PNNL-17263

Pacific Northwest National Laboratory
Operated by Battelle for the U.S. Department of Energy

Transforming CyberSecurity R&D Within the Department of Energy: Getting Ahead of the Threat

D Frincke
Pacific Northwest National Laboratory

C Catlett
Argonne National Laboratory

F Siebenlist
Argonne National Laboratory

R Strelitz
Los Alamos National Laboratory

E. Talbot
Sandia National Laboratories

B Worley
Oak Ridge National Laboratory

January 2008

Prepared for the U.S. Department of Energy under
Contract DE-AC05-76RL01830

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

This document was printed on recycled paper.
(9/2003)

PNNL-17263

Transforming CyberSecurity R&D Within the Department of Energy: Getting Ahead of the Threat

D Frincke
Pacific Northwest National Laboratory

R Strelitz
Los Alamos National Laboratory

C Catlett
Argonne National Laboratory

E. Talbot
Sandia National Laboratories

F Siebenlist
Argonne National Laboratory

B Worley
Oak Ridge National Laboratory

January 2008

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

Summary

This report outlines a preliminary response from DOE researchers to the following three questions:

1 What are the key priorities with regard to cyber security research and development over the next decade?
2. What would we recommend, in terms of a program, to address those priorities?
3. How would a DOE Office of Science program in this area complement other cybersecurity R&D initiatives such as NSF's or other agency programs?

Acknowledgments

This report represents the combined effort of cyber security experts from across the nation, including people from national laboratories, academia, and private industry. The authors acknowledge the valuable inputs and efforts of all contributors:

Deb Agarwal, Lawrence Berkeley National Laboratory
Mine Altunay, Fermi National Accelerator Laboratory
Robert Armstrong, Sandia National Laboratories (CA)
Tony Bartoletti, Lawrence Livermore National Laboratory
Patrick Burns, Colorado State University
Charlie Catlett, Argonne National Laboratory
Matt Crawford, Fermi National Accelerator Laboratory
Susan Estrada, Aldea
Ian Foster, Argonne National Laboratory
Deborah Frincke, Pacific Northwest National Laboratory
Mark Kaletka, Fermi National Accelerator Laboratory
Celeste Matarazzo, Lawrence Livermore National Laboratory
Miles McQueen, Idaho National Laboratory
Leonard Napolitano, Sandia National Laboratories (CA)
Don Petravick, Fermi National Accelerator Laboratory
Anne Schur, Pacific Northwest National Laboratory
Frank Siebenlist, Argonne National Laboratory
Mike Skwerak, Argonne National Laboratory
Joe St Sauver, University of Oregon
Richard Strelitz, Los Alamos National Laboratory
Craig Swietlik, Argonne National Laboratory
Edward Talbot, Sandia National Laboratories (CA)
Troy Thompson, Pacific Northwest National Laboratory
Keith Vanderveen, Sandia National Laboratories (CA)
John Volmer, Argonne National Laboratory
Brian Worley, Oak Ridge National Laboratory

Jane Carlson, Pacific Northwest National Laboratory, Administrative Support
Bob Allen, Pacific Northwest National Laboratory, Technical Writer

Contents

About this Report

Dr. Raymond L. Orbach, Under Secretary for Science, U.S. Department of Energy, requested a response to three basic questions relating to cyber security:

1. What are the key priorities with regard to cyber security research and development over the next decade?
2. What would we recommend, in terms of a program, to address those priorities?
3. How would a DOE Office of Science program in this area complement other cyber security research and development initiatives such as National Science Foundation or other agency programs?

A grassroots community of cyber security researchers formed three groups to respond to these questions. The results are contained in the three appendixes to this report.

Appendix A

Area A – Science-based Cyber Security Research Priorities for the Next Decade

Area A – Science-based Cyber Security Research Priorities for the Next Decade

This paper provides a recommendation for the formation of a five to ten year transformational, forward-looking Department of Energy (DOE) Cyber Security Research Program, intended to move all of DOE from reactive to proactive and to enable DOE to move ahead of the threats. The paper addresses the unique cyber security challenges inherent in DOE's Open Science and Energy Control Systems environments, provides criteria for the focus and direction of research areas, and outlines a research program that would address the most significant threats and issues. Four specific thrust areas are presented in more detail; these were identified by the security community in a DOE-organized cyber security workshop and in subsequent discussions. These thrust areas emphasize the needed R&D in understanding security problems in computer systems from a fundamental level, in determining the tradeoffs that can be made between usability and security in future architectures, in security awareness and response, in human factors, federated trust, for both DOE's open science programs and energy control systems. Our overall conclusion is that such a research program is urgently needed to address DOE's current, emerging and future cyber security requirements.

Background and Program Objectives

DOE is responsible for the integrity of the nation's energy delivery systems, where cyber attacks might have extreme consequences to public health & safety and the nation's economy. In addition, DOE's vast cyber resources, its high international visibility, its mission, and its open nature renders it a prime target for hackers, cyber espionage and cyber terrorism. DOE cyber systems are continually under attack and several of DOE's cyber environments have been compromised, with a very deleterious effect upon operations, reputation, and the privacy of its constituents.

These are areas where the DOE is "behind the curve" in the area of cyber security. An immediate and aggressive cyber security program to mitigate all of these problems must be a DOE, if not a national, imperative.

Fortunately, DOE is uniquely well positioned to make a major contribution to solving the nation's cyber security problems through a program of fundamental research. DOE has a reputation, unique among federal agencies, in planning and executing large-scale scientific research. DOE and its labs have conceived and executed programs that have made major contributions in fundamental and applied physics, biology (including the Human Genome Project), chemistry, computer science (pioneering the terascale), materials science, and many others. An aggressive research program will not only address DOE's needs, but also advance the state of this critical art to the benefit of the nation. According to a recent report from the National Research Council and the National Engineering Academy, "… a secure cyberspace is vitally important to the nation … but the United States faces real risks that adversaries will exploit vulnerabilities … causing considerable suffering and damage." [NRC-2007]

The threats to different parts of the DOE complex are as diverse as the agency's mission, and improving cyber security is a complex, daunting task. DOE's open science environment poses special challenges. Some of the unique factors pertinent to DOE's open science mission are: 1) access is required to extremely valuable, centralized resources, 2) emphasis is on "big science" that can be at unprecedented scales in exceedingly complex, and sometimes multi-national environments, 3) users are numerous and highly decentralized among diverse IT settings, many of which are not well secured, 4) legacy systems are pervasive elements of the environment. Besides open science, the DOE mission has classified components requiring even higher levels of protection.

When cyber security incidents occur, they tend to be tremendously disruptive to the operational environment, they can besmirch DOE's reputation for operating trusted environments, and remediation can be extremely expensive. At the same time DOE has significant programs of unclassified international research requiring secure participation in world-wide collaborations. Malicious alteration or deletion of data could significantly impede scientific progress or cast doubt on the outcomes of experiments, but inappropriately restrictive security controls might cause DOE participation to be shunned. Furthermore, DOE has some unique cyber security requirements because its research projects are at the leading edge of technological possibility. Consequently, DOE will experience some cyber security issues and challenges distinct from the commercial sector, requiring solutions before they become commercially relevant. This combination of factors makes DOE unique in its cyber security needs, demanding fundamentally new approaches.

Immediate efforts are needed not only in securing DOE information systems, but also in developing advanced methods and concepts to secure and sustain the nation's energy infrastructure, ensuring that it remains among the most robust, reliable, secure, and technologically advanced in the world. Improving the security of energy control systems is a crucial requirement to protect our national energy delivery infrastructure.

This call to action augments and distills both the discussions that took place at the "Cyber R&D Planning Meeting" on October 17, 2007, in Washington, DC, and the *Cyber Security Research Needs for Open Science Workshop Report* that was the culmination of the DOE workshop held July 23–24, 2007 in Bethesda, Maryland, sponsored jointly by the Office of Science and the Office of Electricity Delivery and Energy Reliability [DOE-CS-Report]. That report identified seven comprehensive thrust areas for long-term cyber security research. During subsequent meetings at Sandia, at the SC'07 conference in Reno, and in Washington DC, several more complementary research areas have surfaced. This report distills those areas into four specific research programs targeted to address DOE's most critical cyber security needs.

This proposed program would create a proactive and forward-looking approach to research and development in the cyber security area from a rigorous analytical and technical basis that would stimulate new open science research directions and have a lasting impact on cyber security. The intent is for the program to be transformational as well as visionary – to move our cyber security capabilities beyond traditional "catch and patch" reaction to a proactive posture. It is crucial that the research establish a firm scientific foundation and allows broad participation of researchers, whether or not they have clearances. The output of this open program is intended to contain many elements also usable by classified enclaves and power delivery control. Fortunately, DOE has resources and expertise that render it uniquely capable of contributing to such a research agenda, including the world's most advanced computing platforms, operational environments for initial deployment at the largest scale, and unparalleled expertise embedded in its human resource base.

Research Program Criteria

A DOE cyber security research program should, on a regular basis, evaluate predictions about the relevant technologies five to ten years out and derive the associated cyber security needs and requirements. A gap analysis of the R&D programs in other agencies and industry will allow DOE to define a focused, directed R&D program to ensure the future security requirements of DOE and the nation will be addressed properly.

These decisions should be based on a risk analysis by considering the consequences of a future in which DOE does not have the tools and technologies required to address the predicted cyber security challenges.

In other words, DOE’s program should not substantially duplicate nor compete with research in other agencies and industry, but complement those efforts to ensure that DOE's particular requirements are in focus. Just as DOE’s advanced science projects are often years ahead of common adoption by industry and society, the solutions to DOE’s particular cyber security requirements may benefit society at large at a later stage. For the same reason, DOE will also accumulate unique expertise and capabilities in the advanced cyber security related research areas. Part of the R&D agenda and program should include methodologies by which these solutions can be transitioned to the larger community – providing additional benefit to the nation.

By setting targets five to ten years in the future, we will identify research areas and directions that will have a strong science orientation as opposed to a purely applied engineering effort. Many existing research programs and investments emphasize near-term solutions. While these are important, a focus on six- to twelve-month outcomes draws attention from the longer-term research needs and tends to lead to incremental rather than transformational change. Another difficulty in existing research programs is the tendency to fund research without including a path towards eventual deployment. Unless science outcomes are infused into the cyber security field in a usable ways, the problems they were intended to address will remain. Therefore, a transformational cyber security research program that focuses on longer-term goals, considers the investments of other agencies and industry, and operates in such a way that the science can be translated into solutions that can be applied, is necessary.

Cyber Security Defense Taxonomy

It is useful to categorize the elements of end-to-end architectures and the higher-level aspects that must be protected in a cyber security environment, so as to ensure that the domain is covered in an effective way. Such a categorization will facilitate aggregating research directions into the aforementioned focused areas to result in a coherent and consolidated cyber security defense R&D program. Figure 1 shows a taxonomy for this purpose, beginning at lower levels with hardware components and extending upwards to culminate in data and information. Note that cyber security can and should be implemented at each of the levels shown and in many cases, across the boundaries shown in the figure. Moreover, the areas of Middleware and Users cut across all elements, even extending down into hardware components.

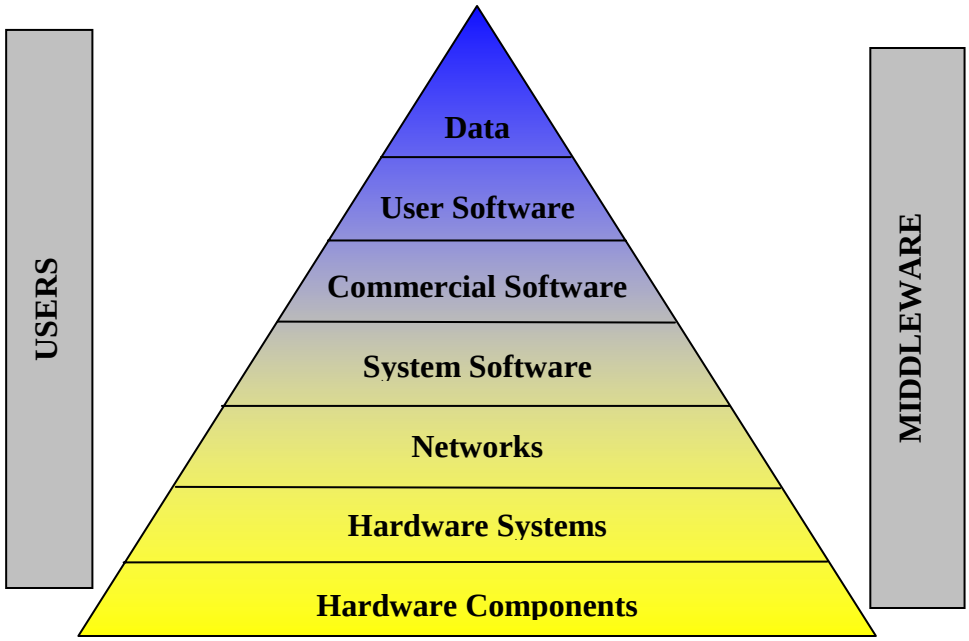

Figure 1. Cyber security taxonomy

Research and Development Focus Areas

The thrust areas from the workshop that are most pertinent to and perhaps even unique in DOE's Open Science and Energy Control Systems environments should be the focus of an initial research and development program. Specifically, these are areas where DOE has both unique needs due to the scale and nature of its environments and unique capabilities evidenced in its mission. Indeed, these are areas where DOE can make the most significant and most enduring cyber security research contributions. Securing the design and operational integrity of the exascale computing enterprises of the future is by definition an exascale challenge. Cyber security science and technologies must keep pace with evolving computing architectures developed if there is a hope to sustain scalable open computing resources and the nation's energy delivery infrastructure.

A number of research areas will be essential to both the DOE's open science and classified cyber security needs. We anticipate that a more comprehensive evaluation of focus areas will result from a series of both classified and open workshops, and forums that we recommend be held beginning in early 2008. However, we have identified four areas as critical topics and expand upon these in this section. These areas are:

- Open Science security architecture for an exascale future
- multi-layer security understanding, awareness and response
- human aspects/factors & federated trust
- intrinsically secure control of critical systems.

Open Science Security Architecture for an Exascale Future

To make significant progress in the miasma of cyber security, it is categorically apparent that cyber security must be built into systems from the ground up. This, in fact, may be the most important cyber security research direction that emerged from the workshop; the theme continued at the October meeting in a discussion of the importance of intrinsically secure or inherently secure computing. Thus, new architectures containing new hardware (e.g., TPM+ chips) need to be designed to include

- embedded cyber security monitoring and processing capabilities (e.g., on-board or peripheral cyber security processing virtualized architectures)
- hardware and software design to accommodate new cyber security analytics (e.g. processors designed for ultra-fast data comparison and analysis encompassing searches, sorts, merges, joins and pattern recognition)
- new encryption and decryption techniques.

Multi-core capability and field programmable gate array (FPGA) processing offer promise in this regard. DOE has unique, ultra-large-scale hardware platforms and associated expertise that provide the environment for processing at the required rates in DOE's environment. This research would apply at the lower levels of the cyber security taxonomy, involve interdisciplinary work between computer scientists (to include cyber security researchers), and should include close collaboration with hardware and operating system vendors.

Current developments in virtualization technologies will facilitate system management and deployment by enabling new service-based architectures that enable autonomic and self-healing systems. However, these advances will cause paradigm shifts in the way we deploy resources (Gartner Data Center conference: "…virtualization will be the most 'impactful' infrastructure and operations technology through 2012…"[Gartner-Virtualization]), and the implications on the security policy enforcement are far from clear. DOE, as an early adopter of many of these new technologies for computers, databases and networks, will have to understand the security impacts of new virtual machine technologies before the private sector. Furthermore, DOE can expect such virtual machine technologies to evolve into the management components of the power grid infrastructure, where it will also impact security policy enforcement. An interim approach would entail a development effort to deploy portions of legacy systems to address these evolving threats and needs. A follow-on, longer-term approach is to design security processing directly into systems from the ground up.

One additional concern is an expected increase in system complexity by orders of magnitude, as DOE's projects continue to push the limits of Moore's law and embrace ever-larger numbers of processors and embedded sensors. Our current management and policy tools are unable to cope with the increase of the number of entities whose lifecycle have to be managed while the correct security policies are enforced on each interaction. Virtualization technologies add additional complications as resources become ephemeral, are replicated, and physically are moved around. Further research is needed into architectures that include policy-enforcing frameworks that present administrators with human-friendly abstractions while automating and correctly enforcing interaction policies of the myriad of affected components. Certainly, as part of this research area, an essential aspect is R&D on more efficient crypto algorithms and crypto hardware solutions to ensure integrity of DOE's networks, data, and communications infrastructure.

The threats posed by hacker communities, the malware industry, and foreign political adversaries will only become more sophisticated and malignant [Schneier-10Year, Gutmann-Malware]. Research into how to better use virtualization technologies could yield tools that allow

- a finer grained access control enforcement of the physical resources like data and network
- the deployment of service appliances on thinner, feature-free, more secure operating systems
- transparent encryption of local file systems
- the trusted computing base (TCB) to extend to virtual appliances where application secrets and keys can be moved and processed.

Many of those possible applications are transformative: they allow us to break away from our current dependencies on popular but flawed operating systems and change the paradigm of what we consider to be our desktop and server.

Multi-level Security Understanding, Awareness, and Response

Cyber security today is primarily defensive, largely reactive, and labor intensive. System providers and attackers engaged in an unending “arms race,” with exploits and countermeasures in an endless cycle of co-evolution. Threats and vulnerabilities are defined and addressed only after they emerge, are then isolated, analyzed, and distilled into specific findings for which exact-matching is required for determination. Adversaries have adapted to these detection techniques by encrypting or randomizing content, employing large proxy servers as destinations (rendering most all destinations both good and bad in order to frustrate IP-blocking) and have adapted to the modern network security practice of disallowing services on unusual ports by "tunneling" malicious command traffic and data exfiltration within the standard service protocols. Progress in such a cycle is incremental and invariably temporary; thus notions of assurance or quantitative risk assessment are short-lived and fragile. More flexible and intelligent "behavior-profile-based" detection methods are needed.

Concurrently, DOE information systems are distributed and based on commercial technologies from hardware and firmware through middleware and application software, with each interdependent layer introducing potential for vulnerability. Likewise, mission-critical hardware and software systems for energy and other critical infrastructures have become increasingly complex and rely extensively on commodity hardware and software components. The DOE carries out its science mission through multidisciplinary teams comprising employees, contractors, and collaborators from other agencies, universities, and countries with a variety of security postures and interests that are not always aligned. Similarly, the information resources that agency teams require are located both within the DOE complex and at multiple laboratories. The complexity and scale of this infrastructure is such that component or systematic failures—software errors, human errors, security vulnerabilities—are inevitable. This is particularly true given the high reliance on commercial components, each of which is managed via a constant series of updates and patches to address the latest vulnerabilities. Today’s information systems are inherently distributed and complex much like an ecosystem—failures in such systems are the steady state, not the exception. Security architecture must address the steady state.

Similarly, the information resources that agency teams require are located both within the DOE complex and at multiple laboratories. The complexity and scale of this infrastructure is such that component or systematic failures—software errors, human errors, security vulnerabilities—are inevitable. This is particularly true given the high reliance on commercial components, each of which is managed via a constant series of updates and patches to address the latest vulnerabilities. Today’s information systems are inherently distributed and complex much like an ecosystem—failures in such systems are the steady state, not the exception. Security architecture must address the steady state.

A scientific approach, examining fundamental assumptions and architectures, is necessary in order to transform cybersecurity into a proactive discipline. Such an approach has the promise to deliver systems that are capable of anticipating and effectively addressing vulnerabilities that arise from the inevitable human, hardware, and software failures endemic to complex systems. Consequently, a science-driven approach to security must focus on *understanding* and *awareness* that inform *response*. Benefits of a science-driven approach to security include better understanding and quantification of risk, improvement in the ability of system components to detect and respond to failure or potential vulnerabilities, and an overall information architecture that provides security and assurance.

Security awareness constitutes the abilites to 1) understand the current state of the elements that make up a security domain, including systems, objects, humans, and data, 2) infer the general security level of the domain by combining the individual state information, and 3) develop response and containment actions based on the level of domain security. The special needs in DOE's open science environment make addressing the security awareness properly through research a difficult problem. The open science environment is complex: researchers from autonomous security domains collaborate, share access to remote instruments and resources, and move enormous data sets across different laboratories and even countries. Thus, elements that affect the security of a domain are spread throughout several autonomous domains. For example, a malicious user who has broken into a security domain may be detected by using local monitoring and detection tools. However, the local tools become ineffective in alerting and informing other security domains against the attacker, yet the active participation of these other domains may be necessary to thwart the activity. Even more difficult, proactive approaches such as active intervention and elimination of the threat may require cooperation as well; how this can be accomplished is not yet understood. Although there is ongoing research in this area, existing approaches are limited to the perspective of a single domain. The challenge we face in DOE's open science environment is the fact that we live in a collaborative and open environment, and thus must interoperate across multiple, autonomous and heterogeneous security domains.

An aspect of this research area focuses on managing and creating security awareness and the capability to respond (or proactively intervene) for open science environments at several different levels: 1) the network level by focusing on intrusion detection and denial of service tolerance, 2) the system level by analyzing the human actions on systems and on state changes of system objects, 3) data level by analyzing and characterizing the data sets, linking the dots, and enabling security-data sharing 4) the human level by creating a trusted link between and among human operators and automated tools. Characterization of human threats using signatures to facilitate early warning and detection and predictions also can trigger actionable behaviors to mitigate vulnerabilities.

Security awareness is not limited to inferring the current domain security, but also taking appropriate *response* for a change in the domain security. This would require automated response and containment tools that can eliminate human intervention in order to reduce response time. Continuing with the above example, after a security domain is attacked, the other domains that may be affected must be automatically informed about the attack so that they could prevent access from this attacker. The security awareness techniques described above each play a role in this scenario to detect a threat proactively. The response and containment research enriches security awareness by ensuring that appropriate security mechanisms are in place ahead of or just in time. The challenges in this area are numerous: scale, speed, and multi-domain nature. New techniques in machine learning, control theory and group dynamics are needed for this research direction.

A portion of this research area should be devoted to development of a flexible modeling and simulation (M&S) test-bed capability to understand impacts and gain insights about the usability of policies on systems used for open science and open science practices, the development of methods and metrics to

assess audit policy implementation for correctness and usefulness, and the development of observable human system and network behavior signatures as early warning offensive and defensive indicators of vulnerabilities. This M&S capability would be proactive in nature, for example addressing *how proposed policies impacts security usability prior* to their implementation as mandates in real world operational contexts.

Usable security is an emerging research field, and was explicitly highlighted in [NRC-07] as a critical technology for promoting deployment of security technologies; participation in this area of research will be increasingly important to DOE in the future.

Human Aspects & Factors and Federated Trust

"In the Bentham calculus of protecting our systems, networks and data, the user is often forgotten, ignored, or even neglected, sometimes profoundly affecting productivity and impeding open science discoveries." - from the Human Factors session of the Workshop.

Painful experience has indicated that human factors are often the weakest link in any cyber security environment. DOE is unique in this aspect of its Open Science environment. Users of DOE open science systems are vast in number, exist in highly distributed, unverified cyber environments, and have access to extremely costly, unparalleled resources. This environment represents the "perfect storm" of challenges in the area of cyber security. Nowhere is the need greater for improved access, control, and cyber security than in DOE's Open Science environment.

New, quantifiable trust frameworks and the tools to model, simulate, and analyze trust in open science environments must be explored, devised, implemented, tested, and refined. Cost-risk-benefit analyses for cyber security trust must also be developed, tested, implemented, optimized, and periodically refreshed to address threats and vulnerabilities as they continue to evolve and emerge. The research must address the challenges of an open science community that exists in a highly decentralized environment, involving many sites, each with different policies and infrastructures for trust. New cyber security discoveries include novel techniques for trust negotiation among systems and users. Some of the common research elements in this area are the development of a quantitative tool for assessing trust, development of assessment and profiling tools to duplicate or simulate environments upon which security may be implemented and tested, and development of techniques for evaluating and fine tuning how trust and security policy can best be implemented in multiple, distributed, complex systems and architectures.

The challenges involve extending trust across levels of the taxonomy and maintaining cyber security when transitioning among virtual environments. Better, smarter federated systems for authenticating users and authorizing access to varying classes of DOE assets will facilitate secure access to DOE assets. It might, for example, be a policy that protected Personally Identifiable Information (PII) be stored only once, at a user's home location, in encrypted form, and never be exchanged with or stored on DOE systems. This would limit identity theft and preserve privacy, but requires a new model for a web of trust to be developed and implemented. A research program in this area will encompass both legacy via existing webs of trust and new systems via emerging webs of trust. DOE is uniquely positioned both in its need for solutions in this area and its environment for defining, deploying, testing and refining solutions in this area.

Areas in which new cyber security discoveries are required include novel techniques for user privilege negotiation among systems, user authentication, user authorization, and possibly remote configuration of cyber resources in decentralized environments. The benefits of this research will be better cyber security, easier accessibility to DOE resources, and distribution of the effort required to implement cyber security,

allowing the burden of user enrollment and authentication to be assumed mostly by the users' home sites, rather than solely on the broad shoulders of DOE. The research is expected to take 3 to 5 years for initial efforts (federated authentication and authorization), and 5 to 7 years for federated dynamic configuration and management in remote environments. All areas of the cyber security taxonomy, especially users and middleware, are involved, and new approaches and algorithms from the field of computer science will be required. New software and possibly hardware also are expected to result from this research.

Intrinsically Secure Control of Critical Systems

DOE and its laboratories have a responsibility to ensure that critical systems are controlled in a secure manner. DOE has a responsibility (shared with the Department of Homeland Security) to ensure that systems critical to meeting our nation's energy needs (including power generators, electrical grids, pipelines, and refineries) can be made secure from attacks, including cyber attacks. DOE also has a special responsibility to ensure that nuclear weapons, which it designs and produces, are secure from attack and misuse.

Much of the proposed security research is applicable to both of these areas as well as to open science and will be tested, productized, and implemented in these environments that have their own unique implementation nuances. Indeed, much of the cyber security research should be conducted in liaison with the Office of Science, the National Nuclear Security Agency, and the Office of Electricity Delivery and Energy Reliability, so as to realize maximum benefit and quickest time to deployment in these critical sectors. Since control systems in general, and energy control systems in particular, are often integrated with information networks, joint investigation of vulnerabilities and research to mitigate them is critical.

Several areas of the proposed research are applicable to control systems where the impact of system failure or a breach of security would have far-reaching national and international consequences. In particular, template architectures for control systems including models of survivability, designs for graceful failure (controlled degradation), and improved support for human intervention are imperative. The research challenges are numerous, including: the distributed, heterogeneous nature of systems and system components; how to quantify, measure, and evaluate survivability and trustworthiness with respect to cyber and physical threats; how to identify and prioritize failure and degradation; the requirement to maintain a high level of service during an energy systems incident; and the need to avoid high-consequence failures (nuclear weapons and nuclear power plants).

Other areas of the proposed program address the gathering, logging, distilling, anonymizing, and sharing of threat data. Control systems involve a multitude of private sector and public sector organizations, many of which are not motivated to take preemptive precautions due to return on investment constraints. The research challenges are numerous, including

- the distributed, heterogeneous nature of systems and system components
- how to quantify, measure, and evaluate robustness with respect to cyber and physical threats
- how to identify and prioritize incident response, including factors of cost
- how to quantify and predict responses to operator interaction
- how to enforce cyber security in the face of real-time requirements
- the requirement to maintain a high level of service during an incident.

Conclusion & Next Steps

DOE's cyber security workshop in July 2007 resulted in broad recommendations for a research program. The authors of this white paper strongly concur with those findings and believe that a progressive cyber security program is urgently needed to address DOE's cyber security requirements over the next five to ten years. The workshop report enumerated a number of specific thrust areas for the program, while subsequent discussions have added additional complementary topics; an important subset of which is presented in this paper. All these findings provide an excellent starting point for the actual realization of a focused DOE Cyber Security R&D Program, and we offer energy, commitment, and assistance in the process to bring such a program to fruition.

Contact Information

Frank Siebenlist, Senior Security Architect
Argonne National Laboratory
franks@mcs.anl.gov
408 656-6787

Ed Talbot
Sandia National Laboratory
etalbo@sandia.gov
925 294-1225

Charlie Catlett, CIO
Argonne National Laboratory
catlett@anl.gov
630 252-7867

Don Petravick
Fermi National Accelerator Laboratory
petravick@fnal.gov
630 840-3935

Deborah Frincke
CyberSecurity Chief Scientist
Pacific Northwest National Laboratory
deborah.frincke@pnl.gov
509 375-3969

Tony Bartoletti
Lawrence Livermore National Laboratory
bartoletti1@llnl.gov
925 422-3881

References

[DOE-CS-Report] DOE. 2007. *Report of the Cyber Security Research Needs for Open Science Workshop*. U.S. Department of Energy, Washington, DC. Accessed December 12, 2007, at http://www.sc.doe.gov/ascr/Misc/CSWorkshopFinalReport.pdf

[Gartner-Virtualization] Harris, D. December 3, 2007. "The End of IT as We Know It ... Thanks, Virtualization." *Grid Today*, http://www.gridtoday.com/grid/1918476.html.

[Gutmann-Malware] Gutmann, P. Undated. "The Commercial Malware Industry." Accessed December 12, 2007, at http://www.cs.auckland.ac.nz/~pgut001/pubs/malware_biz.pdf.

[NRC-2007] Toward a Safer and More Secure Cyberspace, National Research Council and National Academy of Engineering, The National Academies Press, 2007.

[Schneier-10Year] Schneier on Security: Security in Ten Years, http://www.schneier.com/blog/archives/2007/12/security_in_ten.html

Appendix B

Area B: Structure and Components

Area B: Structure and Components

There can be no question that securing cyberspace is of the utmost priority; it is not even a matter of trying to act pre-emptively because the attacks are daily, growing in number, and growing in sophistication every day. The nation in general relies on computers and the Internet for everything from simulation to control. DOE, in addition to information on the newest advances in science and technology, controls a stockpile of nuclear weapons data; its vulnerability is correspondingly greater and more critical. Significant resources need to be committed to the defense of our cyber-resources and the protection of our computing assets, we also need to develop a serious, long-term, and broad program to build the foundation for continued security. In this paper, we will address these needs and propose a structure to manage and advance such a cyber-security program.

1. Purpose

a. **Cyber security:** Cyber security has many facets, from protecting computers and data from theft and attack to ensuring that time and resources are not bound up in unsolicited or dangerous material. We need to cover all bases without interfering with ease of use or erecting barriers to sharing and learning that only hamper legitimate work while offering little or no protection from organized attackers. Speed bumps and stop signs on the information superhighway will only bother the user and never affect the determined intruder.

b. **Secure resources**: When the Internet was first conceived, few could foresee the immense opportunities for mischief, much less malevolence. Cybercrime is so widespread and takes so many forms that users are becoming wary of using the resources even as many applications migrate to the net for convenience. We need to develop means for making use of the network more secure and reliable, and thus make users more confident.

c. **Maintain open computing and classified computing** Cyber security takes on an added dimension when applied to the DOE with its mix of open computing and classified work, with its need to use the best scientists and engineers, regardless of citizenship in the open, and the concurrent need to provide the cleared scientists with the best and best protected resources. Open computing and open source software is useful for rapid and multi-perspective improvement, but it also exposes all of the flaws and weaknesses for those whose job it is to find backdoors. Balancing these needs, these conflicting priorities must be the primary consideration in the design of this program. And, so shall we make it our top priority.

d. **Build sustainable infrastructure**: Cyber security is not a matter of patching, but a long term effort to establish trust and to limit if not prevent unauthorized usage while not hampering legitimate work nor escalating minor use infractions into time consuming incident reports.

2. Goal

a. **Matrix, not pipeline**: It is widely believed that research and development define a 1 dimensional continuum from pure theory at one end and deployment–engineering at the other. While this view has merit, it is more informative to consider science and

application as orthogonal dimensions, as in Fig.1. To deepen the resource pool for cyber security, this second view has definite advantages. It increases the flexibility of lines of communication and establishes a structure without setting up hierarchy or competing value systems. In the linear mapping, some derive comfort in staying in the science end, while others prefer to reside in the product area at the other end. The multidimensional view increases the opportunities for interaction and permits greater flexibility in planning. The DARPA programs are based on the more old-fashioned idea-to-product pipeline model; it does deliver products, but the science and foundations are abandoned with each product and do not become part of an infrastructure or a an institutional resource. With a problem as important and protean as cyber security, we cannot afford this narrow view.

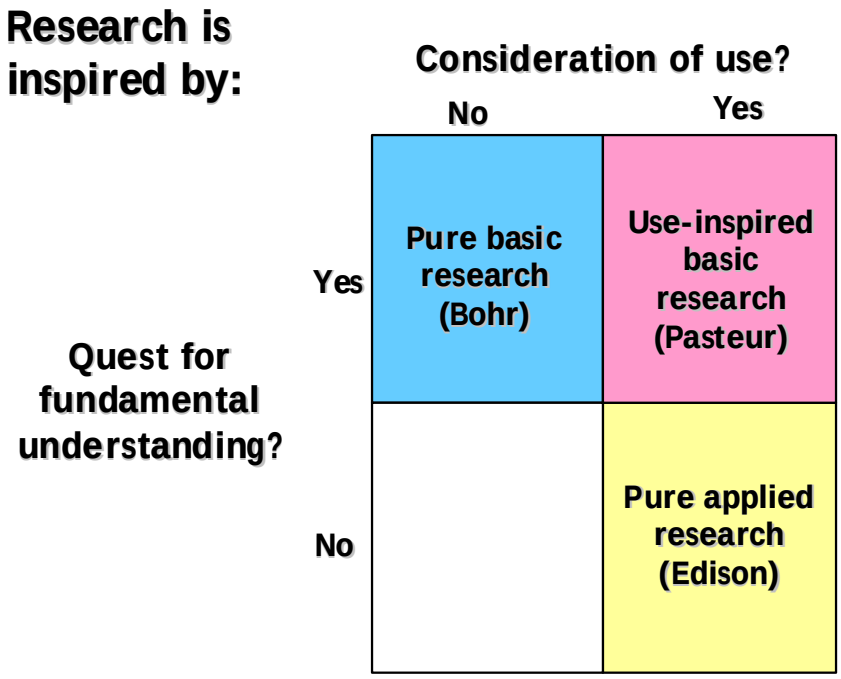

Figure 1. The Research Matrix

(Adapted from *Pasteur's Quadrant: Basic Science and Technological Innovation*, Stokes 1997.)

b. **Broad Science Basis**: Cyber security is not just a matter of plugging holes or building walls; it touches upon every aspect of computer design, technology, social behaviors, knowledge discovery and management, and user awareness and education. The DOE program must not only nurture work in judicious proportion across a wide spectrum of sciences, it must help to develop a strong infrastructure that will organize the various thrusts and establish standards for professionalism, education and credentials, most likely in connection with a fellowship program like that in High Performance Computing. The SciDAC program provides an excellent template for the construction of a broad yet end-directed research program that meets the needs of the DOE while advancing science in the most fundamental manner without sacrificing security.

c. **Integrate bidirectionally front line ↔ research**: Instead of the DARPA model where a single grant would cover a project from idea to delivery, the proposed Cyber Security research program will let groups maintain their specialization and focus, relying on the program infrastructure for hand-offs and interaction. The program management

will be key to the success, serving as messenger, guide, planner, reviewer, and most importantly, recruiter–advocate. The best example would be the aptly named "technology evangelist" at Apple.

d. **Balance the competing needs of open science with the secrecy demanded by the adversarial nature of cyber security**. We must realize that all work that touches on cyber security is under close scrutiny from those who wish to breach our systems. The tension between the discussion and sharing so essential to good science and the need to keep not only results but also priorities and research needs closely held is not new; the mathematics and cryptography communities have long realized the problem. It would be naïve and wrong to ignore this issue in the design of a comprehensive open science research program for cyber security. For this reason especially, we will advocate deviating from the SciDAC model to include extra groups to review and guide the research.

e. **Act as a proving ground or testbed for best practices in cyber security**. We hope that one of the fruits of this program will be to establish a high standard for computer use and protection that will have wide general use and acceptance. More so than the scientific goals of SciDAC or the overall DOE commitment to greater acceptance of supercomputing, the research and results that will arise from this program will be of immense value to every aspect of internet and computer use. We hope to lead by example as much as by report in this critical fight.

3. Priority Research Directions and Management Timeline

The Priority Research Directions (PRDs) are if nothing else, comprehensive; yet like all lists, a simple enumeration fails to capture the true topology of the cyber security space. It is vital that we not splinter or stovepipe the research so early in the game; by acting as a centralized funding mechanism, this program should also function as a clearinghouse and forum, increasing collaboration and cross-pollination as often and as actively as possible, via meetings and the direct contact of the program managers with each other and the wider community of research and systems administrators manning the front lines of the cyber security struggle. Because of the somewhat unique need for keeping data and methods internal that comes with all cyber security research, we cannot accept leaks from this program any more than we can accept them from the data we are trying to protect. It is all too obvious that hackers, both freelance and state-sponsored share knowledge of exploits and vulnerabilities; we must take care not to make it easier for them to learn of our methods and interests. Page rankings and spam detection rules are closely held; this program should be no less careful to protect its intellectual assets from prying eyes and roving bots.

a. **Taxonomy–ontology of needs**: The first goal must be to show the true and complex structure of the needs and research thrusts of cyber security. And, not in merely the sense of taxonomy and ontology, but also in view of the program managers and advisory panels. One of the strengths of the community is its breadth and size. We must coordinate this deep pool of intellectual capital and harness it to the task at hand. The obvious parallel is the Manhattan Project with its calculated mix of brilliant theorists and proficient experimental scientists.

b. **Project Centered Management**: Management, always key to the success a program, plays a greater than usual role here. Unlike most other scientific endeavors, the landscape here is constantly shifting, more like a chess tournament than a puzzler. Management

must take responsibility for harvesting and sharing information, for forging links across disciplines and projects and for guiding research as needed. After all, the structure of the program is essentially that of the management infrastructure, and thus, it is they who will be most able to push the program from successful to exemplary.

c. **Rolling 1, 2, 5 year plans:** The constantly morphing nature of the cyber security threats demand a commensurate flexibility in timelines, grants, and levels of effort. Some of the more successful goal directed research programs have been based on rolling near-,mid- and long- term goals; it seems appropriate to emphasize this for the cyber security effort. Likewise, there have been programs that have made the potential of a team nearly as important as the actual work proposed, realizing that changes in direction and scope can be cued from without as well as within. Cyber security needs to incorporate a wide variety of interests.

d. **Handoffs, phase-outs, startups**. The flip side of a flexible time line is the realization by all involved that project and work efforts have a lifetime and a life-cycle. The program should take an active role at all stages of development; as some projects spin down, plans should be made so that the knowledge is not lost, the resources not archived, the skills not buried.

4. Communications

If the program structure and management are designated as the chief communicators within the program, one cannot downplay the need for multidirectional communications. In situations where some information must be closely held and some widely shared, it will naturally fall to the managers to impose discretion as needed and to inform as desired. The pipelines should include: upstream from researcher (both current and putative) to management, downstream from users and management to project leads, including feedback to guide, not just assess progress, and most importantly, across projects.

5. Documentation

Some of the communications will be oral and interpersonal (see above), but the bulk of the visible results will be in papers, both peer-reviewed and status reports. In the fast paced universe of cyber security, timeliness is a paramount virtue. We also favor a new measure of full disclosure to inform the community of both successes and roadblocks. In that spirit, every effort should be made to regularly update the priorities and roster of promising avenues. For the sake of security in all senses of the word, some of this information will be publicly posted, while others will exist in a more secure form.

6. Open vs Closely-Held vs Classified

Cyber security is not to be restricted to protecting the classified data of the DOE and the critical infrastructure; we are all at risk of crippling attacks by both the merely malicious and the dedicated agent. Under this unified but partitioned umbrella, we should design a program that attacks common problems in a unified manner while leaving room for handling special needs and special situations. There are many surrogate problems that can be presented to the open research community that will in no way compromise or even inform enemies of our plans and status. We suggest once again joining in with industry and the general internet community in solving

problems of common interest using analogous data sets which come from the outside but present many of the same features and problems that we encounter.

7. Infrastructure: As Important as Research

One further difference between this proposed program and SciDAC-like programs is that first and foremost this program is aimed at moving the results of research into actual implementation and deployment. To do so means developing an infrastructure for software and systems that will allow for testing and proving and, later, plug and play. Allowance and support for the development of such an infrastructure must be an integral and vital part of the program, along with a suite of calibrated test sets and scenarios.

8. Conclusion

The goal of this program is to place the study of cyber security on a firm and scientific footing, and to forge a community of disparate elements united by a common goal through a strong, well funded and consistent research program.

9. Contact Information

Richard Strelitz
Los Alamos National Laboratory
strelitz@lanl.gov
505 665-7746

Miles McQueen
Idaho National Laboratory
miles.mcqueen@inl.gov
208 526-5872

Charlie Catlett, CIO
Argonne National Laboratory
catlett@anl.gov
630 252-7867

Ed Talbot
Sandia National Laboratory
etalbo@sandia.gov
925 294-1225

Deborah Frincke
CyberSecurity Chief Scientist
Pacific Northwest National Laboratory
deborah.frincke@pnl.gov
509 375-3969

Appendix C

Area C – Overview of Synergistic Programs and Research Directions for the Department of Energy

Area C – Overview of Synergistic Programs and Research Directions for the Department of Energy

Introduction

The computer science research community has been actively engaged in cyber security research for the past 30 years. In the past five years, there has been a flurry of computer security research owing to the "importance of cyberspace to nearly all aspects of national life" [NRC-2007]. Some of these research agendas are being set based on internal agency needs and missions, others on general research needs identified by the community, while still others are based on documents outlining sweeping programs, such as the *National Strategy to Secure Cyberspace* [White House 2003]. Additional reports on research emphasis areas have been developed over recent years, including the NITRD Cyber Security and Information Assurance Working Group report, *Federal Plan for Cyber Security and Information Assurance Research and Development*; and *PITAC Report to the President: Cyber Security a Crisis of Prioritization.* Presently, cyber-security research is being actively sponsored by all of the major U.S. funding agencies. DOE has unique cyber security requirements that are not currently met by existing R&D or commercial activities, and unique talents that speak to the ability of the agency to devise a transformational research program. As that path is explored, it will be important to ensure that the DOE R&D program complements existing programs, and is in collaboration with and leverages other agencies (and research). To that end, this document summarizes some of the agencies and programs that should be considered. We incorporate this both in narrative form in the next section, and tabular summary in the Crosswalk Table to be provided in a separate document.

An important consideration for this program is the need for both classified and open aspects of the research. As discussed in the DOE Cyber Summit held at Sandia, some elements of threat identification cannot be discussed in full detail except within environments that are appropriately secured. However, advancement of cyber security research as a whole, and specifically for the open science activities within DOE, requires employment of the broadest possible research community. It is therefore critical to provide mechanisms for transitioning research questions (and some outcomes) from the classified community into the open community, as well as for transitioning the open community results into the classified realm, for protection of those systems. We recommend continued discussion in this area early in 2008, and this report includes a summary of some of the questions that should be considered.

Furthermore, a vehicle is needed to provide support for transitioning scientific advancements into general use. Too often, good research is performed but does not enter into practice. This occurs for many reasons: lack of sufficient market to support commercial development, lack of sufficient depth in an area (the research may be exploratory only), large scale problems that require numerous researchers working together for long periods of time, and lack of availability of test data to permit examination of theories. The DOE R&D program should consider the need to transition science into practice, and support very large scale research efforts as well as smaller ones.

Using the Cyber Security R&D Crosswalk Table, one can identify areas of common interest addressed across funding agencies and sponsors, as well as those areas that are gaps. Gaps emerge for many reasons; sometimes these occur because a given research need is unique to specific mission space or agency's requirements. Alternatively, they can emerge when an agency has a different perspective on the need or performance requirements (e.g., many agencies invest

in improving performance, but the sensitivity of the instrumentation in DOE is unique, making the performance needs more stringent). It is recommended that early in 2008 the research emphasis areas identified by the development of a DOE Office of Science R&D Roadmap/Vision be reviewed in the context of the broad view of activities conducted and evaluated by other organizations. A consensus view of the gaps from these two different perspectives will be important to establishing a program that is both complementary and relevant to the DOE, and would be helpful in identifying partners.

Synergistic Programs

This section outlines several programs that have made longstanding investments in cyber security research. It includes examples of many existing programs, though it is not intended to be comprehensive. A wide variety of agencies are involved in these programs:

- National Security Foundation (open research)
- Defense Advanced Research Projects Agency (open and classified)
- Office of Naval Research (open and classified)
- Intelligence Community (IC) and Other Department of Defense (DOD) (open and classified)
- Department of Homeland Security (DHS) (open and classified)

These programs range from basic science to applied research. Some of the programs have strong classified programs as well as open programs (and in those cases details have been removed for this unclassified report). DOE researchers are frequently either participants or cognizant of these programs, and those relationships will assist in coordinating between them.

The character of the research produced by these agencies varies considerably, and the nature of the relationship that a DOE program might have with each varies as well. For example, an agency focused on basic research teamed with an agency focused on deploying applications would be an ideal partnership to create new knowledge and rapidly convert that knowledge to hardware and software in the field.We recommend that a variety of interactions be considered and explored early in 2008, so that the DOE program can be focused on DOE missions, effective in outcome, and integrated with other efforts.

A discussion of individual (example) programs follows.

National Science Foundation (NSF)

The primary funding vehicle for cyber-security research at NSF is the *Cyber Trust Initiative*, Program Solicitation 07-500. Cyber Trust has focused on research related to security at the operating system level and at the user level (including human-computer interaction research to improve security). Cyber Trust has also investigated secure routing, and trustworthy wireless network security. Additionally, extensive research is being done on formal methods, network intrusion detection, denial of service mitigation and worm/bot-net propagation. Finally, there is a small group of researchers investigating the intersection of economics and network security.

NSF Center Funding and Other Large Scale Efforts

NSF Cyber security projects also include center-level investments, such as TCIP (Trustworthy Cyber Infrastructure for the Power Grid), TRUST (Team for Research in Ubiquitous Secure Technology), and STIM (Security through Interaction Modeling). There is additional NSF investment in joint industry–university alliances and REU (Research Experience for Undergraduates) programs. NSF grants tend to focus on basic research. An additional opportunity for NSF collaborations may involve the Global Environment for Network Innovations (GENI) program. Town hall meetings called to investigate GENI have included discussion of security requirements, and ability to support security research [GENI-2006]. The GENI town hall meeting forums, which were facilitated by NSF and the Computing Research Association, are potential models for DOE program development.

Cyber physical Calls within NSF

Other related recent NSF calls include *Software for Real World Systems (SRS)*, NSF 07-599; *Cyber Enabled Discovery and Innovation (CDI)*, NSF 07-603; *Emerging Frontiers in Research and Innovation (EFRI-2008)*, and NSF 06-596, and *Computer Systems Research (CSR)*, NSF 07-504.

Real Time Knowledge Discovery (RTKD) is a proposed call that will focus on the following: finding and learning patterns, RT pattern discovery of streaming data, RT Classification and Identification, RT Link Analysis, RT analysis of heterogeneous data, RT social network analysis, online learning as data arrives, explanation , RT federated identity search, near RT secondary search, answers always ready, data reliability, RT data cleaning, RT tools for information mapping across heterogeneous data into uniform representation, RT data enhancing, building models for testing, and RT adaptive question trees.

Defense Advanced Research Projects Agency (DARPA)

In August, DARPA's Strategic Technology Office (STO) released the *Scalable Network Monitoring* Broad Agency Announcement (BAA). The objective of this BAA is to stimulate research in network monitoring technologies that would scale linearly in cost and computation time to the size of the networks being monitored. Currently, cost/computation time scaling is exponentially larger than the network grow rate. Respondents were encouraged to seek algorithms that did not rely on traditional signature based or heuristics based methods for intrusion detection and network monitoring.

Office of Naval Research (ONR)

In 2006, the Office of Naval Research issued a Multi-University Research Initiative (MURI) topic *Trust Management in Service Oriented Architectures.* The purpose of this MURI was to develop mathematical principles for ensuring trust. In addition, the ONR has sponsored University Research Initiatives (URIs) on critical asset and infrastructure protection (CIP). URI/CIP program research topics spanned a variety of areas from encrypted computing, to securing Java, to power based attacks for identifying cryptographic keys in secure hardware, and finally to investigations of the spread of viruses in computer networks.

Intelligence Community (IC)

The intelligence community has long regarded cyber-security as a top priority. Naturally, a significant portion of research in cryptology and cryptanalysis has been sponsored within this community. Recent efforts include the *National Intelligence Community Enterprise Cyber Assurance Program* (NICECAP). This program was focused on two specific areas: *Accountable Information Flow* and *Large Scale System Defense*. Accountable information flow was concerned with the problem of managing the flow of information in document form from user-to-user throughout a large enterprise. Problems to be addressed including automated classification and declassification, monitoring of user contributions, user access restrictions, and control of accidental or intentional leakage of classified or sensitive electronic information. *Defense of Large Scale Systems* was a more classical program focused on the defense of a large enterprise from a number of cyber-attacks.

IC – XYZ –Real-Time Knowledge Discovery

Acceleration of Search: The speed and rate of convergence on meaningful results for searches and other queries is the primary interest. Exploring enhancement of search algorithms, data representation schemes, clustering technologies, and other potential opportunities to enhance search is an important R&D priority.

Dynamic Question Streaming: Dynamically generate questions for interviewers

Deception detection: Develop algorithms to model and predict the likelihood that a subject is seeking to deceive an interviewer.

Anomaly detection: Identify, detect, and characterize anomalies in the data presented by an interviewee and/or data.

Human Computer Interaction Related: Research on enhanced models for human-computer interaction in the interview-support process.

Evidence Validation & Data Confidence: Research on enhanced models, algorithms, and methodologies to verify and validate evidence, including documentation of its source, accuracy and quality would support broader access to information that is relevant to interview support, as well as automation of information collection and validation. Similar research could be undertaken to enable data "confidence measurement."

IC – IARPA

Topics of interest include knowledge discovery and data mining, knowledge discovery in databases, large-scale data mining, workflow, modeling and simulation, natural language processing, advanced video, multi-source visual pattern recognition, human-computer interface research, visualization, fusion of multi-INT information, cryptography, quantum information, cyber security research.

The Department of Homeland Security (DHS)

DHS has actively pursued cyber security research through its collaboration with NSF on the *Cyber Trust* program. In addition, they have been actively developing a *Cyber Security Test Bed* as well as looking at secure protocols for routing infrastructure, including the interaction of multiple *Border Gateway Protocols* (BGP). Finally, there has been significant work in the development of "large" datasets for information security testing. DHS is currently interested in new methods of insider threat detection, internet mapping, risk assessment for complex systems, cryptographic techniques, and other cyber security related research problems. Because of the nature of the DHS mission, they are most closely aligned with the goals and objectives of the Department of Energy in protecting the nation's critical infrastructure.

DHS – S&T

The DHS S&T cyber security effort focuses on three areas:

- *Large Semantic Graph* research and development
- *Cyber Security Testbed* – secure protocols for routing information
- *Intrusion Detection, Internet Mapping,* and *Risk Assessment for Complex Systems.*

DHS S&T solicits research proposals through the Homeland Security Advanced Research Projects Agency (HSARPA), as described in http://www.hsarpabaa.com/index.asp.

Cyber Security Research and Development (CSRD), HSARPA BAA 07-09, presents the following research goals:

- To perform research and development (R&D) aimed at improving the security of existing deployed technologies, and to ensure the security of new emerging systems.
- To develop new and enhanced technologies for the detection of, prevention of, and response to cyber attacks on the nation's critical information infrastructure. To transfer these technologies into the national infrastructure as a matter of urgency.

The Institute for Information Infrastructure Protection (I3P) is a consortium of experts who work together to identify and mitigate threats aimed at the U.S. information infrastructure; it operates as a "virtual national laboratory", and is managed by Dartmouth College, with funding from DHS and other sources. Additional information about past projects is posted on www.thei3p.org .

Considerations for Classified and Unclassified Programs: Research in a Mixed Environment

A critical element for a DOE R&D agenda is the recognition that the problem space includes both classified and unclassified elements, and that the research community best suited to address these issues includes both cleared and uncleared personnel. A DOE R&D program must balance the competing need to obtain broad participation in the development and deployment of solutions with the need to protect national security. This issue has been faced by other agencies and can certainly be resolved. Our recommendation is that a forum or working meeting be convened, early in 2008, to focus on how the details of how a DOE program in this area might operate.

There are several considerations; a few of them are listed below:

- How to identify an open research agenda that addresses areas of interest within the classified space without compromising the classified mission (e.g., without providing information about potential vulnerabilities).
- How to scientifically validate work that is done entirely in the classified sphere. This may involve a cultural mind shift between traditional peer review in open science and the more compartmentalized view of research that tends to dominate in classified environments.
- Synergistic activity around areas of mutual interest – such as high performance computing and high performance networking in such a way that both classified and open research efforts benefit.
- Complementary and conflicting approaches and needs may exist – for instance, protocol analysis may be done for different reasons in open and classified space. One may need to emphasize performance, with security secondary or requiring less emphasis; the other may need to emphasize security, with performance secondary.
- How to handle the transition from open to classified, and mitigate the negative effects on uncleared researchers who may feel disenfranchised.
- Improved dissemination of research results and individual research activities in both the open and the classified communities; this is particularly important in the classified realm, but is also a need in the open space as well. It will also be necessary to facilitate ways to identify which researchers have clearances of appropriate levels to work on specific problems that require these, and to ensure that the pool of available researchers in this area is sufficient to support the research need.
- Proper handling and peer review of proposals that include classified elements.
- Managing the additional expense required for work that is conducted in a classified environment.
- Managing a clear delineation between open and closed in a research project that spans both elements – how is this documented and monitored.
- Indications of success or failure in a research project with classified elements may not be able to be communicated to the researchers working on the open elements, since success/failure parameters may be part of what is classified.

Additional agencies that should be surveyed in more detail early in 2008:

- NASA, due to the joint nature of their scientific and security-oriented missions
- NSA has a long track record of funding both open and classified research as well
- The “5 I” model for the Intelligence Community interactions with international counterparts
- Law enforcement.

Each of these has to meet the challenge of highly integrated missions, across both classifications and national boundaries.

We recommend that a forum or workshop meet to discuss further details, and that representatives from potential DOE collaborators, as well as agencies with similar needs, be invited to attend. These meetings should include both classified meetings as well as open meetings, possibly held at a shared location. It will be important for both the open and the classified communities take part in the development of this aspect of the program, since both are necessary for its success.

Contact Information

Brian Worley
Oak Ridge National Laboratory
worleyba@ornl.gov
865 574-6106

Celest Matarazzo
Lawrence Livermore National Laboratory
matarazzo1@llnl.gov
925 423-9838

Charlie Catlett, CIO
Argonne National Laboratory
catlett@anl.gov
630 252-7867

Ed Talbot
Sandia National Laboratory
etalbo@sandia.gov
925 294-1225

Deborah Frincke
CyberSecurity Chief Scientist
Pacific Northwest National Laboratory
deborah.frincke@pnl.gov
509 375 3969

Troy Thompson
Pacific Northwest National Laboratory
troy.thompson@pnl.gov
509 375-2384

References

[NRC-2007] Toward a Safer and More Secure Cyberspace, National Research Council and National Academy of Engineering, The National Academies Press, 2007.

[GENI-2006] National Science Foundation's Town Hall Meeting on GENI- Global Environment for Networking Innovations, http://www.cra.org/nsf.geni/san.francisco.agenda.html

[White House 2003] The National Strategy to Secure Cyberspace, the White House, 2003.