in this series, ULN'01 and from a recent workshop "Guarding Your Business", held at Steven Institute of Technology. We would focus specifically on the issues of security and robustness in ultra-large networks. Users of cyberspace would help identify critical vulnerabilities and failures of security in today's networking technologies. Network simulation modelers would help translate these limitations into requirements for design of future networks. Participants would address the need for new techniques and approaches to build models of cyberspace networks and develop simulation environments for studying their behaviors. They would also assess whether current design approaches can be evolved to deal with the large increases in scale or whether revolutionary paradigms are required. Suggestions for borrowing points of view from other areas such as complex adaptive systems and from basic theory of modeling and simulation would be encouraged.

The workshop would result in a report providing significant guidelines to stimulate network infrastructure research by

- consolidating existing research findings,
- identifying network requirements from user's points of view, and
- generating recommendations for modeling and simulation-based infrastructures to support the design of secure and robust large scale networks of the future.

5. Final Agenda

First Day (Thursday, May 29, 2003)	
Times	Activity
07:00 - 07:45	Breakfast
08:00 - 08:10	Welcome, Dr. George Korfiatis, Dean, Schafer School of Engineering, Stevens
08:10 - 08:20	Review of ULN '01, Prof. Hessam Sarjoughian, ASU
08:20 - 08:30	Overview of ULN '03, Prof. Sumit Ghosh, Stevens
08:30 - 10:30	Network Security Keynote presentations <i>Experiences with Internet and Intranet Mapping</i> , Bill Cheswick, Lumeta Corp. <i>Towards Building a Secure Internet</i> , Alan Boulanger, IBM Research <i>Network Security: More than an End-to-End Problem</i> , Tom Tarman, Sandia National Labs
10:30 - 10:45	Break
10:45 - 12:00	Modeling and Simulation/Network Security Keynote presentations <i>Simulation of Ultra-Large Networks: Simulation, Emulation, and Modeling</i> , Erol Gelenbe, UCF <i>Secure Networked Systems and the Future</i> , Sumit Ghosh, Stevens Institute of Technology
12:00 - 14:00	Lunch and Keynote Presentation <i>Embedded Values: the Importance of a Multi-Discipline Approach to Network Security</i> , Elliot Turrini, MDM
14:00 - 17:00	Parallel Breakout Sessions
18:30 - 21:00	Dinner
Second Day (Friday, May 30, 2003)	
07:00 - 7:45	Breakfast
08:00 - 08:15	Welcome to Stevens, Dr. Frank Fernandez, Director of Institute Initiatives
08:15 - 09:15	Keynote Presentations <i>Large-Scale Network Simulation: How Big? How Fast?</i> Richard Fujimoto, Georgia Institute of Technology <i>Modeling and simulation of security in ULN: can we apply ideas of how brains focus attention on the most urgent inputs</i> , Bernard Zeigler, UoA
09:30 - 12:00	GroupSystems-facilitated Anonymous Assessment of the First Day's findings
12:00 - 14:00	Lunch and Keynote Presentation <i>Changes Required to Secure the Distributed Intelligent Network of the Future</i> , Bill Way, Bytex Corp.
14:00 - 15:00	Keynoters Panel discussion
15:00 - 16:00	Summarize Findings, Recommendations, and Wrap-up
ACIMS Board Meeting (Saturday, May 31, 2003)	

6. Summary of Findings

The outcomes of this workshop are based on i) the keynote presentations and their deliberations and ii) the formulation and assessment of a set of proposed ideas and steps toward the realization of secure ultra large networks. The first set of findings (see Section 7.1) provided a basis for formulating a set of recommendation (see Section 7.2) to be objectively and critically considered by the workshop participants during an anonymous two-hour group session meeting.

6.1 Keynotes and Discussions:

ULN'01 had focused on the role of modeling and simulation in the design of ultra-large networks. As the next logical step, ULN'03 focused on security, one of the most important aspects of network design, and its impact on ultra-large network design. A unique characteristic of ULN'03 was that it brought together leading experts from diverse disciplines and the user community, beyond the traditional engineering and networking areas, to focus on the multidimensional nature of secure ultra-large networks. A summary of the keynoters' comments is:

- ✍ The first keynote by Bill Cheswick from industry observed that the true connectivity in the current Internet is virtually impossible to document for a number of reasons. He presented a partial though detailed connectivity map of the worldwide Internet that he was able to generate utilizing knowledge of the design and operation of the routers (primarily Cisco brand) and sophisticated port scanning and pinging techniques. The map, however, was static and it lacked information on the bandwidth of the links.
- ✍ Alan Boulanger, also from industry, described how network security has become one of the most important issues and that many of the security weaknesses in the Internet are fundamentally tied to its original design. He explained that industry was increasingly relying on authentication and private-public keys and stressed the need for novel techniques in the future.
- ✍ Tom Tarman from Sandia government research lab, stressed that network security is a much bigger problem than the current thinking that relies on authentication and encrypted end-to-end pipes. For the future, he stressed research into new network designs that will integrate connection-oriented networking principles with a mechanism to encapsulate a network's security resources in the form of a quality of service metric, similar to the Fundamental Security Framework proposed by Schumacher and Ghosh.
- ✍ Erol Gelenbe, from academia, proposed novel non-IP protocols as a means to overcome the vulnerabilities of the current Internet and described a testbed to validate the idea in a realistic setting by combining the Internet with experimental systems.
- ✍ As a representative of the law enforcement community that uses networks to fight crime, Elliot Turrini, explained why ensuring privacy on the network is crucial to the democratic principles upon which the nation is founded.
- ✍ Bill Way represented network security vendors and described the conflicting requirements of the different aspects of a network design. He advocated modeling and simulation as holding the key to systematic design of such complex networks. He detailed the evolution of GigBE, the Department of Defense's version of an ultra-large network.
- ✍ Sumit Ghosh, from academia, presented a comprehensive picture of secure network design. The key is the Fundamental Security Framework that can assist by encapsulating the security posture of any network as a quantitative measure. The other key elements of the picture include vulnerability analysis and threat scenario design that may be assessed through modeling and asynchronous distributed simulation techniques.
- ✍ Richard Fujimoto, from academia, described in detail parallel and distributed network simulation tools for simulation of large networks in real- or near-real-time.

✍ Bernard Zeigler, from academia, focused on a distributed, scalable approach to increase an ultra-large network's sensitivity and timely response to threats of different levels of severity. He presented key principles that the human brain employs to remain alert to the most active threats while continuing to be aware of lower-level background threats. Many of these ideas may be transferred to ultra-large networks and validated through simulation. Gabriel Wainer and Sung-Do Chi demonstrated their modeling and simulation environments to illustrate these possibilities.

Abstracts of the Keynote presentation can be found in Appendix A.

6.2 GroupSystems Session

The consensus obtained via the GroupSystem session reveals the diversity of engineering and scientific barriers as well as social issues. Technical challenges emphasized the key role security plays in the development of new genres of different kinds of networks, intra- and inter-networking protocols, and applications ranging from operating systems to ubiquitous end-to-end user applications.

The results also singled out the enormity of defining and protecting user privacy rights as embedded in the conceptual and detailed design and realization of ultra large networks. In particular, providing flexible degrees of security measures to ordinary citizens, corporations, and government is a central challenge.

The recommendations listed below reveal modeling and simulation both as a catalyst and as an enabler for handling the inherent scalability and complexity aspects of secure ultra large networks. It is also important to note that the ranking of the recommendations were not widely varied. Instead the variation among the recommendations is relatively small and thus pointing to their close interdependencies.

6.2.1 Recommendations Resulting from GroupSystems Session:

1. Develop a logical set of principles to help design and validate networks with desired attributes such as security and high performance.
2. Develop the "science" of information systems security analysis.
3. Design survivable, scalable and reconfigurable networks together with software which guards against possible attacks.
4. Gain acceptance for modeling and simulation as a must-use tool among "real" network developers.
5. Find analogies with physical/natural systems and research their validity.
6. Develop a "spiral engineering" approach to ULN that has built-in cycles of adaptation based on intensive off- and on-line use of modeling and simulation.
7. Address security needs in the presence of other equally challenging issues such as privacy.
8. Develop "inherently secure architecture" that scales to large networks and does not depend on the ever more frequent patches and security updates.
9. Develop agile network modeling tools that are able to rapidly analyze new scenarios and phenomena that appear.
10. Validate secure protocol design approaches through simulation.

During the first part of the group session, the workshop participants reviewed and debated a set of 12 recommendations which were devised at the end of the Keynote sessions. The outcome of this activity was a consensus on a set of 14 recommendations. Using the GroupSystems software and facilitation by Dr. James Lee, the participants examined and expressed their thoughts and responses to these recommendations. Following the workshop, some of the original recommendations were found to be closely related to one another which were subsequently reduced, and slightly rephrased, to constitute the 10 recommendations listed above. The transcript of the workshop participants' comments and opinions, as well as the complete list of the recommendations, can be found in Appendix B.

7. New Research Directions

Analysis of the keynote presentations, discussions, and GroupSystems session points to the following new research directions:

- ?? The community needs to investigate threat scenarios that cut across the hardware, software, and algorithmic elements of complex networks.
- ?? Studies need to be conducted to develop a logical set of principles to automatically identify threats to different types of networks including communications, control, and sensor.
- ?? It is essential for societal adoption that we understand the difficult tradeoffs between increased security and reduced privacy.
- ?? Identify, comprehensively, the requirements of future network design from the perspective of law enforcement.
- ?? Biologically inspired approaches to strengthen critical infrastructure networks warrant further study.
- ?? Automated mechanisms to generate a dynamic “weather” map of the Internet, especially focusing on the link bandwidths and their utilizations, is an important research topic.

Modeling and simulation is the only feasible approach to enable research in these directions. It is needed to investigate threat scenarios in realistic models of real environments, to develop and test logical sets of principles for network design, to help make the difficult tradeoffs between increased security and reduced privacy, to study the application of biologically inspired approaches and dynamic network-wide maps to defend against increasingly quick, sophisticated, and powerful intrusions and virus attacks.

8. Summary of Recommendations

How can the biological brain offer insights in to the nature of the Internet – a chaotic interconnection of large numbers of computers whose growth is uncontrolled? Are there parallels to biological immune systems that can be useful in developing new approaches to defending the Internet against malicious attacks intended to bring it to a standstill? These are some of the questions that were discussed at the workshop. ...

Besides new perspectives on increasing security in the Internet and other large-scale networks, the workshop discussed ways in which modeling and simulation can be employed to investigate these perspectives. The workshop heard of advances in simulation methodology that employ large numbers of networked processors to simulate realistic models of Internet packet traffic in near real time. This methodology could provide the computational foundation to test theories of Internet behavior and how security might be integrally built in to networks like it in the future. Further, models of the Internet and its vulnerabilities to attack can be running on-line to test preventive measures before they are implemented on the real system.

For more information see <http://www.acims.arizona.edu/EVENTS/ULN03/synopsis.htm> and “Principles of Secure Network Systems Design,” A Springer-Verlag Original Monograph, 0-387-95213-6, April 2002 by Sumit Ghosh.

9. Bibliography

1. Sumit Ghosh, Principles of Secure Network Systems Design, Springer-Verlag, ISBN 0-387-95213-6, April 2002. Translated into Simplified Chinese by Chongqing University Press, China, 2003.
2. H.J. Schumacher and Sumit Ghosh, "A Fundamental Framework for Network Security," Journal of Networks and Computer Applications, Vol. 20, No. 3, July 1997, pp. 305-322. Academic Press.
3. Ed Witzke, Tom Tarman, Gerald Woodard, and Sumit Ghosh, "A Novel Scaleable Architecture for Intrusion Detection and Mitigation in Switched Networks," Proceedings of the IEEE Milcom 2002, Oct 7-10, 2002, The Disneyland Resort, Anaheim, CA.
4. H.J. Schumacher, Tony Lee, and Sumit Ghosh, "Top Security Traffic and the Public ATM Network Infrastructure," Journal of Information Systems Security, Vol. 7, No. 4, Winter 1999 (December), pp. 27-45, Auerbach Publications.
5. Sumit Ghosh, Algorithm Design for Networked Information Technology Systems: Principles and Applications, Springer-Verlag, ISBN 0-387-95544-5, October 2003.
6. National Research Council, "Making IT Better: Expanding Information Technology Research to Meet Society's Needs", National Academies Press, 272 pages, 2000
7. Hessam Sarjoughian and F. Cellier, "Discrete Event Modeling and Simulation Technologies: A Tapestry of Systems and AI-Based Theories and Methodologies", Springer-Verlag, 2001
8. Bernard P. Zeigler, Herbert Praehofer and Tag Gon Kim, "Theory of Modeling and Simulation, 2nd Edition, Academic Press, 2000

Appendices

Appendix 1. Keynote presentations and keynoters' biographies

Experiences with Internet and Intranet Mapping

Bill Cheswick
Lumeta Corp

Abstract:

The Internet Mapping Project started at Bell Labs in 1997 to collect long term Internet topological data and visualize the results. In 1999, we focused on the Serbian internet during the NATO bombing, and observed major connectivity disruptions. In 2000, this technology was spun off to a startup company, Lumeta. Since then, Lumeta has enhanced this technology and scanned over fifty large corporate intranets, and a number of critical government networks. We can now report generalized characteristics of these large networks, showing variations in network management techniques and control over large networks. We are now working on tools to configure the honeyd anti-hacking tool to emulate these large networks.

Biography:

Bill Cheswick logged into his first computer in the fall of 1968, and was graduated from Lehigh University in 1975. In 1987 he joined Bell Labs, where he worked on early firewall and IDS designs. With Steve Bellovin, he wrote Firewalls and Internet Security: Repelling the Wily Hacker, a fairly popular book on the subject. The second edition came out in March 2003 with the help of a third co-author, Avi Rubin. Ches also worked on commercial munitions, application gateways, PC viruses, and a variety of other Internet diversions. He started the Internet Mapping Project with Hal Burch in 1998. In 2000, he co-founded Lumeta, a spin-off from Bell Labs to commercialize various intranet exploration techniques. In his spare time, Cheswick flies RC airplanes, computerizes his house, and has scanned in over 80 GB of images of old photos. He is partial to steak (medium rare), and mint imperials.

Towards building a secure Internet.

Alan Boulanger
IBM Research

Abstract:

The Governments and businesses in racing to use the Internet have chosen a dangerous track. The current Internet is an inherently insecure and unstable platform on which to conduct business critical operations. There are several bridging technologies that have been developed to mitigate the vulnerability of current security exposures, however large security gaps remain. These gaps can only be addressed through significant changes in the underlying architectures of the systems that comprise the Internet. This need for security is now a powerful force influencing current and future technical innovation. Many companies deploying new applications and systems are beginning to build security into the product in the design phase. Organizations are beginning to understand that security is important. The recent news reports of high profile security related incidents, such as the Melissa Virus and DDOS attacks, has brought the issue of computer security into public view. Once restricted to the domain of fantasy books and fiction, hackers and virus authors have become an increasingly visible threat to everyday users. Why is this possible? How can we as a community protect ourselves? This talk will address the current security

related problems with the current implementation of the Internet and the technologies that are currently under development, along with future technologies, that are designed to make the Global Internet an safer place for users and businesses alike.

Biography:

Alan Boulanger joined IBM in October 1995 as a research member of the TJ Watson Global Security Analysis Laboratory. His research interests include network security, intrusion detection systems, applied penetration testing tools and techniques, data forensics, telephony related security, and researching new system vulnerabilities. As a result of his research, Boulanger has numerous filed patent applications related to computer security issues. Since joining IBM, Boulanger has provided technical assistance to numerous Federal Law Enforcement and Intelligence Agencies and Businesses conducting computer security related investigations. As a result of his efforts, Boulanger has received many awards and commendations from IBM and Government Agencies. He is an invited long-standing member of the New York Electronic Crimes Task Force.

Network Security: More than an End-to-End Problem

**Tom Tarman
Sandia National Labs**

Abstract:

Network security is often regarded as an “end to end problem,” meaning that if the endpoints perform appropriate cryptographic and key management, all network security problems are solved. However, network security involves more than encrypted pipes and end-to-end authentication – it requires protection of the network infrastructure as well. This talk describes the shortcomings of regarding network security purely as an end-to-end problem, presents mechanisms for protecting network infrastructure, and introduces future research challenges in securing network infrastructure.

Biography:

Tom Tarman is a distinguished member of the technical staff at Sandia National Laboratories, in Albuquerque New Mexico, where he primarily performs network security research. Tom has been active in the field of ATM network security for the past eight years, having published several conference papers and journal articles on topics such as high-speed ATM encryption, algorithm-agile ATM encryption, and ATM security protocols. In addition, Tom has been an active participant in the ATM Forum Security Working Group, where he has authored numerous contributions and has served as editor for the ATM Security Specifications Versions 1.0 and 1.1. Tom received the ATM Forum's Spotlight Award for his technical and “PR” contributions to ATM security, and has recently co-authored (with Edward Witzke) a book entitled “Implementing Security for ATM Networks,” available from Artech House Publishers. Tom's current research interests include security for MPLS and all-optical networks, network modeling and simulation, and networked multimedia applications.

Simulation of Ultra Large Networks: Simulation, Emulation and Modeling

**Erol Gelenbe
University of Central Florida**

Abstract:

We discuss testing advanced network techniques in "the large" by combining simulation and emulation techniques. Combining the Internet with experimental systems allows experimentation with novel non-IP

protocols to be performed in a realistic setting.. Some experiments that have been conducted on Cognitive Packet Networks will be presented. If time permits, we will also discuss some new research directions in the theory of network QoS.

Biography:

Erol Gelenbe (FIEEE, FACM) has served as the Nello L. Teer Professor and Chair of Electrical Engineering at Duke University (1993-98) and as the University Chair Professor of EECS and Founding Director of the School of EECS at UCF (1998-2003). His research interests include self-adaptive and autonomic networks and systems, as well as performance modeling and simulation.

Secure Networked Systems and the Future
Sumit Ghosh
Stevens Institute of Technology

Abstract:

Networked Systems are here to stay, not for the next 50 or 100 years, but for thousands of years into the foreseeable future. They will be an integral part of our civilization and it is critical that we design them correctly. The origin of many of the winding and confusing roads in New Jersey may be traced back to the colonial days when the world was a very different place and most people did not have a clue of what U.S. was going to become. Over the past 50 years and continuing well into the future, drivers along these roads will be confused, delayed, lost, and angry. The cumulative cost is unimaginably high, a very heavy burden for the design decisions of the past. Networked systems are literally the road systems of tomorrow and, it is imperative, that we make every effort not to impose the slightest burden on the future. This presentation will focus on the fundamental attributes of secure networked systems, the challenges that arise from these attributes, and new strategies to deal with them.

Biography:

Sumit Ghosh is the Thomas E. Hattrick Professor of Information Systems Engineering at Stevens Institute of Technology. He is the author of “Principles of Secure Network Systems Design” (Springer-Verlag, April 2002), “Modeling and Asynchronous Distributed Simulation” (IEEE Press, June 2000), “Algorithms for Networked Information Technology Systems” (Springer-Verlag, Aug 2003), “Intelligent Transportation Systems: New Principles and Architectures” (CRC Press, Jan 2000), and “Hardware Description Languages: Concepts and Principles” (IEEE Press, September 1999). He is co-editor of “Guarding Your Business: An Architecture for Security” (Kluwer Publisher, August 2003). His research interests include network security, networking, hardware design languages, computational intelligence, engineering creativity, ethics, and engineering education.

Embedded Values: the importance of a multi-discipline approach to network security.
Elliot Turrini
MDM

Abstract:

Our current and future reliance on digital networking technology has made network security an important social, legal, and economic issue. Businesses, governments, and individuals have raced to adopt digital networking technology -- with little concern for the downside. The upside of digital networking is clear: substantial improvements in communication capabilities. Unfortunately, however, the downside has been hidden, neglected, or a combination of the two. My presentation contends that a multi-discipline approach

involving law, technology, psychology, economics, and risk management/insurance is required to (a) reveal the downside of digital networking technology and (b) improve the probability that digital networking technology will provide a net social gain. Moreover, I will contend that the scientists, engineers, and technologists working on digital network technology must be aware of the multi-discipline issues, so that they can incorporate that knowledge into their work. Digital networking technology, standing alone, may provide one of the most effective ways to reduce the downside of this technology. Doing so, however, requires a broad scope of knowledge, which can be applied through a multi-discipline approach.

Biography:

Elliot Turrini received a Bachelor's degree from Yale University in 1987 and his Juris Doctorate Summa Cum Laude from Seton Hall University School of Law in 1992, where he was an Articles Editor for the Law Review. Turrini is the former law clerk to the Honorable Morton I. Greenberg, United States Court of Appeals for the Third Circuit, and to the Honorable Kenneth C. MacKenzie, Presiding Judge, Chancery Division, Morris and Sussex Counties. He was previously associated with the firm of Lowenstein Sandler in Roseland, New Jersey, before joining the United States Attorney's Office in Newark where he served for seven years. During his tenure as a federal prosecutor, he prosecuted some of the Department of Justice's most significant chemical diversion cases, as well as one of the Department's largest international money laundering investigations. Moreover, he conducted complex federal criminal trials. Turrini's major accomplishments at the United States Attorney's Office came in his capacity as a Computer and Telecommunication Coordinator, where he prosecuted computer criminals including David Smith for having disseminated the Melissa Virus. As a result of his expertise in computer crime and information security, Wadsworth Publishing asked him to edit an information security/computer crime book that is due to be published summer 2003. The book is a multi-discipline contributed reader that brings together experts in law, technology, psychology, economics, risk management, and insurance to assist the private and public sectors develop efficient, effective, and responsible computer crime/information security strategies. At MDM, as more fully described below, Turrini's practice will focus on two areas: (1) Information Security, Cyberlaw, and Privacy, and (2) Controlled Substances -- such as pseudoephedrine and ephedrine. He will also be doing corporate investigations, complex civil litigation, white collar criminal defense, and anti-money laundering compliance/counseling.

Large-Scale Network Simulation: How Big? How Fast?

Richard Fujimoto

Georgia Institute of Technology

Abstract:

Parallel and distributed network simulation tools are emerging that offer the ability to simulate networks containing millions of network nodes and hundreds of thousands of concurrent traffic flows in real- or near-real-time. This capability offers enormous opportunities for researchers to study scalability issues that could not be previously addressed. At the same time, it also creates challenges to the networking research community to create scenarios and configurations that are realistic relative to current and future Internet configurations. It creates challenges to tool builders to create verified and validated simulators that are easy to use and execute efficiently on parallel and distributed computers over a wide range of network configurations and scenarios. This presentation will describe an approach to realizing scalable network simulations that leverage existing sequential simulation models and software. Specifically, two parallel network simulators have been developed, one based on the widely used ns2 simulator (termed pdns), and another based on a tool developed at Georgia Tech called GTNets. Packet-level simulations using pdns executing on 1024 processors at the Pittsburgh Supercomputer Center yielded performance as

high as 80 Million simulated packet transmissions per second of wallclock time for a network containing over 3.8 million network nodes. This research represents joint work with Drs. Mostafa Ammar, Kalyan Perumalla, George Riley and several PhD students at Georgia Tech, and is funded by NSF (grants ANI-9977544 and ANI-0136939) and DARPA (contract N66001-00-1-8934).

Biography:

Dr. Richard Fujimoto is a professor in the College of Computing at the Georgia Institute of Technology. He received the Ph.D. and M.S. degrees from the University of California at Berkeley in 1980 and 1983 in Computer Science and Electrical Engineering, and B.S. degrees from the University of Illinois at Urbana in 1977 and 1978 in Computer Science and Computer Engineering, respectively. He has been an active researcher in the parallel and distributed simulation community since 1985, and has published numerous technical papers as well as a book on this subject. He has led the development of parallel/distributed simulation software systems including the Georgia Tech Time Warp (GTW) simulation executive on which the TeD parallel network simulator is based, and the Federated Simulation Development Kit (FDK) used to create parallel versions of ns2 and GTNets. He has given several tutorials on parallel and distributed simulation at leading conferences. He led the definition of the time management services for the U.S. Department of Defense High Level Architecture (HLA). Fujimoto is Co-Editor-in-Chief of SCS Transactions (as of July 1, 2003), and has been an area editor for ACM Transactions on Modeling and Computer Simulation since it was founded in 1990. He has served on the organizing and program committees of several major simulation conferences such as the Workshop on Parallel and Distributed Simulation (PADS) and the Simulation Interoperability Workshop (SIW).

Modeling and simulation of security in ULN: can we apply ideas of how brains focus attention on the most urgent inputs?

**Bernard Zeigler
University of Arizona**

Abstract:

Concepts in cognitive science have been developed on how the brain focuses its perceptual resources on the most active elements of its sensory inputs. Such mechanisms have been shown to explain how visual search, otherwise computationally intractable, is rendered feasible. Taking the analogy between the brain and a large scale network one step further, we have developed some distributed attention management mechanisms and studied them via modeling and simulation. The results suggest how detection of threats in ULNs can be implemented in a distributed, scalable manner.

Biography:

Bernard P. Zeigler is Professor of Electrical and Computer Engineering at the University of Arizona, Tucson and co-Director of the Arizona Center for Integrative Modeling and Simulation. He is internationally known for his 1976 foundational text Theory of Modeling and Simulation, recently revised for a second edition (Academic Press, 2000). He has published numerous books and research publications on the Discrete Event System Specification (DEVS) formalism. In 1995, he was named Fellow of the IEEE in recognition of his contributions to the theory of discrete event simulation. In 2000 he received the McLeod Founder's Award by the Society for Computer Simulation, its highest recognition, for his contributions to discrete event simulation. In June 2002, he was elected President of the Society (recently, renamed The Society for Modeling and Simulation, International.) In 2003, his autobiographical

retrospective and the evolution of the theory of modeling and simulation appeared in the International Journal of General Systems.

Changes Required to Secure the Distributed Intelligent Network of the Future
Bill Way
Bytex Corporation

Abstract:

The net.CARE system provides the critical information needed to control and manage today's complex & dynamic high-performance enterprise networks. I will present how this system has evolved from work done at NSA, DISA, and Sandia. The issues I would note are that there are different owners (stakeholders) of each network layer and intermediate transports with potentially conflicting security goals. I will also address our use of models and simulation (micro vs. macro modeling). The fact is that most simulations do not perform well in the end-case situations of the real networks, namely, congestion, buffer overflows, and interfaces that are not clearly defined. The simulation tool costs are such that they are generally used only by vendors and the models are representative of only a vendors' products. I address issues faced in providing security for the future optical networks such as GigBE, a DOD version of an Ultra Large Network.

Biography:

Bill Way has forty years of work experience in computers, supercomputers and networking. He served in a Business Development role for several high tech companies and enjoyed dialoging with almost every computer and networking company in the capacity of buying, licensing or selling technology or potential modeling and analysis. During the last twenty years he has been involved in product planning, first for Network Systems (with HyperChannel and Hippi), then for internetworking. At Network we were early leaders in packet filtering and provider of the first NSA network. Network Systems acquired Bytex, Vitalink and BusTech to fill out their internetworking line. StorageTech acquired Network System to create storage networks (SANs). Way played an active role in this process, learning from many of the founders of internetworking. Way acquired Bytex three years ago with the mission of developing broadband management and security tools. The system has evolved starting with Network Systems research for NSA and the development of the first ATM Firewall then adding the NSA research on mapping and monitoring and Sandia's effort in SNIDE. Way holds a Masters Degree in Econometrics from University of Minnesota.

Appendix 2. Key Findings and Recommendations of the Participants (GroupSystems)

8a. ULN'03 questions and responses

1. Do you feel that the requirement for flexibility leads to vulnerabilities?

It certainly can. There are numerous examples of computer programs that have added features for flexibility, e.g. shell escapes in a variety of Unix programs, that offer flexibility, but lead to vulnerabilities. Java itself can be described as the essence of flexibility, but it requires a carefully designed sandbox to control it in certain environments. {#54}

Sometimes but not always! First, vulnerabilities must be well defined with respect to "assets to be protected" and "threats against those assets". Flexibility (non-essential functionality) may or may not impact these defined "threat-asset" pairs. (Analysis of vulnerabilities without defining "threat-asset pairs" for the security of a system under consideration leads to comparing "apples to oranges".) {#61}

In theory, no. In practice, yes. It really depends on the focus of the system designers.

If your focus is on user friendliness, you may not work enough on security, especially when you have limited resources. {#70}

Flexibility in a system increases the number of potential states in which a system may find itself. At some point, the number of states becomes intractable to human security analysis (unless the system can be mathematically modeled and a correctness theorem can be proved), increasing the probability of undetected vulnerabilities. So yes, I do think that, in practice, flexibility leads to vulnerabilities. {#112}

2. Can multiple intranet protocols be compatible with the Internet?

By definition and default, they are. Most intranets support the same services as the Internet. {#56}

Yes. {#75}

Re # 75, why? {#79}

For a switch to support multiple protocols, the question is not whether but at what cost. Such switches will obviously run slower. Incidentally, if memory serves me right, there was a switch designed to support ISDN and AODI protocols. I would like to hear more from someone aware of the details. {#88}

Why would they necessarily be slower? By definition, intranets are running IP. The speed of a new TCP service depends on the processing requirements of the edge machines, {#92}

The concern was more with traffic flowing from the intranets to the Internet. The core switch that normally processes Internet packets will now have to intercept and decipher intranet packets received at its input ports that may be written in a different protocol. Thus, the core switch will run slower, relatively speaking. {#103}

Yes, if nothing else than by tunneling the proprietary protocol across the Internet, or interworking the protocol to be compatible with the rest of the Internet-attached hosts. Both of these approaches incur cost and some performance penalty (e.g., delay). For example, tunneling works for carrying "new" protocols such as IPv6 and Multicast over the Internet. {#104}

The only "core switch" that should care about the contents of IP packets would be a firewall. ATM is mostly just a transport for IP packets these days. {#113}

3. What are your thoughts with regard to ATM and ATM-Like QoS/virtual circuit switching vs. end-to-end plus store and forward?

ATM is slowly going away, so the question doesn't seem that relevant to me. QOS on the general Internet backbone has been a non-starter, because the ISPs have no economic motivation to honor such requests for externally carried traffic. {#110}

Does everyone agree that this is not a relevant question? {#139}

Telephone, ISDN, IP, ATM, and MPLS are simply names that should not consume us. We should focus on their underlying principles, learn from them, and propagate forward their superior qualities. In life, things evolve in a helical (spiral) manner. We keep coming back to the same things over and over again, every time a little better prepared, with a little better appreciation. {#141}

The question is VERY RELEVANT when framed in the sense of "connection-oriented" versus "non-connection oriented" services. Most security services require establishing "associations" that are very much like "connections", and are facilitated by a connection-oriented protocol low in the protocol stack. If there is no connection-oriented protocol below the intended security service, then the security service usually needs to "re-invent" the concept of a connection or association, in order to provide the intended security mechanism. {#145}

4. What do you feel is the role of Internet weather map (determining whether the internet is up or down)?

It can be an indicator of an economically important event on the Internet, whether it is a general slowdown as a worm massively exploits the Internet, or as a result of an attack on the Internet infrastructure itself.

It can also help a user diagnose the cause of an outage he is experiencing. {#59}

The data that is collected can be used to aid or even drive research in the Internet; minimally it can be used to validate theoretical and simulation models. {#66}

Such a "weather map" is an important but very limited tool. A user of the Internet only cares if his/her application(s) work with respect to selected destinations. Some applications require greater "connectivity" (QOS: security, bandwidth, latency, etc.) than others. Therefore the metrics by which to interpret a "weather map" are different for each user/application and also may vary over time. {#71}

The question of how to tell if the Internet is down was raised. The more general question is "how to measure the health of the Internet." This is another instance in which biological inspiration might be helpful. There are several common indicators such as temperature and pulse rate that

support a first cut assessment of health. These are global measures that can be obtained locally such as by thermometer in the mouth. The global nature comes about because of the circulation of the blood flow throughout the body. This might lead to questions such as can we develop metrics and instruments that can give quick and accurate global measures from any local site. The topology map of the Internet seems to be one such tool. It might be that a rapid model fitting method could be developed by which to extract parameters from the map, such as the exponent of scale. Then monitoring the change from average value of this exponent can give the equivalent of 98.8 temperatures. {#81}

This would be mainly useful to researchers interested in the study of the Internet. Not that useful to clients who use the Internet. {#83}

Given the economic importance of the Internet today, I think global Internet monitoring is extremely important. "Up or down" for the entire Internet is meaningless, however, detection of sudden, large-scale changes is extremely meaningful. {#93}

The Internet weather map will be very useful for financial and security (company, national) reasons. Its role will be of monitoring and forecasting (possible problems?) and feed this information back to the users. {#105}

(83) It could also be useful to determine how to provide "cure" to unhealthy parts of the Internet. If there are means of checking parts of the net that are "sick" (for instance, infected by a worm/virus expanding), shutting down a certain area could help to stop spreading the sickness. Means to determine the level and kind of sickness are required. {#108}

With reference to excellent comment 81, we may also want to publish the time interval (rate) at which information about the weather map is being collected and refreshed. This will help the user get a better feeling how much to rely on the map. The map will always be subject to a lag. The user must be made aware of it. {#115}

Alas, worms can spread worldwide in less than 2 minutes (see paper by Paxson et. al.) Any automated defense to such an attack would have to be extremely agile, and could probably be fooled into rendering a denial-of-service attack. {#117}

5. How important is privacy in the Internet?

It is quite important. For wired people, the Internet can be an important part of their lives. Their privacy on the Internet can be part of the privacy they enjoy in their unwired lives. {#63}

Privacy for Internet users is very important when it comes to personal/financial information. But the level of privacy protection should be up to the users to decide. Some Internet users don't want to give out any information, others want to give some information so that the Internet can provide the right services (movies listing, traffic & weather in a particular area, certain new products becoming available) {#73}

Clearly it is important to increase widespread deployment, especially as ubiquitous computing comes on line and more and more of people's personal lives become accessible electronically. Failure to address this will significantly impede Internet growth. {#76}

Internet users have become accustomed to a certain perception of privacy on the Internet. There is also a perception that civil liberties and privacy rights are being slowly chipped away. The main

utility of the Internet is the large number of users. If the perception of Internet privacy changes, the resulting mass migration away from the 'Net will severely diminish its value. {#80}

Privacy is very important since it must deal with ""flexibility"" just as law requires changes to deal with variabilities inherent in deciding what may be considered "right" or "wrong". I think it is important to address privacy in such a way that it can be interpreted given the unknowns of the future. {#85}

Very important. The email one sends and receives, as well as the web sites one visits should all be protected. However, this is a very complicated issue, which may require government regulation. {#90}

Government regulation won't work in the face of an international Internet. {#94}

There should be means to address both requirements (94 and 90). I would like to see government regulation in some transactions (for instance, on-line purchases), but zero regulation in private issues (email). There should be means to define intermediate levels of privacy, in which the user defines how private the communication is. {#99}

There are also the concerns of law enforcement and, for that matter, counter-espionage. {#107}

I recall an episode from Star Trek Voyager where a crewmember that suddenly expresses anger at someone is condemned to die by a zealous race of beings that happened to rule that quadrant of space. Their reasoning: your thoughts were polluted; therefore you must die even though you have not actually committed a crime stemming from the instance of anger. The question is, are thoughts private? The fifth amendment of the U.S. Constitution affirms it (as of 1990s). However, a degenerate government may, someday in the future, take a position similar to the zealous race and that will herald the end of privacy. So, privacy on the Internet is indeed very important. {#121}

6. What set of attributes of the QoS matrix make the most sense?

The QoS framework gives the impression of supporting a static design process. We should be prepared for a process that is inherently dynamic and incomplete. In software engineering, the concept of spiral development is suggestive. There might be a built-in plan for moving from one generation to the next -- even though foreseeing what the changes from one to the next might not be anticipated. {#98}

Dynamicism in the QoS matrix may be realized in two ways, as follows. The QoS parameters are multiplied by some coefficients and then summed up to yield a cost function value. While the QoS parameters are dynamic (in time), the coefficients may also be modified in time depending on the current state of the network, etc. {#124}

Availability and reliability {#126}

I do not see the difference between availability and connectivity.
Connectivity is basic. Reliability is important.
Recovery from disaster is a means to improve reliability. {#129}

The subject "QoS Matrix" seems pretty complete from a security perspective, except that the "with respect to:" column is missing. For example, integrity of user data traversing the network

vs. authenticity of the transaction entering the network? (Or of control data used to assure that it gets to the right place, etc...) {#143}

7. How difficult is it to go from local to global security?

Very hard, as they are quite different problems. It is one thing to build a wall around my town, and quite another to build a wall around every town, or even change the culture such that walls are no longer needed.

Local solutions generally involve local considerations, like cost, availability, etc. Global solutions require global changes and the economic considerations of others. Or they require global changes in attitudes. "Why can't we all just be friends?" {#65}

This is a very difficult problem because what a local group considers "secure" may not be secure to the global community. Local security implementations should result from local requirements, which probably do not apply to the global community. {#67}

It is fundamentally difficult to arrive at global security from local security. It may be that global security can emerge. In a sense, global security may have to be synthesized from local security. The synthesis itself brings up a great deal of complexity of its own (scalability, heterogeneity, etc.). Nevertheless, this may be one of the few choices we have in addressing security. {#68}

Almost impossible. One must have full control of the network to be able to make the system secure, or, to be more exact, securer. Therefore the concept of "global security" is difficult to define. {#95}

Then again, we could all agree on some general and fundamental aspects of global security. People do travel between countries and there is generally an agreed-upon norm which, when followed, keeps one out of trouble. {#128}

Agree with #128. It is very dangerous to rely on "emergent" global security precisely because without a framework it is moving a target. {#130}

Scalability of security mechanisms is the real issue. For example, one issue I am concerned about is the scalability of PKI computations and infrastructure. One would like to be able to do PK computations with less computational complexity to fit into many more corners of low-power requirements. MORE IMPORTANTLY, PK authentication (and therefore, confidentiality) techniques depend on valid, fresh certificates. The only way we have to ascertain certificate freshness is by examining a "certificate revocation list" which does not scale to a large number of authenticated nodes or entities.... We need authentication techniques that scale for use in authentication of extremely large numbers of entities in order to build secure ULNs, but these are presently unavailable! {#140}

To fully address global security is enormously difficult if there are national boundaries. Future of economy and earth itself is shaping and will like to be governed by ULN (or more accurately by its direct and indirect effects). Therefore while it is too difficult to achieve, having some known, measurable, we must strive toward whatever degree of global security we can achieve. {#142}

8. Which box in the National Strategic Priorities on security is the most interesting/urgent/feasible for research and development?

The local problems are the most feasible. The large enterprises and the federal government have the most urgent problems, but I don't see any easy answers to them. {#69}

Research is about addressing hard problems. Therefore, as the 60's flower children would say, "think globally, but act locally". The current success of the Internet is based in large part to the fact that the protocols were (more or less) designed with scalability in mind... even to network sizes that were unfathomable in the late '70s. Design for any smaller scale, and the idea could be DOA. {#87}

Most urgent: Awareness & Training for Home/Small Business users (use of internet can have dangerous/immediate consequences for naive users... and the utility of the internet depends on trust/acceptance of its use by consumers (commerce)). Financial system vulnerabilities seem to have had the least open scrutiny. Are we living in a "house of cards" that may truly fall at some moment due to someone exploiting vulnerabilities caused by layering more and more complexity on a not-well-thought-out check processing / credit card processing system? A major catastrophe in banking industry related to an Internet attack or failure could be more than devastating to our economy. {#100}

It is possible, but the people running businesses on the Internet have now had several years to build their business models and deal with a variety of attacks. Most think they have a pretty good idea of the risks on the Internet. Insurance companies are starting to write policies against hacking attacks. Of course, they are still very concerned about the Internet equivalent of hurricane Andrew. {#120}

All are urgent since by definition all are required. If I have to choose one, my choice is NCS response system.

The most feasible is vulnerability reduction system.

The most interesting is accounting for Priority 5. {#122}

I would vote for no. 3 (critical sections of the government) by which I refer to the national infrastructure that includes power grid, telecom, etc. {#132}

9. Should we rely on random and/or intelligent security given finite resources including time?

Intelligent security {#57}

Re #57, Why? {#77}

I wouldn't give up on the "intelligent design" philosophy. Can collectives be engineered? Can evolution be directed? As with school students, the development of machine intelligence can be directed, as opposed to a random walk. {#62}

Security is an engineering discipline. It requires distinct economic and cost/benefits analyses. These should not be done at random. {#72}

I think a mixture of both is needed. Random security (e.g., checking 10% of packets for their content) considers the amount of data transmissions. Intelligent security, however, can deal with "content" instead of "quantity". {#111}

Every set of alternatives should be studied from a cost/benefit point of view. Modeling and simulation can help to surface hidden costs that might not be noticeable otherwise and it might help to characterize the conditions under which an alternative is the most beneficial for its cost. This would then allow a multi-strategy approach where conditions are monitored and the best alternative is employed at that time. Of course, this itself is an alternative to be evaluated. {#123}

If one interprets "random security" as in Point # 111, (checking a random percentage of transactions), then this is really describing an intelligently designed "deterrent" rather than "random security". If one interprets "random security" as "genetically evolved security mechanisms" or the like, it is unclear to me that there would be significant gain over "intelligent security". Hmm... What do we mean by "random security" in this question? {#133}

Throwing a dart in the dark sometimes works but a scientific approach is always the better choice. {#134}

Design of secure systems needs multiple ways to address variabilities that are inherent including structure of the network itself and what is communicated across the network. {#136}

When there are limited resources, it is not practical to wait for the perfect solution -- assuring security for everything. Random security measures can significantly reduce the number of incidents given a high penalty for breaking the law! {#138}

10. Should there be a unified approach to security at all levels of classification (defense)?

No. I don't believe in "one size fits all" approaches. Highly secure implementations that may be suitable for some can be overkill for others. {#55}

My view is also no. {#58}

Re # 58, Why? {#78}

Diversity helps to improve security. Look at all the attacks on Microsoft software. They are effective because of the lack of diversity (I'm glad I use a Mac!). {#60}

It would be nice, but it is not economically or politically feasible. Those who run top secret networks wield power over those networks that are probably not available on larger, less critical networks. {#74}

I agree that diversity can help to improve security {#60}. Simultaneously, diversity can increase the difficulties in achieving security at all levels of classification. I think that the use of an integrative multi-level approach could help to improve security. Unified approaches are more vulnerable to attacks, but testing results could benefit from a common core. The best solution I see would include similar techniques at multiple levels, while keeping diversity, which would enable improvements thanks to variety. {#96}

Yes, as long as the approach offers inherent flexibility in ways of "structures" it can encourage as opposed to discourage. My focus is on an approach/methodology that can support handling competing requirements in a unified manner. {#101}

No, because different systems (or subsets of systems or networks) have differing assets to be protected and consequently different threats against those assets. Only by understanding a specific "threat-asset" context can one intelligibly analyze or design specific security mechanisms. This is not to say that security should be an afterthought rather than to be designed in from the beginning. By identifying the basic components of information assets to be protected and general threats against those assets, better-generalized tools can be designed to be inherent in network architecture, available to be turned on or configured to provide appropriate security/functionality tradeoffs. Today we lack many of the basic tools (try protecting on the basis of "need-to-know" for example.) So maybe I've argued myself into "yes" on this question? {#127}

Re # 78, one size fits all solution I believe will compromise the whole system even though only a small, unimportant system has been compromised. The same goes for different security layers. {#135}

11. What are the areas of security that are the most promising to address with modeling and simulation?

Network security/network vulnerability quantification {#53}

Analysis of response/downtime under attacks. {#84}

The effects of new routing protocols, and changes to existing protocols. For example, several changes to routing protocols and router behavior have been proposed to help quell distributed denial-of-service attacks. Simulations have been used to attempt to judge the efficacy and impact of these changes.

The behavior of routing changes to the Internet is quite non-linear, and simulations can help us understand the impacts of these. {#102}

Discovering abnormal traffic patterns. {#106}

Simulation can be used to understand the impact of attacks beyond their effect on the network. For example, cyber attacks (e.g., DDoS) have large economic impacts whose ramifications (including secondary and tertiary effects) are not well understood. By understanding vulnerabilities and quantifying them with dollars (or some other metric) that can be used to help formulate policy and priorities. {#109}

Modeling and simulation can address the potential for degradation of functioning for the common good by allowing uncontrolled security for the individual customer. For example, will security become only the luxury of those who can pay the most for it -- because with no limits on resources such security features will leave others with very little to defend themselves. Will attackers always choose the weakest target where the differential between has and have-not is easy to detect? {#114}

Prevention and management of security attacks, their counterattacks, and recovery as well as analysis and design of the security apparatus. {#118}

Point # 114 is very interesting. Attack of weakest target happens always ... think of the continuously emerging scams (internet or snail-mail... no difference) that target the separation of the elderly, gullible, and/or naive people from their money. {#119}

M&S can be used online as discussed this morning. One application is to continually probe the model for new vulnerabilities that arise as a result of changes in the network that may be arising from several sources, including new defensive mechanisms installed to correct earlier vulnerabilities. In this manner, the defenses might maintain an edge over the attackers (who are also increasing their capabilities). {#131}

M&S can be used continuously, running concurrent with an actual system so that any abnormal functioning of a system can be studied quickly through simulation. Apparently, NASA did something similar during the Apollo 13 troubled mission and was able to help the stranded Astronauts in a timely manner. {#137}

12. What subset or superset of biologically inspired principles should serve as a guideline for future network development?

Protocol mechanisms that adapt to changing threat environment {#52}

A suggested addition to the set of principles: Encapsulate the state information of the network through a comprehensive and scientifically defensible metric. {#64}

A clarification: Our classification of whether a system is continuous or discrete is dependent on the resolution of time, either ours or that of the instrument we have at our disposal. However, discrete event characterization is of greater value than characterizing a system as continuous because, today, it is amenable to more efficient simulation by digital computers. I am very interested in hearing others' thoughts on whether analog simulation will return as a strong competitor (speed-wise and accuracy-wise) of digital simulation someday in the future. {#82}

Biological systems employ a number of appropriate security approaches: defense-in-depth, reactive security when the cost of defense is high or the attacks cannot be predicted, time-to-market and other economic concerns (the first oak leaves of a new season are produced quickly, but with few defenses. The energy is switched to the production on noxious chemicals after the leafs are producing energy.) {#86}

Analog simulations are appropriate for some forms of physical systems, such as the gas and water distribution systems in cities, which can be simulated nicely with resistor networks. But future simulations will have to be digital. Consider a simulation of the operation of an entire eucaryotic cell. {#89}

I think one cannot state apriori whether a continuous or discrete approach is appropriate for this (or nearly any) domain, without first understanding what one is trying to learn from the simulation. For example, in circuit simulation, if one is trying to understand what clock rate a circuit can run, continuous models plotting voltage over time are important to determine when signals have settled, requiring continuous models. If one is trying to figure out the best organization of a cache, this level of detail usually isn't needed. Similarly, continuous models for networks work fine for some problems but not others. {#97}

In addition to the "biologically inspired principles" perhaps one should enumerate the differences between a biological ULN (brain) from an ULN that we may design for external computation/communication purposes. (Geographic dimension, functional purpose <not all ULNs process sensor data, etc.>, distributed storage for reliability/redundancy, etc.) {#116}

Structure as pointed out yesterday and communication of significant changes. {#125}

My strong claim is that discrete event abstraction is more effective and efficient for most real world systems than either continuous or synchronous sequenced (automata) formalisms. It is true that we have a tremendous legacy of writing models in continuous state transition approaches such as differential equations. Putting aside analog computation for the moment, such models are currently "solved" or simulated using time stepping techniques from numerical analysis. However, these techniques assume, in effect, that every component is potentially changing its state at every time step -- leading to tremendous computational effort that is not needed most of the time. It turns out that we can easily reformulate such models into discrete event terms based on quantization -- only significant change needs to be communicated along with the time of its occurrence. The result is that the simulator pays attention to only those components that are currently active, which could be a relative small percentage. The same principle could underlie the operation of the brain itself. Neurons are discontinuous processors and may have evolved to be efficient decision makers. {#144}

8b. Key ULN Recommendations?

1. Developing the "science" of information systems security analysis. Critical for the future.
2. Gaining acceptance for modeling and simulation as a must-use tool among "real" network developers
3. Secure protocol design approaches and validation through simulation.
4. Security needs to be addressed in the presence of other equally challenging issues such as privacy
5. Finding analogies with physical/natural systems and research their validity. Very important.
6. Addressing security at different levels while keeping diversity
7. A process governing the development of ULN is necessary to handle its many competing requirements.
8. Agile network modeling tools that are able to rapidly analyze new scenarios and phenomena that appear.
9. Developing "inherently secure architecture" that scales to large networks and does not depend on the ever more frequent patches and security updates.
10. Designing survivable, scalable and reconfigurable networks together with software which guards against possible attacks.
11. Synthesis of customizable components/sub-systems to enable evolvable nature of ULN
12. Developing a "spiral engineering" approach to ULN that has built-in cycles of adaptation based on intensive off- and on-line use of modeling and simulation
13. Developing a logical set of principles to help design and validate networks with desired attributes such as security and high performance
14. Customers and stakeholders in addition to developers, participating in the evolution and/or revolution of ULN

8c. Voting Results of ranking Key ULN Recommendations

Voting Results

10-Point Scale (Allow bypass)
Number of ballot items: 14
Total number of voters (N): 8

Issues re-numbered based on voting score

Mean

- 8.25** 1. Developing a logical set of principles to help design and validate networks with desired attributes such as security and high performance.
- 7.38** 2. Developing the "science" of information systems security analysis.
- 7.00** 3. Designing survivable, scalable and reconfigurable networks together with software which guards against possible attacks.
- 6.88** 4. Gaining acceptance for modeling and simulation as a must-use tool among "real" network developers.
- 6.63** 5. Customers and stakeholders, in addition to developers, participating in the evolution and/or revolution of ULN.
- 6.38** 6. Finding analogies with physical/natural systems and research their validity.
- 6.38** 7. Developing a "spiral engineering" approach to ULN that has built-in cycles of adaptation based on intensive off- and on-line use of modeling and simulation.
- 6.13** 8. Security needs to be addressed in the presence of other equally challenging issues such as privacy.
- 6.13** 9. Developing "inherently secure architecture" that scales to large networks and does not depend on the ever more frequent patches and security updates.
- 6.00** 10. Agile network modeling tools that are able to rapidly analyze new scenarios and phenomena that appear.
- 5.88** 11. Secure protocol design approaches and validation through simulation.
- 5.75** 12. Synthesis of customizable components/sub-systems to enable evolvable nature of ULN.
- 5.75** 13. Addressing security at different levels while keeping diversity.
- 5.50** 14. A process governing the development of ULN is necessary to handle its many competing requirements.

Number of Votes in Each Rating

	10	9	8	7	6
1. Developin	2	3	1	0	1
2. Developin	2	1	1	2	0
3. Designing	2	1	1	0	2
4. Gaining a	2	1	2	0	0
5. Customers	0	2	1	2	0
6. Finding a	1	0	1	1	2
7. Developin	0	1	3	0	1
8. Security	1	1	1	1	0
9. Developin	1	1	1	1	0
10. Agile ne	1	0	1	0	3
11. Secure p	1	1	0	1	1
12. Synthesi	0	0	2	1	1
13. Addressi	0	0	2	2	1
14. A proces	0	0	2	1	1
	5	4	3	2	1
1. Developin	1	0	0	0	0
2. Developin	1	0	1	0	0
3. Designing	0	1	1	0	0
4. Gaining a	1	1	0	0	1
5. Customers	2	0	1	0	0

6. Finding a	2	1	0	0	0
7. Developin	1	1	1	0	0
8. Security	1	2	0	1	0
9. Developin	2	1	0	0	1
10. Agile ne	2	0	0	1	0
11. Secure p	1	2	0	1	0
12. Synthesi	2	1	1	0	0
13. Addressi	1	1	0	0	1
14. A proces	2	1	0	0	1

	Total	STD	n
1. Developin	66	1.83	8
2. Developin	59	2.45	8
3. Designing	56	2.67	8
4. Gaining a	55	3.23	8
5. Customers	53	2.13	8
6. Finding a	51	1.92	8
7. Developin	51	2.20	8
8. Security	49	2.80	8
9. Developin	49	2.95	8
10. Agile ne	48	2.33	8
11. Secure p	47	2.70	8
12. Synthesi	46	1.83	8
13. Addressi	46	2.38	8
14. A proces	44	2.33	8

Ballot Items in Original Order

1. Developing the "science" of information systems security analysis.
2. Gaining acceptance for modeling and simulation as a must-use tool among "real" network developers
3. Secure protocol design approaches and validation through simulation.
4. Security needs to be addressed in the presence of other equally challenging issues such as privacy
5. Finding analogies with physical/natural systems and research their validity
6. Addressing security at different levels while keeping diversity
7. A process governing the development of ULN is necessary to handle its many competing requirements.
8. Agile network modeling tools that are able to rapidly analyze new scenarios and phenomena that appear.
9. Developing "inherently secure architecture" that scales to large networks and does not depend on the ever more frequent patches and security updates.
10. Designing survivable, scalable and reconfigurable networks together with software which guards against possible attacks.
11. Synthesis of customizable components/sub-systems to enable evolvable nature of ULN
12. Developing a "spiral engineering" approach to ULN that has built-in cycles of adaptation based on intensive off- and on-line use of modeling and simulation
13. Developing a logical set of principles to help design and validate networks with desired attributes such as security and high performance
14. Customers and stakeholders, in addition to developers, participating in the evolution and/or revolution of the ULN