Stanford University

C I S A C

Center for International Security and Cooperation

The Center for International Security and Cooperation, part of Stanford University's Institute for International Studies, is a multidisciplinary community dedicated to research and training in the field of international security. The Center brings together scholars, policymakers, scientists, area specialists, members of the business community, and other experts to examine a wide range of international security issues.

Center for International Security and Cooperation
Stanford University
Encina Hall
Stanford, California 94305-6165

(415) 723-9625

http://www.stanford.edu/group/CISAC/

Workshop Report

Regional Interest Group on Information Security: Sharing Information and Exploring Collaborative Opportunities

December 7, 1998

Kevin J. Soo Hoo
Gregory D. Grove
Ekaterina A. Drozdova
Stephen J. Lukasik
David D. Elliott
Seymour E. Goodman

Consortium for Research on Information Security and Policy (CRISP)

CRISP is a research collaboration of the Center for International Security and Cooperation, the Institute for International Studies, and the School of Engineering, Stanford University.

January 1999

About the Authors

Kevin J. Soo Hoo is a Ph.D. candidate in the Department of Engineering–Economic Systems and Operations Research at Stanford University. **Gregory D. Grove** is a CISAC Visiting Scholar. **Ekaterina A. Drozdova** is a researcher with the CRISP program. **Stephen J. Lukasik** is a CISAC Visiting Scholar; he was director of DARPA and held executive positions at RAND, Northrop, and TRW. **David D. Elliott** was staff director for science and technology at the National Security Council and then vice president at SAIC and SRI. **Seymour E. Goodman** heads the CRISP program at CISAC and is professor of Management Information Systems and Policy at the University of Arizona.

Contents

Preface

The Consortium for Research on Information Security and Policy (CRISP) has been created at Stanford University for the purpose of developing a better analytical and policy understanding of how to strengthen the nation's information infrastructures and how to mitigate the effects of malicious actions directed at those infrastructures. CRISP studies explore the technological, legal, organizational, international, and policy dimensions of these problems. CRISP is a consortium of university researchers, including individuals from the Center for International Security and Cooperation and from two departments of the School of Engineering, the Department of Computer Science and the Department of Engineering–Economic Systems and Operations Research. CRISP works closely with companies involved in various areas of information technology, network users and providers, and parts of the federal government. The specific projects undertaken by CRISP draw on the interests and knowledge of this community. The three main areas of work are a university/industry/government forum, technology and policy research, and international participation.

CRISP's main function is to provide a forum to continue and expand the dialogue among the main stakeholders in our nation's information infrastructures (i.e., the infrastructure owners, the industry that provides network technology, the major users, the federal government, and the research community). CRISP members will continue to assist in the process of developing common views among these interested organizations through analysis of the surrounding issues.

In the technology and policy area CRISP defines and conducts research projects on subjects that are important to understanding the vulnerability of information infrastructures, barriers to solutions, and possible remedies. These projects investigate and analyze technical constraints on infrastructure protection and possible technological developments, international and policy considerations in protecting infrastructure, and the effect of existing and proposed laws and regulations on the goal of securing infrastructure.

Information infrastructure security is a manifestly international problem since usage, and hence dependence, are becoming global. Cyber attacks can move easily across borders, and adequate remedies will require a high degree of interstate cooperation. CRISP will through conferences and other forms of exchange undertake to build an international constituency to address the problems of securing information infrastructures on a global basis.

Executive Summary

On December 7, 1998, a cross-industry group of professionals interested in information security met to discuss perspectives on information security and prospects for multilateral cooperative activity to advance information and infrastructure security. Participants reviewed the information-security activities of their respective organizations, identified areas of mutual concern, and generated ideas for future group efforts.

A new perspective on security is evolving among the information-security industry and its customers—one that stresses the role of security as an enabler of business and as a means of achieving a more robust information infrastructure. Individual companies should (for the immediate term) develop security products to address vulnerabilities in existing architectures and (for the longer term) design new architectures with security "built in" to the system as a major design criterion. Industry associations and government agencies may usefully promote a greater understanding of the immediate and longer-term risks facing users of information infrastructures and thereby raise consumer consciousness regarding information-security issues and encourage use of security products and migration to secure architectures.

The rate of adoption of information-security measures will be dictated in part by their cost, ease of use, and performance/security trade-off. The shift to more secure hardware platforms may take many years. Even with more secure architectures, attackers will continue to use "social engineering" and "open sources" of information to help them characterize a target and learn its vulnerabilities. Automated information-collection tools may assist them. Companies with an interest in security should review how much information about their networks is available, especially on the World Wide Web, where automated tools may be particularly effective.

Many participants noted the pent-up demand for virtual private networks and the anticipated explosion of electronic commerce. The strong demand for rapid implementation of new technologies can lead to inability to thoroughly test and develop security measures for products before they enter the market. Balancing security against growth and marketing pressures presents a continuing conflict.

Contributing to the problem of insecurity are a lack of understanding of the risks by infrastructure owners and users and the resulting failure of senior management to devote suffi-

cient attention to it. Consumer interest in security, however, appears to be slowly developing. Fear among network users of unauthorized access and resulting damage is growing. Companies must develop products that reduce security risk and market structures that profitably tolerate the remaining security risk.

An effort to mitigate risk without overprotecting can be started by developing criteria-based standards that weigh security against performance and cost. Criteria-based standards will better assist security-product developers than technology-based standards because the state of the art in intrusion would quickly make any technology-based security standards obsolete as new security measures faced the ingenuity of human attackers.

The U.S. government is interested in promoting industry participation in protecting the infrastructure. National labs are eager to collaborate with industry on security issues, and government money will likely be directed at infrastructure security soon.

Legal issues shape a portion of the risk for infrastructure-related companies, but legal structures can also create opportunities. Legal liability for high-technology industries may be more difficult to avoid than for low-tech industries. Balancing of costs of prevention against the likelihood and magnitude of possible harm may be displaced by a presumption of negligence for network-security industries, precisely because the industry's advanced technology may be expected to provide a higher degree of protection. Two laws that create opportunities to decrease antitrust liability risk and increase access to capital and expertise, respectively, are the Registered R&D Joint Venture statute and the Cooperative Research and Development Agreement statute.

Ultimately, a regional shared-interest group based in Silicon Valley and facilitated by Stanford may help clarify issues of information-infrastructure security, promote better understanding and recognition of risks, test and review security proposals, experiment with new concepts, educate the public, and develop standards for measuring and assessing security.

Introduction

Information security is a part of the general public good of a secure information infrastructure, regardless of whether the information networks that provide public goods such as emergency services, defense, or basic infrastructure components are publicly or privately owned and operated. Either way, all legitimate users of the network have an interest in seeing that its security and reliability are maintained. Each of the workshop participants has an interest in information security, is working on some aspect of it, and believes that attention to these issues is needed.

The workshop participants represented a cross-section of organizations from the Silicon Valley region, including several industry representatives, academic and research organizations, and national laboratories. The objectives of the workshop were to improve communications between organizations and to identify opportunities for longer-term collaborative activities. To those ends, most of the participants were asked to speak briefly and informally, on a not-for-attribution basis, about three central questions: how information network security was perceived within their organizations, what related activities were taking place, and whether the participating organizations have considered cooperative actions with other organizations. In the concluding session, participants discussed the usefulness of forming a continuing regional interest group for multilateral collaboration and for understanding and providing input to government activities in information security.

The following report summarizes views expressed during the workshop about the nature of information security today and in the future, the business trends in the security industry and of information technologies as a whole, the technical and process challenges facing information security, changing customer needs across industries, legal liability issues, and opportunities for collaboration.

Information Sharing

Views of Security

A fundamental change is needed in the way information security is viewed. The old view of castle-and-moat security with paranoia being the driving force compelling the construction of ever stronger walls and deeper moats will not be practical in an age of increased inter-organizational connectivity, collaboration, e-commerce, and extensive multinational operations. In the future, components of a secure infrastructure may be able to determine independently the trustworthiness of users seeking access.

The new perspective of security must stress security's role as an enabler of business opportunities and as a means to a more robust information infrastructure. Security should also be perceived as an annual process of review and update that requires a long-term commitment from corporate management. Some participants were concerned that top management did not perceive the importance of information security to their businesses. Because both the information infrastructure and the problem of information insecurity are global, the new perspective must also reflect that global nature and not be trapped in the provincialism of strict national security.

In selecting an appropriate level of security, a company must consider its place in the "pantheon of targets." Controversial or prominent government agencies, companies, and universities are often the target of frequent attacks; for example, the Department of Defense and national labs that work on nuclear-weapons projects. Malefactors may infiltrate the networks of companies with security expertise to obtain security information or to test new methods of attack.

A great deal of information about computer systems and users resides in the public domain. In just a few weeks, a would-be attacker could characterize a target fairly well by using either automated information-collection tools or social-engineering techniques. One participant experimented with semi-automated collection tools to filter publicly available information on the World Wide Web and discovered, in just three weeks, entry points, usernames, and version numbers of software running on a target system. Recognizing that any system can be penetrated if the attacker is willing to devote the necessary resources, the purpose of improving security is to make the cost of penetration sufficiently high to deter people from wanting to attempt it and to reduce the level of damage that an attacker can inflict even after successful system penetration.

Information-Security Industry Challenges

The information-security industry faces many issues and impediments that hinder the progress of securing the information infrastructure. These obstacles include a lack of education of both individual users and businesses about the dangers and severity of information insecurity, lack of high-level attention due to other distractions such as the Year 2000 problem or industry restructuring, and serious confusion in the marketplace for information-security solutions. This confusion stems from the sometimes exaggerated dangers of Internet commerce; the lack of standards for public-key infrastructure, digital signatures, and other security strategies; and the deleterious effect that export-control laws have had on the domestic deployment of strong encryption.

Companies also face difficulties selling overseas because of economic nationalism. Clients in foreign countries tend to prefer products made in their own countries, wishing to support the development and growth of their domestic software industries. Many also distrust U.S. standards either because they do not understand the standards or do not understand their purpose. For example, clients in foreign countries may not understand why U.S. standards layer security measures. They may also be concerned by the possibility of the United States imposing export restrictions on security-related software and in so doing potentially cutting them off from their security software provider.

Industry needs to make its products more transparent to the user (i.e., easy to use, financially accessible, and without significant impact on workflow), to develop interface standards that will lower the cost of ownership, to establish best practices that most effectively enhance security and are not just the most convenient ones to implement, and to accept the fact that customers are unwilling to pay for perfect security but will purchase some measure of admittedly imperfect security.

Security must also be made scalable. Local solutions to vulnerabilities may prove impractical on a national scale. Security developers must design products that may be applied as the market for those products expands to its maximum extent without compromising performance.

Some technology companies today are offering insurance to protect against losses resulting from information-security failures, thus helping customers manage their information-security risks. The insurance industry has made very limited attempts to enter the market for infrastructure insurance, probably due to the lack of reliable actuarial data for determining appropriate premiums. The problem facing electronic commerce today is the challenge of creating a system that can touch everyone in the world while simultaneously managing the existing and emerging risks. Baseline criteria for assessing security, understanding risks, and comparing different security products are needed. Tools that enable companies to manage risks, such as insurance, are also needed.

"Transparency" is often used to describe the goal that security measures be unobtrusive to the user, but, in an international context, transparency also means that people inspecting the security of a system are able to see and to understand the security measures in place. Such inspection transparency is useful when mutually distrustful parties need to know the mechanics of security measures so they can be sure those measures are not being tampered with or used to their disadvantage. Such transparency has proven particularly useful when employing security measures to protect, authenticate, and verify the integrity of communications regarding international arms-control verification, and would be useful whenever any mutually distrustful parties communicate.

Another international challenge centers on the fact that different cultures value security differently. This situation presents a dilemma for infrastructure protection, because areas of the world where security is valued less become weak links in the global infrastructure. Even a multinational company with a uniform security policy may suffer from unwanted "backdoors" to its network because some foreign subsidiaries may not have fully implemented the corporate security policy.

Enlarging the community of information infrastructure users yields direct benefits for those businesses that use the infrastructure for advertising or e-commerce, but expanded access is directly at odds with security and robustness. Vast increases in the user population stretch the capabilities of systems and increase the chance of failures from overuse. Quickly growing populations of users also stretch the capabilities of system operators to keep watch over the

traffic capacity and security of the systems they administer. Business demand for access is magnified by user demand for access, not only to the information pipeline, but also to more and more information that can be carried by that pipeline.

Users of infrastructure value privacy, but access is even more important to them. Users want privacy, but privacy competes with access to information and with security. While a reasonable balance may be struck between privacy and access to information by allowing information owners to make information public, semi-public, or private as they desire, finding a similar balance between privacy and security is more difficult. To detect suspicious activity and to deter intrusion, system administrators must monitor the activities of all users, even ones who may be legitimate. Encryption appears to provide substantial improvements in both privacy and security, but encryption standards have not been widely adopted or implemented. Encryption may also be used to conceal malicious activity. Even if data flows and perhaps control traffic were encrypted, infrastructure-security personnel would need to monitor user activity to prevent intrusions.

Further, the tradition of open access to information in the computer networking culture is at odds with security. Users of the Internet, for example, are strongly resistant to government regulation. Regulation may restrict access to information or information conduits and would almost certainly increase the cost of use. Both users and providers see freedom from regulation as a fundamental strength of the Internet, permitting rapid development of Web-based markets for products and ideas. Security should come predominantly from solutions developed by industry, not solutions mandated by government.

There may be little or no degradation and even side benefits from appropriate security measures. However, it is likely that the question users will face is whether the possible performance degradation that security measures precipitate is worth the protection they provide. Security measures must not seriously hamper people in their everyday activities or prevent them from efficiently completing their work, or people will circumvent the security measures. Some security is desirable, and industry needs to tell consumers about the risks they face to help them understand, manage their risks, and choose an appropriate level of security.

Technical and Process Challenges

Ongoing and future research must address problems in building basic protections for existing systems, architectures for future systems, methods for testing large-scale networks and systems, standards for security, and standards for the comparison of security products. Research is currently focused on both hardware and software solutions for protective strategies such as firewalls, Internet Protocol security, authentication, intrusion detection, cryptographic research and development, and ATM network security.

One of the major challenges in intrusion detection research is to reduce the high false-positive rate. The false-positive rate is both a technical problem and a process implementation problem, rooted in corporate, bureaucratic, and institutional culture issues.

Although the Internet has certain security building blocks (such as authentication technologies, encryption, etc.) already in place, it needs to be made more robust against different kinds of threats. Architectures need to be constructed to synthesize these building blocks and make security a primary design criterion. Building such a secure system is easier than trying to fix a system's security problems after it has been built.

Existing systems, however, cannot be ignored. The investment in those systems is immense and many users will be financially unable or unwilling to upgrade to secure architectures

simply because those new architectures are more secure. Because existing systems currently perform vital functions and cannot practicably be replaced in a timely fashion, research is needed to help make these systems more secure as well. Process, distribution, and configuration problems may also require careful attention as the deployment of security solutions to current systems becomes a challenge. For example, with regard to trusted distributed systems, research is needed to look at how security patches can be distributed in a secure and authenticated manner so that people can have confidence that the patches are themselves free of malicious code.

The challenges of securing large distributed systems are only expected to grow as the market for virtual private networks (VPNs) is expected to explode in 1999. This trend is fueled by a shift in basic corporate information infrastructure toward a client-to-host structure. The scales of VPN deployments currently being discussed range from tens to hundreds of thousands of users per network, making the task of securing and testing such systems daunting. The demand for VPNs worldwide is pressing suppliers to install products before the security implications have been completely considered. VPNs do and will increasingly contain sensitive commercial and financial information and trade secrets; therefore, an incomplete consideration of the security implications of widespread deployment is particularly troubling.

Another complicating design parameter for large systems with multiple international users is the issue of distrust, as in the case of systems supporting arms-control verification or, in some cases, between businesspersons negotiating at arms' length.

Industry's processes for designing and constructing systems may need to be revised in light of the special needs of secure systems. Specifically, industry must take care to ensure the trustworthiness of the personnel working on secure systems and of the components being used to build secure systems. The engineers who work on critical infrastructure systems must be trusted not to intentionally damage the systems on which they work. The nuclear power industry has well-developed personnel security procedures and may be used as a model by other infrastructure providers. If personnel security measures are adopted procedures must be reasonable from the worker's perspective and employee desires for privacy must be considered to avoid labor–management conflict. To ensure security for government purposes, the clearance level of each person working on a particular system must be equal to the level of secrecy of information that is likely to flow through the system. Industry must also be aware that employees working for foreign intelligence agencies or criminal conspirators may have imbedded trapdoors or other backdoors in components obtained from foreign suppliers, enabling those agencies to access otherwise secure systems through planted secret portals.

Customer Security Needs

In the past, customer interest in information security was low, but more recently the interest has increased. Businesses today have two primary expectations of information security: to protect their computers, networks, and information; and to generate and enable new business opportunities. Although the risk of overwhelming losses, both monetary and in consumer confidence, was a key motive for the early adopters of information security (e.g., banks), it has become less of a factor in recent months. Instead, businesses today appear to have different reasons for implementing computer security. Two of the most often cited are to limit liability, as has been recently required by insurance companies or regulators, and to save money that would have otherwise been lost handling security breaches.

Virtual private networks are rapidly becoming a solution of choice for businesses to carry internal communications because they allow a company to authenticate access to its network, to secure internal communications, and to escrow or back up company information in the event the information must be recovered.

Many companies tend to fear intrusion more than any other computer-related problem. They worry about what an individual can do once inside their systems, but they seem unwilling to pursue criminal prosecution as a deterrent for would-be intruders because of the fear of negative publicity. Companies often attempt to handle security breaches internally, tracking down intruders and warning them of severe consequences. Despite this tendency to handle matters internally, if an intrusion is suspected to be linked to organized crime, the stakes are raised from business risk to personal physical risk, and companies will generally go immediately to law enforcement.

One example of publicity gone awry is the Citibank case. In August 1995, Citibank publicly acknowledged that its computer security had been compromised and that approximately $10 million had been electronically stolen by a Russian hacker and his accomplices. Citibank also made public its intention to pursue criminal prosecution of the accused hackers. Immediately following the acknowledgment, Citibank's competitors pitched their services to Citibank's largest customers, claiming they could better protect those customers.

Many users of the Internet today believe that the information infrastructure must be made more robust and reliable in the future. Just as fraud-tolerant economic and business models were developed to foster growth in the cellular telephone industry, despite the high incidence of fraud,[1] business models for e-commerce that tolerate fraud, intrusions, and damage must be developed to account for the security environment of the Internet, present and future. A mixture of security measures, risk sharing, and cost allocation will be required to make e-commerce profitable in the long term. Fraud-tolerant market models and cooperation with law enforcement to prosecute computer-assisted theft will help build trust in e-commerce infrastructures.

Security needs for information assets tend to vary from one industry to another. Historically, the largest banks and financial institutions were the major customers of information-security products. Wealthy banks that faced loss of both money and consumer confidence had the means and the motives to take information security seriously, demanding protection from intrusion and the ability to rapidly send and receive millions of secure, authenticated communications.

In the entertainment industry, feature films are often conceived, composed, and edited on computers. Tens of millions of dollars worth of intellectual property may be contained in the large files transmitted between those participating in the production. Unauthorized underground releases of scenes from a film in either raw or edited form could damage the market for the film. Therefore, the entertainment industry needs secure, authenticated transmission of very large files between the major players and participants.

In the health-care industry, data integrity and the maintenance of privacy are the primary issues. A compromise of data integrity could threaten a patient's life, while a compromise of privacy could expose the health-care organization to legal liability. One participant emphasized that the nature and scope of the risks associated with routinely using communications infrastructures to perform actions upon which lives depend are poorly understood. For ex-

[1] One participant stated that 40 percent (60 percent in Los Angeles, California) of the value of cellular telephone services used in the United States is uncollectable because those services are fraudulently procured.

ample, tele-surgery may be a convenient way for an experienced surgeon to assist a novice with a complicated procedure; however, if the communications link is severed, the novice may be required to continue the procedure alone. Other risks include deletion or alteration of patient records, which may result in improper treatment. Improper administration of pharmaceuticals (to an allergic or contraindicated patient) could result in serious harm or, in extreme situations, death. One solution might be to remove critical-to-life operations from the general public infrastructure and place them in a separate network that is better protected than the rest of the infrastructure.

The utility industry, once the epitome of a closed system, is dramatically changing. Fully one-third of utility control communications travel over public networks; massive fiber-optic networks built by the utilities for internal use are becoming increasingly public as excess capacity is sold to non-utility firms; and deregulation is fueling a radical change in the landscape of the utility industry itself. Where once a completely vertically integrated company existed, several companies (power generators, power schedulers, power marketers, independent system operators, power exchange markets, utility distribution companies, meter data management agents, energy service providers, billers, and customers) now exist, each needing links to the others through which power and information can flow. In this example, competition is driving the industry toward open standards, greater system and control automation, open access, increased connectivity, increased use of public networks, more outsourcing, and customers who demand more services. Despite the move toward greater use of public networks, the utilities have been building their own private networks for handling critical control functions so that they do not have to deal with system intrusions.

Significant changes are also occurring in the national research laboratories. The national labs are eager to find partners to help develop cryptographic technologies for international treaty and nuclear materials monitoring. There is a particular need to develop low-power, computationally constrained authentication mechanisms in support of those monitoring activities. Other interests include fast transmission with fast encryption, high-performance computing distributed computing security, distributed key management, vulnerability assessment tools, and software surety and secure operating systems. The national labs are also looking at the broader problem of dealing with intrusions and national security, specifically from a privacy perspective, with emphasis being placed on programs that can efficiently produce useful technology and not just pure research.

Legal Liability

Whenever a product is placed into the stream of commerce, the manufacturer may become liable for defectiveness. Defectiveness is defined by a negligence argument which, in turn, is based on a cost–benefit analysis of repairing the defect. Thus, if the expected negative consequences of a defect outweigh the cost that the manufacturer would have incurred to fix it, then negligence exists. However, if the cost of fixing the defect can be demonstrated to outweigh the consequences of it not being fixed, then no negligence should be found.

In software, negligence is very difficult to prove. The accounting of costs and benefits is not as straightforward as in other defect liability cases such as the Ford Pinto's exploding gasoline tank. The calculated cost of the Morris worm incident is still disputed, with estimates ranging between $96 and $200 million. The fact that this controversy persists several years after the event itself undermines the case for liability. Further complicating negligence analysis, in recognition that economic damages resulting from lost opportunities remain con-

troversial the courts have tended to deny liability when people are not physically harmed and when property damage was not evident. However, some states have passed legislation determining that information is property, providing a basis for inferring that damage to information, like damage to property, may justify a finding of liability.

The law also has a doctrine called *res ipsa loquitur*, which translated from Latin means "the thing speaks for itself." The doctrine basically states that by virtue of the act itself, negligence can be inferred without performing a cost–benefit analysis. For example, a surgical instrument is not usually left inside a patient without someone failing to take reasonable care; therefore, if a surgical instrument is found inside a patient after an operation, courts will usually find negligence under the doctrine of *res ipsa loquitur*.

Negligence under the *res ipsa loquitur* doctrine is also more likely to be found when advanced technology is involved. Technological advances tend to increase the liability exposure of product manufacturers. Technology is presumed to improve products and reduce the number of defects in them. Thus, products with greater levels of technology may be subjected to stricter liability standards. For example, two similar cases were decided by the Supreme Court on the same day with very different outcomes. The cases were similar in that they both involved vehicles disappearing at sea. In one case, a fishing boat disappeared without a trace, and in the other, an airplane vanished over the ocean and was never recovered. Relying in part on the fact that the airplane involved fairly advanced technology whereas the boat was comparatively primitive, the Court held the airline liable under *res ipsa loquitur* but did not hold the boat owners liable.

Circumstantial evidence cases can be built if the consequences are disastrous enough, and the solution is cheap and available. In the case of software controls for infrastructure, an actual accounting may be unnecessary because the scale of the consequences is so dramatically out of proportion to the costs of fixing a defect that the failure to fix a defect may "speak for itself" and the details of a cost–benefit calculation may be unnecessary.

Cooperative Frameworks

Two legal mechanisms for companies to collaborate on activities either amongst themselves or with the government are the Registered Private R&D Joint Venture and the Cooperative Research and Development Agreement.

A Registered Private R&D Joint Venture must be registered with the Department of Justice as a joint venture and in doing so must inform the Department of the purpose of the joint venture and the identities of the participants. Once such a venture is registered, the participants receive two significant benefits under antitrust law. First, any possible violations of antitrust laws for unlawful agreements in restraint of trade are judged under the lenient "rule of reason" standard instead of the much more harsh "per se illegality" standard of inquiry. Second, if antitrust liability is assessed, maximum damages are reduced by two-thirds, because the statute relieves joint-venture participants from the danger of having to pay the treble damages that would have otherwise been assessed.[2]

Cooperative Research and Development Agreements (CRADAs) can give a company access to government scientists, money, equipment, and other resources, but require that the fruits of the research be shared with the government. Government rights can be limited to a non-exclusive government right to practice the resulting inventions, but the exact scope of

[2] 15 U.S.C. §§ 4301-05 (1998).
[3] 15 U.S.C. § 3710a (1998).

any greater government rights is negotiable. Importantly, government laboratory employees can assist in the commercialization of a product while they remain on the payroll of the lab.[3]

March-in rights are often inserted in CRADAs to allow the government an option to recapture the right to market the technologies developed in a CRADA in the event the company fails to effectively commercialize the technologies. A CRADA is an agreement between a government laboratory and its cooperating partner, however, and the government is eager to collaborate with the private sector on infrastructure security matters, so this issue may be effectively negotiated away if it is important enough to the partner.

Patenting Methods of Doing Business

Until recently, many believed that "methods of doing business" were not patentable. In contrast, the U.S. Patent and Trademark Office (PTO) has recently granted patents on what some claim are methods of doing business on the Internet. A strong public policy argument can be made that no one should be able to lock up an important channel of commerce, upon which people have come to rely, with a new patent. Specific improvements in security, for example, might be patentable, but patents should not be issued for devices or methods in public use before the patent applicant has developed his version of the invention. Occasionally, technology gets ahead of the PTO's ability to evaluate it, and sometimes patents are improperly granted. Court challenges to the claimed novelty and non-obviousness of improperly granted patents may be necessary until the PTO gains sufficient expertise and builds libraries of prior art related to Internet commerce. If court challenges fail, legislation may be necessary to clarify congressional intent regarding an inventor's ability to control huge portions of an important and previously existing marketing channel.

Collaborative Activities

Cross-industry activities are taking place to improve communication and collaboration within industries by exchanging information, building consensus, and identifying opportunities for collaborative operational activities. Regional interest-group meetings are advantageous for building personal and professional relationships, learning about new attack strategies, and learning how to defend against them. Because most of the participating organizations have e-mail lists, general queries can be sent out to the whole group easily. Forums for sharing information include the San Diego Regional Information Watch, Agora, National Security Telecommunications Advisory Committee, Cross-Industry Working Team (XIWT), International Information Integrity Institute out of SRI, and the European Security Forum. Notably, the regional groups lack nationwide coordination, even though such coordination would likely benefit them all.

Existing collaborative efforts bring stakeholders from many private-sector industries together with public sector stakeholders; define technical requirements for a sustainable information infrastructure; prepare technical papers on performance, security and architectures; discuss threats to infrastructure (e.g., design deficiencies, Y2K, scaling deficiencies, and system congestion); and plan to improve robustness. A cross-industry group may be particularly well suited to address robustness on three separate levels: first, improving robustness of individual organizations; second, improving robustness of the overall infrastructure against failure of component subsystems; and third, improving the ability of individual organizations to protect themselves against failure of such component subsystems.

Some participants believe that the government should be responsible for protecting the infrastructure against large-scale threats, while businesses should be responsible for day-to-day security relating to computers under their control. Some effort should be devoted to determining how to draw the line between large-scale and day-to-day threats, and to determining whether these two types of threats are completely separable. Collaboration between government and industry beyond the groups in existence today is certainly needed to accomplish both jobs.

Next Steps

Role of Government

Government will attempt to address the infrastructure protection problem with or without industry input. Government is already clearly involved in information infrastructure protection policy. It currently controls exports in a manner that complicates some business efforts to improve infrastructure security. Positive government roles include that of a very large user of security products, that of a sponsor for long-term research, and that of an independent observer that can address problems beyond the purview of any one company.

The report of the President's Commission on Critical Infrastructure Protection calls for research and development investments to be made in technologies required to address the nation's infrastructure security problems. In the near future, the government will likely be spending money to develop those technologies. If the government becomes interested in commercial products for security, the market might benefit from the interest, especially if the involvement helped to establish best practices which in turn would help foster the industry.

Government would like to see industry adopt best practices standards. In other fields, engineers and technical people from universities and industry set standards. The legal establishment and government then legitimize those standards. Because the telecommunications infrastructure is complex, large, and evolving, the standards that are set for it would likely be set by a standing committee and be revised periodically. If this regional interest group decides to work on standards, then the first step would be to decide what kinds of standards need to be established.

The state of the art in security is rapidly changing as the risks it addresses also change, and criteria-based standards are best adapted to suit the needs of information-infrastructure operators. Robustness against natural disaster is very different from robustness against malicious activity. Malicious activity, especially covert computer-assisted intrusion into networks, is different in kind because malicious actors can adapt to security measures. Technology-based standards may be adequate to protect against nature's threats, because once a method of disaster prevention has been proven against flood, for example, it will likely work against flooding again. In sharp contrast, human actors will attempt to circumvent previously proven security measures. The state of the art in intrusion will advance, changing security needs; therefore, technology-based standards for robustness against malicious attack would require frequent and extensive revisions whereas criteria-based standards would need fewer and less extensive changes.

Suggested Activities for a Regional Interest Group

Most of the participants found the workshop discussions informative. While everyone is now more familiar with others' technologies and perspectives, no one claims to have a solid grasp of the complete system picture. Strategic objectives should be established for the future meetings. Among those objectives should be the sharing of information and the creation of a database of that shared information.

Research organizations can complement industry in several important ways through an interest group such as this one. For example, face-to-face meetings between researchers and industry provide opportunities for technical feedback that can help prevent technical irrelevance of longer-term research. Also, Stanford tends to attract high-caliber young talent from all over the world and can provide a valuable source of future employees for industry.

Interest within the group for continuing the discussion on infrastructure problems remains very strong. Having the interest group based at Stanford University yields the benefits of putting people at ease about sharing information and reducing government suspicions of industry collusion. Many topic-oriented groups already exist, so the interest group that Stanford assembles should be committed to more than just talking and sharing information. Possibilities for other activities include:

- Raising awareness and educating the public both locally and nationally
- Testing and reviewing one another's work (from red-teaming to legal liability)
- Performing multilateral experiments for testing ideas, legality, and scalability of solutions
- Developing and evaluating security standards
- Conducting specialized workshops on specific security issues

Such an interest group could serve as a crossroads where academia, government, and industry can meet. A mechanism for broadcasting the conclusions of future meetings to a larger audience, including government agencies, would be useful. Of course, a collective communication with the government is contingent upon the group reaching consensus on issues first. Engaging the government on this set of issues is in the best interest of everyone, and yet such engagement has failed to materialize in any substantial form. If the group decides to give input to the government, then it should target specific agencies and perhaps even specific individuals in those agencies.

Workshop Agenda

8:30–9:00 Continental Breakfast

9:00–9:20 Welcome—Mike May
Purpose of the Meeting—Sy Goodman

9:20–10:45 *Session I*
Chair—Dave Elliott
Presentations and Discussion
- Cylink, Inc.
- TRW
- Cisco Systems, Inc.
- Sun Microsystems

10:45–11:10 Break

11:10–12:30 *Session II*
Chair—Ed Feigenbaum
Presentations and Discussion
- SRI
- Lockheed-Martin
- EPRI
- SAIC

12:30–1:30 Lunch

1:30–3:00 *Session III*
Chair—Steve Lukasik
Presentations and Discussion
- Sandia
- LLNL
- XIWT
- Stanford CRISP

3:00–3:15 Break

3:15–4:30 *Establishing a Regional Interest Group?*
- *Generating, reviewing, and testing ideas*
- *Research, development, and experimentation*
- *A forum for tracking and influencing government agendas*

Chair—Sy Goodman

List of Participants

Name	Affiliation	Email
David Alderson	Stanford University	alderd@leland.stanford.edu
Matt Barrie	Securify, Inc.	matt@securify.com
Dan Boneh	Stanford University	dabo@cs.stanford.edu
David Borchert	SRI International	borchert@erg.sri.com
William Crowell	Cylink, Inc.	wcrowell@cylink.com
Meiring de Villiers	Stanford University	mdv@leland.stanford.edu
Steve Drenker	EPRI	sdrenker@epri.com
Ekaterina Drozdova	Stanford University	drozdova@leland.stanford.edu
Taher Elgamal	Securify, Inc.	elgamal@securify.com
David Elliott	Stanford University	ddelliott3@aol.com
Edward Feigenbaum	Stanford University	eaf@cs.stanford.edu
Dee Goodman	Stanford University	gooddee@leland.stanford.edu
Sy Goodman	Stanford University	sgoodman@leland.stanford.edu
Mark Graff	Sun Microsystems	mark.graff@sun.com
Gregory Grove	Stanford University	ggrove@leland.stanford.edu
Richard Hafner	EPRI	rhafner@epri.com
Douglas Huey	TRW Electromagnetic Systems	doug.huey@trw.com
John Illgen	Illgen Simulation Technologies, Inc.	jillgen@illgen.com
Rowland Johnson	LLNL	johnson62@llnl.gov
Dan Kolkowitz	Securify, Inc.	kolk@securify.com
Barry Leiner	XIWT	bleiner@cnri.reston.va.us
Stephen Lukasik	Stanford University	slukasik@leland.stanford.edu
Teresa Lunt	SRI International	Lunt@csl.sri.com
Steve Manning	SAIC	steve.a.manning@cpmx.saic.com
Michael May	Stanford University	mmay@leland.stanford.edu
Ed Meyer	Lockheed-Martin	edward.r.meyer@lmco.com
Steve Montoya	Cisco Systems, Inc.	stmontoy@cisco.com
Judy Moore	Sandia National Laboratories	jhmoore@sandia.gov
Erik Naugle	SAIC	erik.t.naugle@cpmx.saic.com
Erich Oehler	Cambridge Technology Partners, Inc.	eoehle@ctp.com
Diana Sackett	LLNL	sackett2@llnl.gov
Sam Savage	Stanford University	savage@leland.stanford.edu
Jeannie Seelbach	SRI International	jeannie_seelbach@sri.com
Kevin Soo Hoo	Stanford University	kjsoohoo@leland.stanford.edu
Mark Stefik	Xerox PARC	stefik@parc.xerox.com
Joan Woodard	Sandia National Laboratories	jbwooda@sandia.gov
John Woods	TRW Electromagnetic Systems	john.woods@trw.com
Ray Zachary	Lockheed-Martin	raymond.a.zachary@lmco.com

Selected Reports, Working Papers, and Reprints of the Center for International Security and Cooperation, Stanford University

To order, call (650) 725-6488 or fax (650) 723-0089. Selected publications and a complete publications list are also available on the center's website at http://www.stanford.edu/group/CISAC/.

Herbert L. Abrams. *Can the Nation Afford a Senior Citizen As President? The Age Factor in the 1996 Election and Beyond*. 1997 (28 pages).

David Alderson, David Elliott, Gregory Grove, Timothy Halliday, Stephen Lukasik, and Seymour Goodman. *Workshop on Protecting and Assuring Critical National Infrastructure: Next Steps*. 1998 (67 pages).

Andrei Baev, Matthew J. Von Bencke, David Bernstein, Jeffrey Lehrer, and Elaine Naugle. *American Ventures in Russia. Report of a Workshop on March 20-21, 1995, at Stanford University*. 1995 (24 pages).

Michael Barletta, *The Military Nuclear Program in Brazil*. 1997 (38 pages).

David Bernstein. *Software Projects in Russia: A Workshop Report*. 1996 (28 pages).

David Bernstein, editor. *Defense Industry Restructuring in Russia: Case Studies and Analysis*. 1994 (244 pages).

David Bernstein, editor. *Cooperative Business Ventures between U.S. Companies and Russian Defense Enterprises*. 1997 (332 pages).

George Bunn and David Holloway. *Arms Control Without Treaties? Rethinking U.S.-Russian Strategic Negotiations in Light of the Duma-Senate Slowdown in Treaty Approval*. 1998 (21 pages).

Irina Bystrova. *The Formation of the Soviet Military-Industrial Complex*. 1996 (28 pages).

Jor-Shan Choi, *A Regional Compact Approach for the Peaceful Use of Nuclear Energy—Case Study: East Asia*. 1997 (65 pages).

David Darchiashvili and Nerses Mkrttchian. *Caucasus Working Papers*. 1997 (41 pages).

John S. Earle and Saul Estrin. *Employee Ownership in Transition*. 1995 (53 pages).

John S. Earle and Ivan Komarov. *Measuring Defense Conversion in Russian Industry*. 1996 (40 pages).

Lynn Eden and Daniel Pollack. *Ethnopolitics and Conflict Resolution*. 1995 (21 pages).

David Elliot, Lawrence Greenberg, and Kevin Soo Hoo. *Strategic Information Warfare—A New Arena for Arms Control?* 1997 (16 pages).

Geoffrey E. Forden. *The Airborne Laser: Shooting Down What's Going Up*. 1997 (20 pages).

James E. Goodby. *Can Strategic Partners Be Nuclear Rivals?* (First in a series of lectures on "The U.S.–Russian Strategic Partnership: Premature or Overdue?") 1997 (26 pages).

James E. Goodby. *Loose Nukes: Security Issues on the U.S.–Russian Agenda* (Second in a series of lectures on "The U.S.–Russian Strategic Partnership: Premature or Overdue?") 1997 (20 pages).

James E. Goodby. *NATO Enlargement and an Undivided Europe* (Third in a series of lectures on "The U.S.–Russian Strategic Partnership: Premature or Overdue?") 1997 (16 pages).

James E. Goodby and Harold Feiveson (with a foreword by George Shultz and William Perry). *Ending the Threat of Nuclear Attack*. 1997 (24 pages).

Seymour Goodman. *The Information Technologies and Defense: A Demand-Pull Assessment*. 1996 (48 pages).

Seymour Goodman, Peter Wolcott, and Patrick Homer. *High-Performance Computing, National Security Applications, and Export Control Policy at the Close of the 20th Century.* 1998 (170 pages).

Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo. *Old Law for a New World? The Applicability of International Law to Information Warfare*. 1997 (48 pages).

Yunpeng Hao. *China's Telecommunications: Present and Future*. 1997 (36 pages).

John R. Harvey, Cameron Binkley, Adam Block, and Rick Burke. *A Common-Sense Approach to High-Technology Export Controls*. 1995 (110 pages).

Hua Di. *China's Security Dilemma to the Year 2010*. 1997 (22 pages).

Leonid Kistersky. *New Dimensions of the International Security System after the Cold War.* 1996 (34 pages).

Amos Kovacs. *The Uses and Nonuses of Intelligence*. 1996 (68 pages).

Allan S. Krass. *The Costs, Risks, and Benefits of Arms Control*. 1996 (85 pages).

Gail Lapidus and Renée de Nevers, eds. *Nationalism, Ethnic Identity, and Conflict Management in Russia Today*. 1995 (106 pages).

Kenneth B. Malpass et al. *Workshop on Protecting and Assuring Critical National Infrastructure*. 1997 (64 pages).

Michael May. *Rivalries Between Nuclear Power Projectors: Why the Lines Will Be Drawn Again*. 1996 (20 pages).

Capt. Alexander Skaridov, Cmdr. Daniel Thompson, and Lieut. Cmdr. Yang Zhiqun. *Asian-Pacific Maritime Security: New Possibilities for Naval Cooperation?* 1994 (28 pages).

Roger D. Speed. *The International Control of Nuclear Weapons*. 1994 (59 pages).

Xiangli Sun. *Implications of a Comprehensive Test Ban for China's Security Policy*. 1997 (24 pages)

Terence Taylor. *Escaping the Prison of the Past: Rethinking Arms Control and Non-Proliferation Measures*. 1996 (65 pages).

Terence Taylor and L. Celeste Johnson. *The Biotechnology Industry of the United States. A Census of Facilities.* 1995 (20 pages).

Dean A. Wilkening. *The Evolution of Russia's Strategic Nuclear Forces*. 1998 (49 pages).

Dean A. Wilkening. *How Much Ballistic Missile Defense Is Enough?* 1998 (44 pages).

Dean A. Wilkening. *How Much Ballistic Missile Defense Is Too Much?* 1998 (36 pages)

Dean A. Wilkening. *A Simple Model for Calculating Ballistic Missile Defense Effectiveness*. 1998 (29 pages).

Zou Yunhua. *China and the CTBT Negotiations*. 1998 (52 pages).

MacArthur Consortium Working Papers in Peace and Cooperation

Pamela Ballinger. *Slaughter ujhyyof the Innocents: Understanding Political Killing, Including Limited Terror but Especially Large-Scale Killing and Genocide.* 1998 (24 pages).

Pamela Ballinger. *Claim-Making and Large-Scale Historical Processes in the Late Twentieth Century*. 1997 (52 pages).

Tarak Barkawi. *Democracy, Foreign Forces, and War: The United States and the Cold War in the Third World*. 1996 (40 pages).

Byron Bland. *Marching and Rising: The Rituals of Small Differences and Great Violence in Northern Ireland*. 1996 (32 pages).

David Dessler. *Talking across Disciplines in the Study of Peace and Security: Epistemology and Pragmatics As Sources of Division in the Social Sciences.* 1996 (40 pages).

Lynn Eden and Daniel Pollak. *Ethnopolitics and Conflict Resolution.* 1995 (21 pages).

Daniel T. Froats, *The Emergence and Selective Enforcement of International Minority-Rights Protections in Europe after the Cold War.* 1996 (40 pages).

Robert Hamerton-Kelly. *An Ethical Approach to the Question of Ethnic Minorities in Central Europe: The Hungarian Case. 1997* (34 pages).

Bruce A. Magnusson. *Domestic Insecurity in New Democratic Regimes: Sources, Locations, and Institutional Solutions in Benin.* 1996 (28 pages).