LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-TR-473496

Cyber Science and Security - An R&D Partnership at LLNL

J. Brase, V. Henson

March 14, 2011

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

Cyber Science and Security – An R&D Partnership at LLNL

Focusing the Nation's National Laboratory Capabilities
on Its Most Pressing National Security Priority

Lawrence Livermore National Laboratory

The Challenge

U.S. national security is increasingly reliant on large-scale information networks. The security, integrity, and critical functionality of our networks, and the crucial information they contain, are under constant attack. The degree of sophistication of these events ranges from widespread attack by relatively unsophisticated hackers, to the persistent and coordinated activities of organized cyber crime, to extremely complex and extraordinarily difficult-to-detect actions by nation-states. Cyber attack and cyber defense are increasingly used as tools in major conflicts –industrial, political, and military-- and this fact is clearly emerging as the pre-eminent national security issue for the next decade.

Core characteristics that make securing the operation of our networks very difficult are their growing complexity and the easy anonymity that they provide. These networks are among the most complex human creations, largely because in many ways they "evolve" through the independent actions of many, many people, rather than being "designed." We have little capability to predict or model the organization of the networks or the behavior of the traffic carried on them. This fundamental lack of understanding makes any systematic development of defensive methods and approaches almost impossible. The uncontrolled anonymity that today's Internet provides ensures that attributing an attack to its source is almost impossible; as a result there is little or no consequence for launching an attack or even repeated attacks, whether successful or otherwise. In addition, there is little coherent policy in cyberspace – in areas such as identity control, attribution, and potential deterrence. Surmounting the policy issues are at least as challenging as creating the technical capability.

National cybersecurity at the largest and most complex scales is largely unexplored. This is true of critical national governmental networks, dynamic military "command and control" networks, the infrastructure networks controlling the supply of power and water, the ".edu" networks of universities, and the massive collection of business and industrial networks loosely bound together in the ".com" realm. Years of effort focused on protecting the individual computer, local firewall, and local area net have left the nation with very limited capability to understand and mitigate the intricate workings at this extremely complex national-network level. A new focus is needed that brings the nation's leading capabilities in computational and network sciences to bear on these critical national security issues.

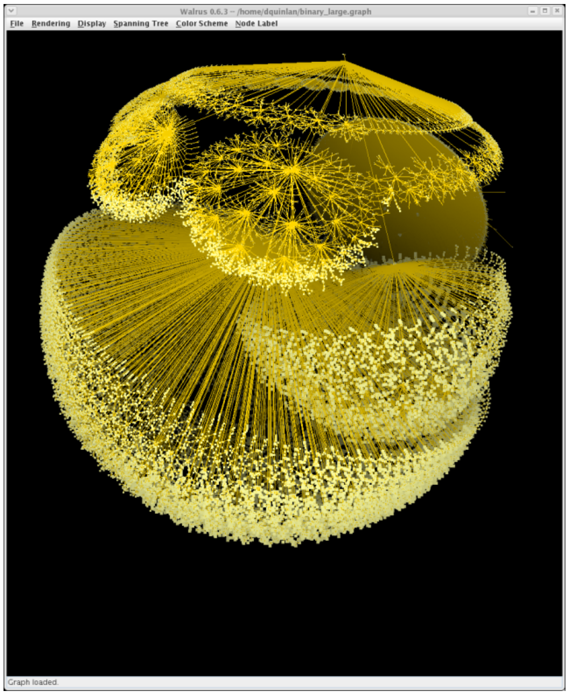
Developing solutions: Partnerships in information science, technology, and policy

The scale and complexity of emerging cybersecurity threats are beyond the ability of government or industry to handle. Even as this is written private industry is creating the next generations of computers, routers, and network hardware and software – they own the networks that must be protected. But no company or group of companies has the wherewithal for fully understanding the full nature of the threats, particularly at the highest levels. Nor do they have the capability of modeling the problem at massive scale. Effective defense against the modern, sophisticated threats requires a new public-private partnership, involving government, industry, and academia. Initially, this partnership must focus on building a sturdy foundation in both information science and policy that will enable new and proactive approaches to network security and defense.

The National Nuclear Security Administration and Department of Energy (DOE) National Laboratories can provide unique capabilities in building the technical approaches and fostering the partnerships necessary to meet this crucial national security challenge. LLNL, along with our industry, academic, and National Laboratory partners, is working to develop both the foundational science and operational technology that will enable the creation of new approaches to cybersecurity that can have near-term impact. Moreover, this symbiotic approach facilitates and sustains long-term programs delivering increasingly effective tools for network comprehension and more sophisticated weapons of cyber defense.

To lay the foundation for the work of the partnerships, LLNL has established efforts in four major areas, building, whenever possible, on expertise garnered in our fifty-plus years of experience as national leaders in computation, analysis, simulation, and national security:

Real-time cyber situational awareness. We are developing new methods of analysis coupled with next generation high-performance computing systems that together will have the ability to determine statistical measures of the activity on a network and compare them to network-activity models developed in real-time. Employing complex interplay of machine-learning and data-mining methods, this approach will allow the use of behavior-based triggers identifying when a system or network does something “unusual” – this new activity can be detected and directed to a human analyst for further evaluation. That evaluation can result in application of reactive or preventative defense measures, and can also be employed in a feedback loop for the anomaly-detection systems, improving their accuracy. In this way, the machines do the initial large-scale screening for anomalous behavior and direct human attention where it is most needed. Tools based on these approaches are being emplaced and evaluated using LLNL



Graph loaded.

Figure 1. Visualization of the abstract syntax tree of a software binary with 800,000 nodes (a small code). This representation is the basis for vulnerability analysis.

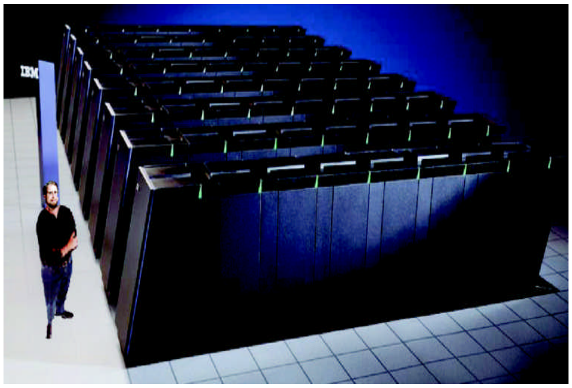
networks as a testbed.

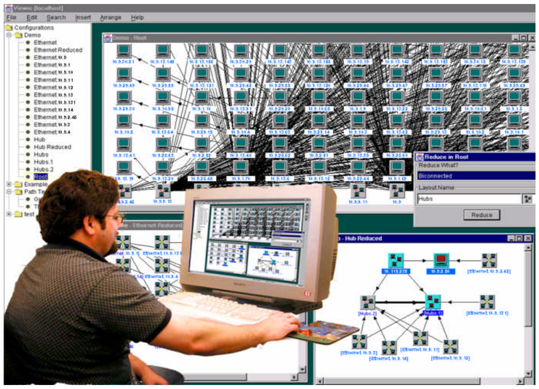
A national capability for predictive modeling and simulation of complex cyber systems at scale. LLNL and our sister DOE Laboratories pioneered large-scale simulation to solve complex scientific problems, and were instrumental in the growing acceptance of computational simulation as a third branch of the scientific method, along with theory and experiment. Simulation will be critical to testing and optimizing strategies for large-scale cyber defense that are very difficult to test on the real networks, and impossible to test at the massive scales of enterprise or national networks and, especially, the Internet. Such simulations are extraordinarily difficult to achieve, as effective models must work at scales ranging from single network packets to international communication flow, and must accurately model the complex interactions of physical network topology, routers, servers, and traffic flow, firewalls, various communications protocols, and the effects of both offensive and defensive tools and strategies. We are leveraging our experience at massive-scale physics simulations on state-of-the-art massive supercomputers to extend LLNL simulation capability to model the behavior of our cyber networks and infrastructure.

Supercomputing for deep software vulnerability analysis. Today, software vulnerability analysis is mainly performed on desktop-class computers, and most frequently depends on analysis of the source code. LLNL is developing new approaches to software analysis that use supercomputing to find and characterize vulnerabilities that are impossible to detect in reasonable times with desktop level machines. This capability will allow these tools to expand to analyze extremely large software systems.

Building the needed public-private partnership. Long-term solutions for cybersecurity will clearly require government, academic, and private components. No truly national program exists, and in striving to develop effective partnerships on which to base one a host of barriers appear. These include complex and inconsistent authorities, policy gaps and contradictions, restrictions due to classification, and complicated intellectual property laws. All these conspire to make the creation of effective partnerships daunting. National Laboratories can help to overcome these barriers by managing technology transition and scaling from industry partners to national programs, providing opportunities for enhanced academic participation, and seeding joint research ventures. Understanding and integrating policy considerations to create an optimal environment for collaborative science and technology will be important components of effective partnership.

LLNL has established a mechanism for partnership that integrates the high-performance computing capabilities of the National Labs, the network and cyber technology expertise of leading information technology companies, and the long-term research vision of leading academic cyber programs. The Cyber Science and Security Center is designed to be a working partnership among Laboratory, Industrial, and Academic institutions, and provides all three with a shared R&D environment, technical information sharing, sophisticated high-performance computing facilities, and data resources for the partner institutions and sponsors. The CSSC model is an institution where partner organizations can work singly or in groups on the most pressing problems of cyber security, where shared vision and mutual leveraging of expertise and facilities can produce results and tools at the cutting edge of cyber science.





Benefits to the Nation

A National Laboratory–Industry–Academia partnership focused on sustainable cybersecurity brings some of the nation's most modern and extensive information science facilities and the strongest technical workforce to its most pressing national security challenges. New approaches to real-time cyber situational awareness using distributed behavioral models, innovations in deep software vulnerability analysis using high-performance computing, and high-speed highly accurate simulation at extraordinary scale are critical areas that will benefit greatly from this R&D approach, leading to a new generation of sophisticated solutions. The information science and computing strength that has been developed through long-term national investment in the Laboratories can play a critical role in supporting national efforts in cybersecurity.

For more information contact

James M. Brase
925-422-6992, brase1@llnl.gov

Everett M. Wheelock
925-422-1152, wheelock1@llnl.gov

Lawrence Livermore National Laboratory
Livermore, California 94550