SANDIA REPORT

SAND2009-6068
Unlimited Release
Printed September 2009

Approaches for Scalable Modeling and Emulation of Cyber Systems: LDRD Final Report

Jackson R. Mayo, Ronald G. Minnich, Don W. Rudish, Robert C. Armstrong

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online ordering: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2009-6068
Unlimited Release
Printed September 2009

Approaches for Scalable Modeling and Emulation of Cyber Systems: LDRD Final Report

Jackson R. Mayo
Visualization & Scientific Computing

Ronald G. Minnich Don W. Rudish Robert C. Armstrong
Scalable Computing R&D

Sandia National Laboratories, P.O. Box 969, Livermore, CA 94551-0969

Abstract

The goal of this research was to combine theoretical and computational approaches to better understand the potential emergent behaviors of large-scale cyber systems, such as networks of $\sim 10^6$ computers. The scale and sophistication of modern computer software, hardware, and deployed networked systems have significantly exceeded the computational research community's ability to understand, model, and predict current and future behaviors. This predictive understanding, however, is critical to the development of new approaches for proactively designing new systems or enhancing existing systems with robustness to current and future cyber threats, including distributed malware such as botnets. We have developed preliminary theoretical and modeling capabilities that can ultimately answer questions such as: How would we reboot the Internet if it were taken down? Can we change network protocols to make them more secure without disrupting existing Internet connectivity and traffic flow? We have begun to address these issues by developing new capabilities for understanding and modeling Internet systems at scale. Specifically, we have addressed the need for scalable network simulation by carrying out emulations of a network with $\sim 10^6$ virtualized operating system instances on a high-performance computing cluster – a "virtual Internet". We have also explored mappings between previously studied emergent behaviors of complex systems and their potential cyber counterparts. Our results provide foundational capabilities for further research toward understanding the effects of complexity in cyber systems, to allow anticipating and thwarting hackers.

Acknowledgment

The authors thank Robert Leland and Robert Ballance for access to Sandia’s Thunderbird cluster for the emulation work.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

The scale and sophistication of modern computer software, hardware, and deployed networked systems have significantly exceeded the computational research community's ability to understand, model, and predict current and future behaviors. This predictive understanding, however, is critical to the development of new approaches for proactively designing new systems or enhancing existing systems with robustness to current and future cyber threats. At the same time, basic theoretical considerations on complexity indicate that cyber systems have "emergent" behaviors that are not straightforwardly predictable. In general, only by explicitly modeling such a system at a sufficient level of complexity and then carrying out a simulation can we predict emergent behaviors with confidence. The limitations of traditional engineering approaches when applied to cyber systems have led to growing reliability and security problems in today's computers and networks, particularly exemplified by distributed malware such as botnets.

The dual role of computers as both the systems of interest and the platforms for simulation creates the possibility of extremely realistic simulations, called emulations, that directly run the real-world software of interest on an experimental computing platform. But the extreme scale of networks relevant to understanding today's cyber threats, such as botnets, makes straightforward replication infeasible even on large high-performance computing clusters. Such a cluster, however, can use virtualization technology to run many separate instances of an operating system on a single physical node. In this way, through creation of numerous virtual machines and virtual network connections, emulation allows a physical computer cluster to trace efficiently and with high realism the behavior of a much larger network of computers. The resulting tradeoff, however, is that the virtual machines must share the available physical resources, such as CPU time and memory. The virtual machines on a physical node must take turns executing via task switching. Furthermore, all virtual machines must fit in memory at once, because swapping their states to disk would have an unacceptable performance impact; thus small-footprint, "lightweight" yet realistic versions of operating systems and other software are necessary.

Such large-scale network emulation (including real operating systems, network routing protocols, and complex topology) is critical to understanding and forecasting the behavior of real-world nation-scale networks and large, distributed attacks such as botnets. While interest in such a capability is high within DARPA, the intelligence community, etc., frameworks that can scale to realis-

tic numbers (e.g., millions) of emulated nodes did not previously exist. In past work at Sandia [1], we demonstrated an emulation environment containing 5000 networked Linux instances (~ 60 Linux instances per host on an 80-node cluster) and the spread of a simple worm through that system. In the present work, we have scaled this emulation capability up to 10^6 virtualized instances using the Sandia's Thunderbird cluster. While this emulation capability is initially focused on representing current protocols, operating systems, and threats, it forms the basis for future exploratory networked environments in which novel protocols, defensive systems, etc., can be analyzed. The large-scale emulation work performed in this project was challenging primarily because various technical details for virtualized emulation of large networks had not been previously solved.

1.2 Research Goals

This project aimed to develop tools that can enable understanding of emergent behaviors in large-scale cyber systems, building both on theoretical insights from complexity science and on Sandia's unique capabilities in large-scale emulation. Complex system modeling and simulation are vital not only to cybersecurity but to other Sandia mission areas as well. Studying the dynamics of large computer networks is a particularly valuable and challenging application for advancing our understanding of complex systems.

Theoretical and modeling capabilities are needed that will allow us to answer questions such as: How would we reboot the Internet if it were taken down? Can we change network protocols to make them more secure without disrupting existing Internet connectivity and traffic flow? Or can we dynamically modify the protocols so as to sidestep a temporarily unworkable Internet – i.e., can we do the equivalent of shifting from AM to FM and become invisible to a denial of service attack? Can a quantifiable increase in Internet security be achieved by greater diversity in "ubiquitous" software and hardware implementations?

We proposed to begin to address these issues by developing new capabilities for understanding and modeling Internet systems at scale. We sought to address the need for scalable network simulation by carrying out emulations of a network with a large number of virtualized operating system instances on a high performance computing cluster – a "virtual Internet". We also wished to explore mappings between previously studied emergent behaviors of complex systems and their potential cyber counterparts.

Chapter 2

Botnets

2.1 Description

Among the current and anticipated future cyber threats that can rise to the level of imperiling the security of a nation-state, some of the most dangerously effective and difficult to combat are posed by botnets. A botnet is a large collection of hacked computers, up to a million or more, that coordinate their malicious activities using a complex communication network overlaid on the Internet. Botnets now infest the Internet as thoroughly as ants infest our houses. They are so widespread, in fact, that any attempt to discover a new type of botnet, or a new mode of botnet information transmission, results in new discoveries; just in the week of September 7, 2009, we found botnets using Apache on Linux and Google Talk for communications. When such usage started is not clear; it is only clear that once the question of a new mode of botnet operations was asked, it was answered immediately, and in the affirmative.

Still worse, botnets operate on such a scale, and in such a manner, that no single organization possesses more than a fraction of the resources needed to run one at scale. While it is known that estimates of botnet size can be off by an order of magnitude, ranging from 200,000 to 10 million nodes, there is general agreement that a minimum size is of the order of 200,000 nodes. Each of these nodes may, in turn, connect to several hundred other nodes. Finally, the set of individual compromised nodes is in continual flux; estimates are that several thousand nodes per hour join and leave a given botnet.

For the newer botnet, worm, and distributed denial of service (DDoS) attacks, which can involve millions of machines, scale is everything. Scalable simulation is necessary to truly understand the phenomenology of large networks. The U.S. Department of Defense well understands the need to simulate the large-scale behavior of networks, which is why DARPA is funding efforts to develop a National Cyber Range [8]; but even the Cyber Range is too small. Large networks such as the Internet exhibit behaviors, such as fast evolution in their topology, that emerge only at scale. Complex patterns of coordination between instances of malicious software, such as that manifested by botnets, also emerge only at large network scales. Trying to reproduce the behavior of bots or other sophisticated malware in small network testbeds has become increasingly difficult. Trying to understand Internet events and behaviors from observations alone is difficult, error-prone, and time-consuming. Just mapping the Internet topology is extremely difficult; it took months to understand what happened during the attacks on Estonia.

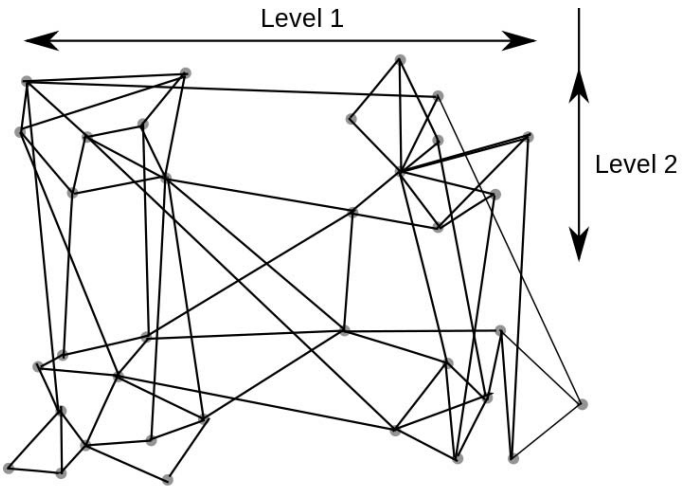

Figure 2.1. Schematic fractal network structure of a botnet using the Kademlia protocol.

A single botnet in today's world can be larger than the entire Internet was at the time the first large-scale worm, the Morris worm, was released in 1989. That worm took over many thousands of systems before it was even discovered, much less stopped. We were lucky that time: Because of the architectural diversity of the systems on the Internet, many systems remained uninfected. Such diversity is now a rarity, as organizations cleave to a single software system and even to a single version of that system. We are now much more vulnerable.

We need to gain an understanding of the behavior of botnets, which requires a system that can provide an emulation environment for botnets. We can then develop mathematical models for botnets. These models might allow us to quickly determine – from a single organizational perspective – that a botnet exists, how large it is, and how many of our organization's machines are infected. The emulation can, in turn, provide a validation capability for the mathematical models.

2.2 Behavior

All known early and current botnets have been built on the Kademlia [10] peer-to-peer sharing algorithm. Providing a binary fractal structure illustrated in Figure 2.1, Kademlia defines concepts like "nearest neighbor" and a distance measure between peers. Interestingly, this distance measure is completely aloof from the the physical location or subnet in which the peer is located. This is accomplished by generating a random 128-bit hash key that will almost certainly be unique in the bot-world and then determining the position of the peer in Kademlia space from there. The implementation of Kademlia most botnets use, called Overnet, provides the connectivity of the Kademlia algorithm as a protocol plus a means for bootstrapping newly infected nodes into the net.

The robust functioning of a botnet depends primarily on maintaining connectivity and coordination among infected nodes. The topological aspect of this – understanding the extent of connected clusters in various graphs – is a well-studied problem in mathematical physics known as percolation. In fact, when the amount of local connectivity among "marked" (infected) nodes in a graph approaches the threshold at which very large connected clusters appear (the percolation threshold), the resulting topology is generically self-similar and can be understood using renormalization-group techniques. This provides a particularly simple and relevant example of critical behavior and associated scaling laws.

The question of coordination, beyond simple connectivity, introduces the detailed entity-level dynamics of botnets simulated as agents. A simple model of coordination involves entities that undergo a quasi-periodic variation in state (representing a sequence of operational phases in the behavior of a bot) and attempt to synchronize these oscillations with one another. The amount of synchronization achieved is closely related to the problem of abstracting a reduced model, such as a Boolean network (BN), to represent the entities in a more idealized and tractable way. When entity activities are uncoordinated (not in phase), the projection to a BN will introduce much "noise" into truth tables and will lead to chaotic BN dynamics. When the topology and dynamics of the botnet model are in a regime such that entity activities become synchronized, the projection to a BN will reflect natural timesteps, and more meaningful and consistent truth-table functions, that produce nontrivial global emergent behavior. This abstraction process can be used to probe the parameters influencing the large-scale dynamics of botnets and means of countering them.

While there exists somewhere a bot-herder that exerts control over his botnet, it is in the bot-herder's advantage to make the bots as autonomous as possible. Because he does not have to attend to the bots personally, the botnet scales to enormous proportions. Probably more importantly, the more autonomous the botnet, the less likely the bot-herder can be traced and prosecuted. For both of these reasons, it follows that a useful and not too idealized model of a botnet is an array of automata. Each bot is a automaton in the array and has some pre-defined role; the array taken as a whole will exhibit an emergent behavior dependent upon, but not necessarily predictable from, the local behavior. This last observation merits some exploration and is at the crux of the reason to model botnets in the first place.

Why must botnets must be simulated in aggregate and at scale? Turing's halting problem, Rice's undecidability theorem and Gödel's incompleteness proof all state that the emergent behavior of an infinite array of automata cannot be decided ahead of letting it "run". Another way of stating this observation is that, in general, the behavior of such arrays is "irreducible": No simpler or more compact description of the system can be derived. Unlike in statistical thermodynamic systems, there is no bound that can be put on the behavior even probabilistically. Understanding the behavior of large arrays of automata is essential to understanding the behavior of botnets: From a simulation perspective, botnets are little else.

As described in Section 3.1, there is ample evidence for this irreducibility manifested in other arrays of automata – for example, the sandpile experiment in cellular automata [5] and other classical observations [11, 16].

Most efforts devoted to analyzing and diagnosing botnets are centered on analyzing the mal-

ware constituting the individual bots. Because the botnet programmers have an incentive not to reveal the mechanics of their individual bots, encryption and obfuscation of the malware makes this task difficult. Even so, if and when a complete understanding of the individual bots is achieved, this does not mean that we know what the botnet in aggregate will do. Citing the theorems above, in the general case, we need to "run" the botnet at scale before we can understand its emergent behavior.

Chapter 3

Complex System Models

3.1 Cellular Automata

Cellular automata provide an especially simple setting to illustrate the emergence of rich phenomena from basic underlying rules. Extensive theoretical and computational results have been previously obtained for cellular automata, showing that these systems exhibit a wide range of behaviors seen in the natural and manmade world [16].

A cellular automaton consists of a lattice of cells, each of which carries a definite state at any given time. The evolution of the system is carried out in discrete timesteps. As a result, a specification of the underlying dynamics of the system can be exactly reproduced in a computer simulation, provided enough memory and processing time are available. The lattice of cells can exist in a "space" of one, two, three, or more dimensions. The procedure for "updating" a cellular automaton (evolving to the next discrete timestep) is usually specified via a function that determines the new state of a given cell based on the current state of that cell and its nearest neighbors.

A well-known cellular automaton that provides an instructive comparison for malware is the Bak–Tang–Wiesenfeld (BTW) sandpile model [5], which is defined on a two-dimensional square lattice. This model represents an idealization of the complex behavior of a pile of sand, which becomes unstable when its height exceeds a critical value. In the updating rule, a cell whose "sand level" exceeds the threshold will relax by distributing sand to its nearest neighbors – potentially causing them in turn to exceed the threshold. As a result, if sand is randomly added to a pile in various locations, "avalanches" eventually occur. Depending on the exact configuration at the location and time of the perturbation, an avalanche may be localized or it may sweep over a large part of the system. If this model is run for a sufficient period of time, what is observed is something similar to a second-order phase transition, where avalanches occur on all scales available to the system, obeying a power-law distribution but appearing otherwise random.

The network analogue would be a possibly unremarkable protocol where each machine is similarly arranged on a logical grid and has a counter that is incremented when either a random event occurs or a neighbor communicates with it. If the counter reaches a specific threshold, then the machine will communicate with its nearest neighbors. Because this behavior is isomorphic to the sandpile model, this innocuous-seeming protocol will result in similar communications "avalanches" that will occur at all scales of the participating machines, including the entire net-

work. Such potentially disruptive avalanches are not "directed" in any way but are an artifact of the emergent behavior of the protocol that each participant identically adopts.

3.2 The Internet

The emergent behavior of complex systems, including cyber systems, can arise spontaneously or it can be the result of an adaptation to solve a problem. It has been found that the morphology and robustness of these two scenarios differ greatly [7]. Recent findings on the structure and dynamics of the Internet as a whole present an interesting comparison to botnets and suggest potential new regimes for network malware. The two system types can be described as follows:

1. *Self-organized criticality* is spontaneous self-organization, usually of a fractal structure – exemplified by the idealized botnet connectivity in Figure 2.1. As is well-known [11, 16], complex networks as dynamical systems can exhibit quiescent, critical, and chaotic behaviors. Here the scales present in the emergent behavior are fractal, with a self-similar cascade reflecting the scales present in the initial conditions and the structure of the dynamical network. Examples are the sandpile model [5] and the preferential attachment generator for "scale-free" graphs [2]. The latter has been proposed as a reasonable physical representation for phenomena as diverse as the Internet and the national electric power grid. A snowflake is a good metaphor for this type of emergent behavior: something that is the same at all scales and regular in structure.

2. *Optimized networks* have been selected or "evolved" by an agency outside the dynamics of the network itself. Often this agency is a "landscape" that imposes constraints or selects for "fitter" networks. An obvious example involves biological organisms evolved from simpler forms [11]. Another example involves "highly engineered" systems [7] that are manmade with optimized design characteristics.

Some controversy has erupted on these two views of complexity and the dynamical structure of the Internet. For some time, the Internet has been deemed to be a network of Type 1 above [2]. Indeed, scale-free networks were credited for reproducing the general connectivity robustness of the Internet but held out dire predictions of catastrophe because the highly connected central routers predicted by such networks implied a severe vulnerability [3]. It became clear to Internet practitioners that the predictions of router connectivity were unphysically high. But these predictions went largely unchallenged until recently [13, 15], when it was suggested that a Type 2 network (highly optimized tolerance) can reproduce newer data on the Internet and better coheres with known dynamics. Nonetheless, the newer models still exhibit a power-law degree distribution similar to the Type 1 networks above.

Beyond Type 1 and Type 2, there is a third possibility: A complex networked system could be Type 2 at one scale and Type 1 at another. This scenario has been observed in studies of large-scale computer networks [6]. It is rationalized [9] that at the level of the data center or organization, the

network is optimized (Type 2) for cost and throughput, but becomes more ad-hoc (Type 1) at much larger scales where there may not be an external organizing principle.

Malware networks such as botnets operate largely independently of the underlying Internet topology, but the same theoretical considerations can apply to their virtual connectivity and communication dynamics. Present-day botnets largely seem to exhibit Type 1 behavior, but as their designs become more sophisticated and/or an "ecosystem" of botnets leads to evolution and selection of fitter specimens, admixtures of Type 2 behavior can be expected to appear. Other potential malware types may be interact directly with the underlying Internet topology and may acquire Type 2 characteristics in this way.

Chapter 4

Emulation Technology

We overcame various technical challenges to develop a capability for instantiating a million-node virtual network on a much smaller computer cluster of several thousand physical nodes, providing the means to study large-scale emergent phenomena such as botnets. As discussed previously, the motivation for such a capability is that since there is no *a priori* way to understand the aggregate behavior of bots forming a botnet, they must be simulated. As a special case achieving high realism, they are emulated. This means that the largest possible number of discrete instances of Linux need to be running and interacting together at once on a single parallel machine.

To accomplish this, we took our lead from embedded systems design, where size and responsiveness are paramount. A special virtual machine, crafted from the "lguest" system [14] for smallest size, was created. The operating system was taken from the standard GNU/Linux distribution, pared down to less than 10 MB per virtual machine yet fully functional with the same kernel and code that all other Linux distributions draw from. Roughly 250 copies of the virtual machine and operating system can be booted and run on a single physical node. Key information on our emulation of 10^6 virtual nodes is given in Table 4.1. The successful booting of this unprecedentedly large emulation garnered public recognition for Sandia via a New York Times article [12].

The emulation can perform all of the operations that malware would be expected to perform:

- SMTP primary mail transfer agent;

Table 4.1. Parameters for emulation of 10^6 virtual nodes.

Cluster	Thunderbird
Location	Sandia/New Mexico
Physical nodes	4480
Virtual machines per physical node	250
Memory per virtual machine	25 MB
Root filesystem	RAMFS
Hypervisor	lguest x86
Linux kernel	2.6.29.2
Management software	OneSIS and XCPU
Utilities	Busybox

- web server complete with CGI scripting;
- ssh server and client;
- routing, port forwarding, and packet manipulation.

Real botnets grow partly because gullible human beings click on links directed at bot web servers that download files and infect their machines. This means that a reasonable facility has to be provided to emulate this behavior. We have chosen to use the Lua embeddable scripting language for this and other behaviors that are not represented by standard GNU/Linux software. Again, this choice is governed by size and responsiveness. Lua is a thin veneer over C and can call and be called easily from C. The Lua implementation used in this work is roughly 100 KB.

Chapter 5

Discussion

5.1 Significance

The principal motivation for developing a platform capable of running 10^6 or more instances of an operating system is to shed some light on the expected behavior of large-scale cyber systems, e.g., of a botnet as a whole. This is particularly important since little data exists on this level. Because much of a botnet is unseen and because it is established in places not accessible to researchers, data for botnet behavior in the wild is necessarily local and anecdotal. The hope is that from an understanding of the essential behaviors of bots, bot models can be constructed and embedded in a sufficiently realistic environment that will allow us to infer realistic behavior at scale.

Theoretical analysis of the structure and dynamics of botnets and the entire Internet as complex systems can also produce useful insights drawing on existing idealized models of emergent behavior. Understanding the range of emergent behavior regimes seen in cyber systems will allow not only better responses to current threats, but also better anticipation of future threats that may exploit large-scale emergent behavior in novel ways.

5.2 Future Directions

The emulation capability developed in this work will provide a foundation for new techniques to be pursued in a funded FY10–12 LDRD by some members of the present team. Extending emulation to $\sim 10^7$ virtual nodes will begin to reach the range of full-scale emulation of the computer networks of a nation-state. Much detailed information on the emergent behavior of botnets and other cyber systems is expected to be discovered using such capabilities.

This work connects programmatically to several current initiatives, including Sandia's plans for the Emulytics Roadmap and the Complex Adaptive Systems of Systems (CASOS) thrust area, as well as the DOE Grassroots cybersecurity initiative [4]. Members of the present team are involved in all these related areas and will work to leverage the results of this project.

References

[1] H. Adalsteinsson, R. Armstrong, K. Chiang, A. Gentile, L. Lloyd, R. Minnich, D. Rudish, K. Vanderveen, and J. Van Randwyk. Using emulation and simulation to understand the large-scale behavior of the Internet. Sandia Report SAND2008-7122, 2008.

[2] R. Albert and A.-L. Barabási. Statistical mechanics of complex networks. *Rev. Mod. Phys.*, 74(1):47–97, 2002.

[3] R. Albert, H. Jeong, and A.-L. Barabási. Error and attack tolerance of complex networks. *Nature*, 406(6794):378–382, 2000.

[4] R. C. Armstrong, J. R. Mayo, and F. Siebenlist. Complexity science challenges in cybersecurity. Sandia Report SAND2009-2007, 2009.

[5] P. Bak, C. Tang, and K. Wiesenfeld. Self-organized criticality: An explanation of $1/f$ noise. *Phys. Rev. Lett.*, 59:381–384, 1987.

[6] G. Caldarelli, R. Pastor-Satorras, and A. Vespignani. Structure of cycles and local ordering in complex networks. *Eur. Phys. J. B*, 38(2):183–186, 2004.

[7] J. M. Carlson and J. Doyle. Highly optimized tolerance: A mechanism for power laws in designed systems. *Phys. Rev. E*, 60:1412–1427, 1999.

[8] DARPA BAA for Cyber Test Range. `http://www.darpa.mil/STO/ia/pdfs/NCR_Qs_and_As.pdf`.

[9] J. C. Doyle, D. L. Alderson, L. Li, S. Low, M. Roughan, S. Shalunov, R. Tanaka, and W. Willinger. The "robust yet fragile" nature of the Internet. *Proc. Nat. Acad. Sci. USA*, 102(41):14497–14502, 2005.

[10] Kademlia. `http://en.wikipedia.org/wiki/Kademlia`.

[11] S. A. Kauffman. *The Origins of Order: Self-Organization and Selection in Evolution*. Oxford University Press, 1993.

[12] J. Markoff. Researchers create a mini-Internet to stalk botnets. *The New York Times*, page D4, July 28, 2009.

[13] S. Robinson. Recent research provides new picture of router-level Internet. *Computing in Science & Engineering*, 8(2):3–6, 2006.

[14] R. Russell. Lguest: The simple x86 hypervisor. `http://lguest.ozlabs.org`.

[15] W. Willinger, D. Alderson, and J. C. Doyle. Mathematics and the Internet: A source of enormous confusion and great potential. *Notices of the AMS*, 56(5):586–599, 2009.

[16] S. Wolfram. *A New Kind of Science*. Wolfram Media, Champaign, IL, 2002.

DISTRIBUTION:

1	MS 0899	Technical Library, 9536 (electronic)
1	MS 0123	D. Chavez, LDRD Office, 1011


Sandia National Laboratories