MEETING RECAP

CYBERSECURITY IN THE COMING DECADE

Using Security to Support the Value of Intellectual Property

Government-University-Industry Research Roundtable

February 8-9, 2011

This meeting recap was prepared by National Academies' staff as an informal record of issues discussed during public sessions of the February 8-9, 2011 meeting of the Government-University-Industry Research Roundtable (GUIRR). The document is for information purposes only and supplements the meeting agenda available online at www.nas.edu/guirr. It has not been reviewed and should not be cited or quoted, as the views expressed do not necessarily reflect the views of the National Academies or members of GUIRR.

There is widespread concern that cybersecurity will become an increasingly critical challenge in the next decade and beyond. More sophisticated efforts by "cyberterrorists" or other malevolent groups pose a difficult-to-predict but real possibility of crippling attacks on financial, transportation, utility, and other U.S. systems. Speakers at the February 2011 GUIRR meeting discussed ongoing government, university, and industry research and development work for improved cybersecurity, as well as current and emerging threats. Current cyber-vulnerabilities and responses were also discussed. Although total protection is impossible, a number of participants stated their belief that meaningful levels of security appear achievable and that cybersecurity should be an ongoing, proactive response to a continuously evolving threat.

In the opening presentation, "The Status of Cybersecurity," **Steven Chabinsky**, deputy assistant director of the Cyber Division of the Federal Bureau of Investigation, described the FBI programs at a general level and provided a perspective on cybersecurity threats and challenges. Cybersecurity threats fall into two general categories: malevolent "cyberterrorist" attacks meant to cripple digital systems, and more clandestine penetrations (e.g., foreign entities and criminals) meant to siphon off information related to intellectual property (IP) or cash.

In the first case, the objective is to cripple national systems. In the second case, the perpetrating groups typically do not want the victims to realize a penetration has occurred and are not interested in damaging the systems that provide the cash. Criminal groups typically outsource the specialized skills needed for a given operation. To date, there has not been much Internet hacking by terrorist groups. There is a very wide variety of potential assaults on digital systems, for example, regulating the phasing of electrical power systems to disrupt electrical power delivery, or digital attacks on nuclear power plants using plant diagnostic systems that are on the Internet. Significant criminal penetration of financial systems such as ATMs has occurred. (In the case of financial institutions, perhaps the largest concern is the overall integrity of the financial services.)

A major FBI cybersecurity activity is to detect IP theft from companies and advise them of that fact. A common way of detecting such penetrations is finding proprietary information about companies posted on other sites that could only have been obtained by clandestine penetration. It is typically difficult to assess the financial impact to a company for a given occurrence of IP theft, since the value depends on the value of the stolen information and how that information will be used by the attackers. The cumulative impact over all U.S. companies, however, appears very significant. In responding to these kinds of threats, a "band-aid" approach – where security tends to be built in as an afterthought – is not a good model to follow.

The meeting continued the next day with a presentation by **Peter Weinberger**, software designer for Google, Inc., and member of JASON. His talk, "Cyber Security and Science," looked at a number of technical and human challenges in responding to cyber threats and improving cybersecurity. Weinberger noted that password protection is not enough, because the same passwords are often used on many different sites with greatly varying levels of site protection. He emphasized that cybersecurity is manageable, but not "solvable," in an environment where cyber threats are continually evolving and yesterday's security has a limited shelf life. In general terms, cybersecurity is highly dependent on the actions of a few large corporate players. Although anti-virus software provides some level of protection, it cannot provide significant security to protect against motivated, technically able people who desire clandestine entry. Weinberger emphasized that although absolute protection is unobtainable, the problem of cybersecurity is manageable, because systems can be checked and the information compared, and security operations are able to see almost everything if they take the trouble to look. He noted that while good cybersecurity is not cheap in absolute terms, spending just one percent of large budgets intelligently should enable a significant level of cyber protection. The necessary R&D has to be done and prototypes tested, and the finished product has to be usable by human beings.

Next to speak was **S. Shankar Sastry**, dean of the College of Engineering, Roy W. Carlson Professor of Engineering, and Director of the Blum Center for Developing Economies at the University of California at Berkeley. In "Public-Private Sector Cooperation," he described cybersecurity programs at UC Berkeley, including collaborations with other institutions. The TRUST Center at Berkeley (Team for Research in Ubiquitous Secure Technology) is affiliated with Carnegie Mellon, Cornell, San Jose State, Stanford, and Vanderbilt. The mission of TRUST is to develop "S&T that will radically transform the ability of organizations to design, build, and operate trustworthy information systems for critical infrastructure." There are a total of 168 TRUST personnel in 2010-2011, ranging from graduate students to faculty and research scientists. Supporting disciplines include computer science, engineering, electrical engineering, law, public policy, economics, and social sciences. The center's approach is to:

- Address fundamental cybersecurity and critical infrastructure protection problems of national importance;
- Tackle "Grand Challenge" scale integrative research projects; and
- Include external (including international) collaboration for research project sponsorship and technology transition.

There are a variety of research thrusts. Examples are user-oriented authentication (people-to-site and site-to-client), open-source browsers, servers and handheld platforms, sharing of vulnerability information, and "Healthcare Informatics" – systems that support patients actively engaged in their own care, personalized medicine, and agile evidence-based care.

Robert Brammer, vice president for Advanced Technology and chief technology officer, Northrop Grumman Information Systems, described Northrop Grumman's cybersecurity programs, including its Cybersecurity Research Consortium. He stated that Northrop Grumman is the leading provider of security systems and services to the U.S. public sector, and is growing internationally. Cybersecurity threats involving IP and other security matters continue to grow in numbers, sophistication, and significance. There is a need for many types of security architectures, with the ability to handle massive amounts of data and make real-time decisions. Addressing cybersecurity challenges requires continuing advanced research from many organizations. The Northrop Grumman Cybersecurity Research Consortium includes MIT, Carnegie Mellon, and Purdue and is currently working on projects like cybersecurity modeling and simulation, innovative approaches to cloud security (used in Afghanistan), cyber testing, insider threats, and supply chain risk. Cybersecurity is a complex and multi-disciplinary subject, and in addition to developing new technologies, there is a need for work on strategic, economic, psychological, sociological, and legal issues.

"Fine Grained Cybersecurity for Providing Continuous Assurance of Intellectual Property Integrity" was discussed by **Chung-Sheng Li**, director of Commercial Systems Research at the IBM T.J. Watson Research Center. Li said that because of rapid technological development and the large increase in information volume, traditional perimeter defense is less effective than before. "Fine-grained" cybersecurity technologies and security approaches are needed, with multi-tier containment spanning across platforms, cloud computing centers, middleware, and collaborations. Li noted that attacks are more persistent, targeted,

and undetected than before, and malicious attacks have surpassed human error for the first time in 2009, with nearly half of data breaches recently caused by insiders. A report by security vendor McAfee estimated corporate IP loss at $4.6 billion in 2008. The advanced persistent threat of recent cybersecurity attacks features a rapidly shifting attack strategy, with dynamic code, persistent repetitive attacks with alternate methods, and emphasis on sensitive, high value information with the operational objective of remaining undetected. Elements of more effective responses will include better "information provenance," attack attribution, integrity management, rapidly adaptive defense, and proactive preparation.

Dr. Li suggested that GUIRR might consider:

- Conducting a G-U-I workshop discussing open metrics and benchmarks, including sanitized incident data;
- Establishing a G-U-I consortium or forum to bridge the divide between what the government knows (e.g., estimated $1 trillion IP loss during 2008-2009) and the general lack of awareness of the severity of the IP theft problem.
- Holding a G-U-I workshop to investigate a mechanism for bootstrapping a self-sustainable ecosystem that allows continued measureable improvement in cybersecurity.

Ravi Sandhu discussed cybersecurity threats, challenges and approaches in his presentation on "What is the Game in Cybersecurity?" Dr. Sandhu is director of the Institute for Cyber Security at the University of Texas at San Antonio. Cybersecurity consists of multiple games played at multiple levels, Sandhu said, where we don't get to set the rules or pick the adversaries, and where defense is asymmetrically harder than offense. Cybersecurity needs to be proactive, not reactive, because the adversary is always thinking outside the box. Sandhu noted that most cybersecurity thinking is done at the "micro" level, whereas most big cybersecurity threats are at the "macro" level. Microsecurity thinking emphasizes "retail" attacks (99% of the total), which are handled without much problem. Big cybersecurity threats (1% of the total) are difficult or even impossible to detect and defend against. Rational behavior concentrated at the micro level can result in highly vulnerable assets at the macro level. Although it is common for cybersecurity to look largely to computer science for help, that pattern needs to be broken. Cybersecurity needs to become its own discipline and not just a subset of computer security.

Michael Carroll discussed cloud computing and cybersecurity in a presentation entitled "How Cloud Computing May Realign the Relationship between Cybersecurity and Intellectual Property." Carroll is a professor of law and director of the Program on Information Justice and Intellectual Property, Washington College of Law, American University. How much is invested in security is a policy question. How can we use security, e.g., to increase the value of the IP being protected? The practice of sending executable code to users for enhanced copyright protection creates gateways into user computers for subsequent malware (e.g., Sony rootkit code). It is wise to be skeptical of copyright cybersecurity as commonly practiced. Watching movies from licensed sources lessens the threat risks by the use of a cloud library, where the cloud security is mainly concerned with preserving the privacy of consumer orders. Carroll noted that in attempting to protect copyrighted material, a lot of collateral damage results from redesigning networks to attempt to distinguish between "good bits" and "bad bits." He proposed a "creative commons" as a helpful approach, where standardized copyright licenses are used. The commons approach basically says that what goes on in the commons is public domain as long as due credit is given. Such an approach is one way of addressing the confusion around the rights of data and the legal requirements that go with bits of code.

Chris Greer, assistant director for Information Technology R&D at the Office of Science and Technology Policy, gave a presentation on the White House's involvement in cybersecurity. In "Change the Game in Cybersecurity" he noted the huge changes in technology and the rapidity of changes in threats. The President's Cyberspace Policy Review of May 2009 identified several key strategies: lead from the top; build capacity for a digital nation; share responsibility for cybersecurity; create effective information sharing and incident response; and encourage innovation (provide a framework for R&D strategies that focus on game-changing technologies). Unclassified Federal cybersecurity research and development investments reported annually by the NITRD agencies (see www.nitrd.gov) total approximately $400 million. The strategic approach of the White House is divided into nearer term "Near Horizon" game changers and "Over the Horizon" goals such as improvements in the science of cybersecurity and research for results (i.e., translation to practice). Greer noted that the asymmetry favoring the attacker, the prohibitive cost of satisfying all cybersecurity requirements, and the lack of meaningful metrics for sound decision-

making result in a misallocation of resources. A major goal is to have a level of security appropriate to the level of risk. Greer pointed out flaws in the conventional wisdom that defense-in-depth is the way to robust security, distributed data schemes provide security, and abnormal behavior detection finds malicious actors.

The final presentation, “Cybersecurity Research at PNNL,” was given by **Deborah Frincke**, chief scientist for Cyber Security at Pacific Northwest National Laboratory. Dr. Frincke described PNNL work on real time triage of cyber events – the challenge being to recognize sophisticated events and discover patterns rapidly. One major challenge in cybersecurity is deciding who does what (e.g., “tragedy of the commons” where a major resource is shared by many users, but with no clearly defined guidelines, responsibilities, and programs for intelligent use over the longer haul). One element of a successful long-term approach is to clarify the appropriate roles for science and engineering. There is a changing perspective featuring the increased need to balance the human, cyber, and physical elements for all users of the Internet, with security as an enabler, but not driven by cybersecurity fears. PNNL cybersecurity programs help protect cyber-based systems that monitor and control critical infrastructure. Intrinsically, Secure Computing at PNNL involves software and systems that will inherently respond to and defend themselves against internal and external threats. "Designed in" security is an ultimate goal. PNNL cybersecurity incorporates corrective and forensic security measures to support and maintain legacy and modern systems. Control systems at PNNL were built with reliable operations in mind, not security. An additional challenge is to take into account the life cycle of control system equipment that may be 20 to 30 years old. A goal is to develop or migrate technology from the information technology world to the control system world without adversely impacting reliable operations. PNNL works collaboratively with national and international standards bodies, vendors, and universities to arrive at better solutions.

ABOUT GUIRR

MISSION

GUIRR’s formal mission, revised in 1995, is “to convene senior-most representatives from government, universities, and industry to define and explore critical issues related to the national and global science and technology agenda that are of shared interest; to frame the next critical question stemming from current debate and analysis; and to incubate activities of on-going value to the stakeholders. This forum will be designed to facilitate candid dialogue among participants, to foster self-implementing activities, and, where appropriate, to carry awareness of consequences to the wider public.”

STAFF

Susan Sauer Sloan, Director, GUIRR
Anthony Boccanfuso, Executive Director, UIDP
David Wright, Executive Director, FDP
Claudette Baylor-Fleming, Administrative Coordinator, FDP
Denise Greene, Administrative Coordinator, GUIRR and UIDP
Laurena Mostella, Administrative Assistant, GUIRR and UIDP
Chris Verhoff, Financial Associate, PGA

For more information about GUIRR visit our web site at http://www.nas.edu/guirr
500 Fifth Street, N.W., Washington, D.C. 20001
guirr@nas.edu 202.334.3486