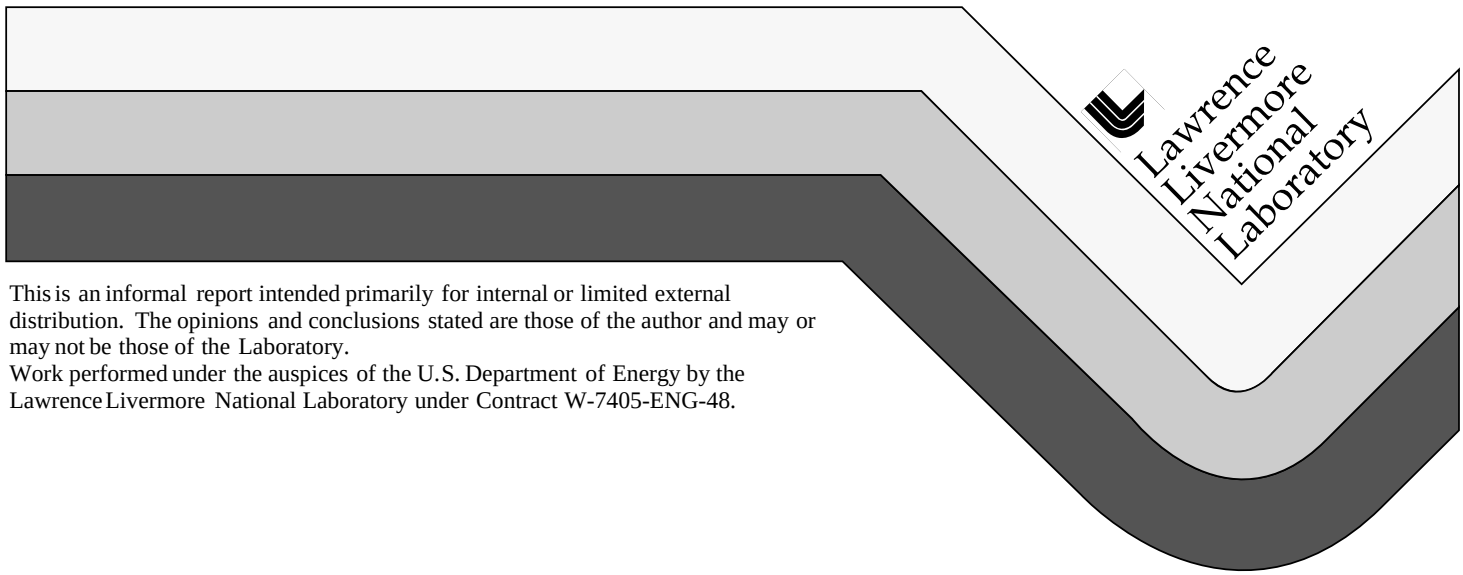
UCRL-ID-128453

Research & Development Priorities for Communications and Information Infrastructure Assurance

W.J. Hunteman
S.E. Jacobsen
W.E. Johnston
D.L. Mansur
K.C. Bailey

June 1997



Work performed under the auspices of the U.S. Department of Energy by the Lawrence Livermore National Laboratory under Contract W-7405-ENG-48.

Research & Development Priorities for Communications and Information Infrastructure Assurance

William J. Hunteman (Los Alamos National Laboratory)
Sharon E. Jacobsen (Oak Ridge National Laboratory)
William E. Johnston (Lawrence Berkeley National Laboratory)
Douglass L. Mansur and Kathleen C. Bailey (Lawrence Livermore National Laboratory)
June, 1997
UCRL-ID-128453, CSTC 97-134

EXECUTIVE SUMMARY

This report outlines the research and development priorities required over the next five years in order to assure that the communications infrastructure (the public switched network and the global Internet) and information infrastructure (the millions of computer systems that store, organize, and analyze the information on which our society increasingly relies) are as secure as possible from potential attacks and/or natural disasters. Recent data[1] indicate that attacks on and accidents involving the infrastructure are increasing and known vulnerabilities are rapidly expanding. In addition, the nation's growing dependency on the infrastructure heightens the need to implement the recommendations in this report. The measures needed to provide such assurance are very complex; they must provide reliability, integrity, confidentiality, and access control of everything from telephone switch configuration instructions to personal medical records.

Deficiencies that must be addressed are diverse, including: better operational procedures for some well-understood technologies; improved, more correct design and implementation of security technologies; cost-benefit tradeoff analyses to enable effective use of technologies; and intellectual capital and

[1] "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks," Chapter Report, May 1996, General Accounting Office, GAO/AIMD-96-84, <http://www.fas.org/irp/gao/aim96084.htm>.

Table 1: RESEARCH & DEVELOPMENT NEEDS

Most Important R & D Needs
1. Characterization and Notification of Threats
2. Detection, Analysis, and Prevention
3. Definition of Security Architectures
5. Advanced Concepts and Theory
6. Management of Information Protection
Very Important R & D Needs
7. Characterization of Infrastructure Required for Minimum Essential Services
8. Valuation of Information
9. Indication and Warning
10. Cost-Benefit Analysis
Important R & D Needs
11. Modeling and Simulation
12. Risk Management
13. Encryption Technologies

4. Response, Recovery, and Reconstitution

Note: R&D needs are not further prioritized within

fundamental concepts to provide the required solutions. The research and development (R&D) priorities are listed in Table 1. Longer range activities in all of the areas are also needed to support future, unknown versions of the infrastructure, as well as new vulnerabilities and threats.

This report also briefly addresses some other significant issues. For example, it is important to balance individual privacy with the pressures to make ever more information available on the Internet.

This report was authored by security experts at four Department of Energy National Laboratories, and was reviewed by several experts from government, industry, and academia. There was general agreement on the list of R&D topics, but there was less agreement on their prioritization.

1.0 INTRODUCTION

The communications and information infrastructure[2] is integral to U. S. national security and U. S. economic competitiveness. Most experts agree that the infrastructure is essential to the functioning of our society and is fragile. The existing infrastructure cannot adequately defend or heal itself. Without continual vigilance and renewed efforts to bolster security, the infrastructure will degrade or fail in event of attack or disaster. Significant new investment and effort in research and development (R&D) is required to protect not only the communications infrastructure, but also the information created, stored, processed, and transmitted on it. The urgent need to develop new means of protection is apparent, given the possibility of major attack or natural disaster, the increasing rate of incidents, the expanding list of known vulnerabilities, and the inadequate set of solutions available.

This report is a brief summary of the R&D areas that must be addressed to help assure the protection and survivability of the communications and information infrastructure. This report has been reviewed and commented upon by experts in government, industry, and academia, for which the authors express their appreciation. The authors did not evaluate R&D requirements in terms of cost, time, or funding sources. Rather, judgments are based on need, using the criteria outlined below (See Section 3.0). The authors view the topics as essential, but the list is not intended to be exhaustive. Prioritization of the list was difficult, as many of the subjects are overlapping, and arguments can be presented that would reduce or enhance the ranking of each.

2.0 THE SCOPE OF THE INFRASTRUCTURE

[2] The communications and information infrastructure is the basis of the national information infrastructure (NII); the terms are not synonymous.

The communications and information infrastructure consists of three primary aspects: an underlying "link" layer that moves data from point to point; a network and transport layer that deals with addressing, routing, and data transport services; and the data manipulation components (computing systems). The combination of these provide a full spectrum of communication, computation, control, information, and human collaboration systems. Most wide-area data networks use "public switched networks"—the system of control centers, communication lines, and circuit switches that are maintained and operated by the telecommunications industry—for their link layer. Internet technology differs from the public switched network primarily in that all communication is accomplished by breaking the data streams that provide all of the services mentioned above into "packets" that are independently routed through an inter-network. Every component of every layer relies on computer control, and increasingly Internet communication is being used to provide control and management of the components of the layers below the Internet, i.e., the public switched network and the routing infrastructure of the Internet itself. [3]

Most modern computer applications use Internet technology for communication, whether through the global, public Internet, or in private (isolated) corporate Internets (sometimes called "Intranets").

The final layer of the infrastructure is the computing systems that generate, manipulate, store, display, or control by using information, facilitating human collaboration and creative activities, etc.

This combined communications and information infrastructure is the basis of our modern information society. The future scope of the infrastructure is difficult to predict, but current trends suggest that it will be directly involved in virtually every aspect of our lives—from energy management of household appliances by energy utilities, to tele-robotic surgery, to remote control of manufacturing; from delivery of every form of multimedia information and entertainment, to the provisioning of our country's defensive capabilities. Therefore, the consequences of disruption, subversion, corruption, or monitoring of this infrastructure will be roughly equivalent to disabling events happening today simultaneously to the telephone, broadcast, and electric power systems.

Many of the research and development issues for securing the infrastructure from attack are common to all of the communications and information infrastructure components. What differs between the layers are the specific techniques, consequences, and recovery procedures. Vulnerabilities at each level provide opportunities (threats of) monitoring, penetration, masquerading,

---

[3] "Internet/Public Switched Network (PSN) Interconnectivity and Vulnerability Report," Customer Service and Information Assurance Division, National Communications System, <http://www/ncs.gov/n5_hp/html>.

subversion (of correct operation), and denial of service.[4] The prevention, detection, impact, and recovery from these actions, as well as their analogs that are due to human or system failure, or natural disaster, are the subject of the research and development agenda of this report.

3.0 CRITERIA FOR PRIORITIZATION

Ideally, R&D needs would be determined according to a set of criteria developed from functional needs and experience—particularly the number and type of actual attacks. However, attacks against the infrastructure are poorly reported in the United States and many surely go undetected. The lack of solid information on threats, attacks, vulnerabilities, and interdependencies is a severe constraint on making informed judgments about infrastructure protection. Available data indicate a growing variety of attack methods as well as an increase in number and sophistication. However, despite the absence of solid data, decisions on R&D must be made. The working group therefore assessed R&D needs against the questions listed in Table 2. These questions take into consideration whether the R&D topic would result in immediately usable, useful products, and whether they address the greatest risks and threats. They also address the question of whether the result would be consonant with the existing infrastructure, or substantial—perhaps unacceptable—changes would have to be made before the product could be used. It should be noted that many of the changes that might result from the suggested R&D will require significant changes to commercial operating systems and application products.

Table 2: Criteria for Prioritizing R&D Needs

Note: Criteria are not prioritized.

- Does the R&D topic or activity address significant threats to national security and U. S. economic competitiveness?
- Will the R&D results significantly reduce vulnerabilities?
- Will the R&D results have near-term, versus long-term, impact?
- Is the R&D objective achievable? Is the product of the R&D deployable once completed?

These criteria should be part of a continuous process of assessment and re-evaluation. Each review of R&D needs should identify some near-term and some long-term goals to assure both a flow of useful results into the commercial systems community and a consideration of likely future issues for software and systems.

[4] "The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications: An Awareness Document," Information Assurance Branch, National Communications System, <http://www/ncs.gov/n5_hp/html>.

4.0 ASSUMPTIONS ABOUT FUTURE INFRASTRUCTURE

Assumptions about the future clearly play a role in determining R&D needs. For example, mobile and wireless computing may be used on a vast scale. It may be possible to control the manufacture of products and the operation of scientific laboratories remotely. Distribution and use of multi-media over the communications and computer networks may be common. Much of the nation's business will be conducted over the Internet. Current work in active networks—networks whose behavior can be changed by the data they are carrying—may lead to new and unexpected vulnerabilities in the routing infrastructure. Normally functioning adaptive systems—those that change their behavior according to the content of the information they are processing—may change in ways that cause the security requirements to change dynamically. And, the infrastructure will extend throughout the industrialized world and to large populations in less developed countries. Such changes will raise some security issues that we can fairly safely predict. For example, infrastructure extension will expose more users and systems to attack. Also, increased computing power and storage will enhance the abilities of attackers to break encryption algorithms, aggregate information, and develop more sophisticated attack methods.

The use of computer networks, particularly the Internet, is the fastest growing segment of telecommunications. One of the reasons for this is the tremendous versatility and power inherent in coupling computing and communications—as the Internet and the public switches (carrier) networks do for their own internal operation. The range of services offered over the Internet grows daily because the protocols required to support new services are easily added to the associated computers. This has, for example, lead to many new multimedia services that were not even research topics a few years ago. On the other hand, this flexibility endows the Internet with many of the same vulnerabilities as general computer systems. However, since this flexibility is a major strength, the coupling between communications and computing will increase rather than decrease, and this will lead to new vulnerabilities in the infrastructure.

As the complexity of systems continues to increase, understanding the security implications of changes and new developments will be more difficult. Synergism between systems is equally complex, making it hard to determine the consequences on the total infrastructure of failure in one system.

Many aspects of infrastructure evolution are difficult or impossible to predict. As they occur, they will generate issues not currently anticipated. It is therefore crucial that the R&D priorities list regularly be updated and reevaluated.

5.0 OTHER IMPORTANT NEEDS

There are priority needs that are not R&D topics, but which are vital to the success of R&D activities. For example, there is a requirement for enhanced academic education and for diversification of research. There are too few students entering the field of communications and information protection, and there are too few academic institutions with relevant, high-quality research programs. More academic institutions should have curricula and degrees related to communications and information protection, which, in turn, requires support for course development and computing resources for students. Current research topics and objectives are too limited. It is important to foster creativity by assuring that research groups and individual researchers are consistently funded.

Legal questions relating to liability must be resolved.[5] In event of an attack on the communications and information infrastructure, what responses are allowable, legal, and acceptable? Also, who has legal jurisdiction to investigate or prosecute? Many legal issues immediately arise when virtually any individual or group of individuals can make an electronic visit to our country without the protocol and checks and balances employed for a physical visit. Perhaps one solution to the jurisdiction issue is to establish virtual borders that will enclose domains where certain rules and laws will apply.

Questions associated with privacy and anonymity also must be addressed. Currently, it is possible to aggregate data from multiple sources—such as from social security, medical, and government files—to learn information about individuals and businesses that, in the world of paper files, would be considered confidential. Further, there are many modes of communication and interaction in society that provide anonymity, and people will expect comparable capability from the infrastructure. Governments are currently working to define principles to insure privacy,[6] but implementation of the principles will depend on an effective security. The solution to the privacy question will be complicated by the need to reconcile the means of protecting privacy with the technologies and policies related to detecting and responding to intrusion. Once legal and privacy issues are resolved, industry will be more willing to devote substantial R&D resources in areas they once may have avoided due to fear of liability or litigation.

---

[5]For a discussion of some of the legal problems, see "Information Warfare: Legal, Regulatory, Policy, and Organizational Considerations for Assurance," Joint Chiefs of Staff, US Department of Defense, July, 1996 <http://www.infowar.com/mil_c4i/joint/joint.html-ssi>

[6]Examples include: "Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information", Privacy Working Group, Information Policy Committee, Information Infrastructure Task Force, <http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html>, and "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," <http://www2.echo.lu/legal/en/dataprot/directiv/directiv.html>.

To design and implement effective countermeasures, and to make effective decisions about the use of resources, the research and development community must have more information about vulnerabilities, threats, and incidents. There must be enhanced collection and dissemination of intelligence information (both foreign-origin and domestic) on the nature and extent of threats to the communications and information infrastructure. Security classification and information-handling guidelines must be reassessed to maximize dissemination of threat and vulnerability information so that this information can be made widely, though not necessarily openly, available. Many individuals who do not possess security clearances must have access to this information.

The United States should initiate cooperation agreements, and lead collaboration efforts, to develop and enforce infrastructure protection measures. At the same time, care must be taken to develop key security software in the United States. Currently, a significant amount of U.S.-produced consumer software has security capabilities that are produced by contractors in Finland, Australia, Germany, and Russia. For example, Netscape selected a German company to provide security software and Sun Microsystems security software is produced by a Russian company. U.S. policies and laws, including a reasonable encryption policy, should support domestic production.

6.0 RESEARCH & DEVELOPMENT PRIORITIES

Table 1 lists the areas for R&D needed to protect and preserve the national communications and information infrastructure. The list, which is not necessarily comprehensive, has been reviewed by several experts from government, industry, and academia. The list is divided into three categories, and items within the categories are not further prioritized. It could be argued that the overall prioritization is not meaningful, because all of the R&D areas are vital to the future. The authors acknowledge that setting priorities is exceedingly difficult, but have categorized R&D needs to assist decision-makers in allocating urgently needed resources.

6.1 MOST IMPORTANT R&D NEEDS

1. Characterization and Notification of Threats: The identification, collection, organization, and dissemination of information on potential threats and attacks.

The threat posed by an attack does not necessarily depend on whether its origin is international or national because widespread connectivity (via the Internet and other international systems) gives people in and out of the country equal potential for aggression. However, the implication of threats will vary, depending on the target—international, national, corporate, or individual—and on the objective—information warfare, terrorism, espionage, crime, or mischief.

A methodology is required to identify and characterize threats with varying motivations and from all origins.

Proper characterization of threats will require information about the capabilities and intent of potential attackers, as well as their veracity and potential impact. This may, in turn, require new approaches to intelligence collection. Meaningful information must be systematically sanitized to an appropriate classification level to permit sharing among government, commercial, and private organizations.

In addition to intelligence gathering and dissemination, there is a need to develop the means by which data on threats, attacks, and consequences can be reported without the reporter of such incidents being punished. This might enhance reporting of incidents. One model might be the National Transportation Safety Board's incident reporting system for pilots.

The methodology should also support the identification, collection, organization, and dissemination of low-level attack information, such as viruses and their automatic detection and removal. Also, methodologies should be developed to relate known vulnerabilities and threats to specific defenses, and to recognize patterns in the nature and types of threats posed.

2. *Detection, Analysis, and Prevention: The identification, collection, organization, and dissemination of system, network, and infrastructure vulnerability information; and, the development of methodologies to avoid, reduce, or eliminate vulnerabilities while developing or integrating hardware and software products. The development of techniques to identify and analyze actual or suspected intrusions.*

Vulnerability issues:

Designing computer systems correctly, so that they are robust and well protected, is the objective. An additional goal is to identify vulnerabilities in administrative controls for operating and managing computer systems. Until this is achieved, however, detection and response may be the best approach to protecting information and communications infrastructure.

- Theoretical work is needed to expand fundamental knowledge, including the definition and taxonomies of vulnerabilities, and development of new approaches to detection (e.g., policy-based detection rules).

- Measures of effectiveness or metrics must be developed to gauge the effectiveness of both hardware and software in avoiding, reducing, or eliminating vulnerabilities—particularly when different software components are integrated or composed into an single information environment.

- In addition to building secure software from the outset, much can be done to improve testing methods and other after-the-fact approaches to protection. The theory and practice of testing, to include testing criteria, needs to be greatly improved.

Intrusion issues:

Intrusion detection systems are able to detect large numbers of attacks or suspicious short-term changes in user or system behavior,[7] but there are a number of related areas that need R&D. For example, current systems have a high false alarm rate, and an unknown but probably very high false negative rate. Specific topics for R&D in the area of vulnerability detection, analysis, and prevention include:

- Definition of infrastructure-wide attacks and a scaling of existing intrusion detection systems to many thousands of nodes.

- Intrusion detection systems must be measured using standardized methods to demonstrate how well they detect and respond to attacks.

- New approaches are needed to address vulnerabilities that will arise from, for example, autonomous agents (software automatically received and executed without explicit user action), virtual networks, and multimedia/collaboration systems.

3. Definition of Security Architectures: The organization of security components and services to provide confidentiality, integrity, and availability for information and communication systems.

Information protection architectures organize individual security components and services into working systems that provide information and resource confidentiality, integrity, and availability. Architectures specify how protection protocols and data exchange interfaces allow the interoperation of security components. The role of well designed and tested architectures is becoming steadily more important as the security services themselves become distributed like the systems that they protect, and as individual security services start to be provided as independent modules by the software industry.

Currently, significant effort is being devoted to defining public-key cryptography-based security architectures because this approach works well in distributed computing environments. Public-key approaches appear to have considerable potential for addressing a wide range of current vulnerabilities in

[7]For details on the current state of the field and some of the major R&D requirements on intrusion detection systems, see National Infosec Technical Baseline: Intrusion Detection and Response, report to the Infosec Research Council, October 1996, (http://doe-is.llnl.gov/nitb/ids.html).

the infrastructure. However, there is little real experience in the deployment and operation of these architectures and infrastructures. Over the next several years, the ease of operation, scalability, strength against attack, and interaction with other communication and information infrastructure components will all be significant R&D topics.

Research and development of architectures must address standards for evaluating information protection when different tools and measures are combined in the infrastructure**.** Currently, most protection systems cannot directly interact with security products from other vendors. For example, intrusion detection systems and firewalls function as independent elements, with only a small amount of work being done to make them cooperate and collectively detect, analyze, share, and react to information. Standards for emerging technologies—which should include well-tested, high-confidence "reference implementations"—will help ensure the interoperability of information protection capabilities, including the exchange of information protection information across different hardware platforms, operating systems, network topologies and the integration of information protection information received from other applications and tools. An important component of this effort, of course, will be development of methods to review the abilities of products to meet the standards.

Architectures need to be characterized for robustness, scalability, and for overall strength of security. They need to be analyzed with respect to providing security services to a diverse set of uses, as noted above. Some of the use scenarios are relatively straightforward, and others, like the new Nimrod architecture for Internet routing, are very diverse and complex in their security requirements and in their demands on the security architectures.[8] These architectures must also protect non-traditional computing systems, such as very small systems involved in management of household energy demand and automated traffic control.

Yet another need to be addressed by security architectures is streamlining performance of protective systems to reduce the costs of using them—particularly in terms of time and ease of operation. For example, it is common practice for organizations to deactivate encryption to reduce costs and increase system performance. Key management over a large population is complex and often requires more resources than organizations are willing to invest. Therefore, it is critical for less complex, less resource-intensive tools and methodologies to be developed.

The architecture R&D activity should also investigate, and incorporate where feasible, advanced information protection concepts, such as information that carries its own use conditions with it. This would allow consistent enforcement

[8] "Securing the Nimrod Routing Architecture," K. Sirois and S. Kent, Symposium on Network and Distributed System Security. February 1997, San Diego, CA.

of the protection requirements whenever and wherever the information is accessed, independent of the operating system or storage device where the information is located. Investigation into the use of advanced concepts will support and encourage other government and commercial organizations to consider revolutionary approaches to information protection that could improve protection and reduce costs.

4. Response, Recovery, and Reconstitution: The development of methodologies to contain, stop, or eject intruders, and to mitigate damage or restore information processing services in event of attack or disaster.

As mentioned above and below, detection of intrusion or attack is essential to protecting the communications and information infrastructure. In addition, methods must be developed to reject, eject, and/or contain intruders—at all stages of all types of attacks, including those designed for denial of service—and to respond to major disasters of natural origin. This will require R&D on the means to successfully automate a response to an attack or disaster because, given the short time frame of such events, human intervention will not be possible or adequate in most cases. However, a fully automated response can generate a new set of problems. For example, an attacker may be able to use knowledge of the defending system for offensive purposes (such as an attacker sequentially throwing five improper passwords at every account on a system, knowing that some systems will then shut down access to all accounts to "defend" itself). A few intrusion detection systems are now incorporating response mechanisms that can control routers and other network components. Much more research and operational experience is required to identify other mechanisms and actions that are beneficial without causing inadvertent harm.

Tools and techniques for identifying perpetrators, tracing them back, and supporting prosecution need to be developed. A meaningful component of protection is deterrence.

Recovery and reconstitution techniques, both manual and automated, are also needed to determine what damage has been caused and to what systems, how to limit further damage, and how to bring systems back to a secure and usable state. This is an especially complex problem in the communications infrastructure, where the notion of "system" is poorly delineated: outages or failures in certain parts of the communications infrastructure may have wide-ranging effects.

Additional topics for this R&D work include defining: how much recovery or reconstitution is necessary, who should initiate the recovery process, when should the recovery process be initiated, who is responsible for performing the recovery action, and who is responsible for determining the scope of the recovery effort.

5. Advanced Concepts and Theory: Fundamental research into the protection of information.

Considerable R&D is needed to provide the proper theoretical base that will protect the communications and information infrastructure and support different paradigms, models, and implementations. Fundamental research to generate new concepts is required on: intrusion detection, malicious software, access control, authorization, authentication, composability, interoperability, denial of service, system complexity, information protection policy development and use, reconstitution and recovery for all levels of the infrastructure, and distributed hardware and software approaches.

6. Management of Information Protection: The development of methodologies and tools for the application and management of information protection in communication and information systems.

Methods and techniques for the use and management of information protection methods, tools, and practices are needed to support correct operation of the infrastructure. Improved methods for remote and local configuration management of the infrastructure components are needed. The methods and techniques must also anticipate and support advanced infrastructure and networking concepts, such as active networks and adaptive systems.

In the emerging communications infrastructure of the Internet, the notion of management methods and techniques for protection again becomes very complex because of the interaction of many independently managed routing systems and domains on which the Internet depends. With the transition from the centrally managed Internet when the National Science Foundation organized a small number of contractors, to the free enterprise free-for-all of today where non-interoperating methodologies are the norm, the importance of commonly agreed on and well understood management of information protection methods is both more important and complex than ever before.

6.2 VERY IMPORTANT R&D NEEDS

7. Characterization of Infrastructure Required for Minimum Essential Services.

Research should be conducted on the communications and information infrastructure required to support essential government services and military communications and operations in the event of degradation or failure of the infrastructure.

8. Valuation of Information: The development of methodologies and tools to assist information owners in determining what protection is appropriate for information, and in evaluating the impact of aggregated information.

Methodologies should be developed to assist information owners in understanding the value of information, which will enable them to judge what, where, and how much protection is needed. The methodology should help determine what information assets are critical, and thus aid in the priority use of resources in a degraded environment. A consideration in this R&D must be the effect of aggregation of information because it is increasingly easy for nefarious individuals or entities to cull data from multiple sources to acquire a "picture" or "report" that would otherwise be considered sensitive or confidential.

9. Indication and Warning: Identification and reporting of the precursors of an attack, or an actual attack, on the infrastructure.

Indication and warning differs from detection in terms of scale, methods, and timeframe. The tools useful for detecting intrusion on a local or individual level will not apply in event of an attack on the infrastructure as a whole. Today, the research community is just beginning discussion on indications and warning, as they relate to a nationwide or global perspective. Specific measures and analysis methods are needed to recognize a large-scale attack or its precursors. Manual methods, such as means to improve communication between existing incident handling teams, may be required until automated indications and warning systems become available.

10. Cost-Benefit Analysis: Development of methodologies and tools to compute return-on-investment in competing security technologies.

Further research is needed in the area of cost-benefit analysis of security technology. Issues to be considered include: human factors, coverage, direct and indirect costs (initial purchase and long-term management costs). Much of this work is dependent on other issues which have been discussed, such as the availability of solid incident and threat information, and measures of effectiveness.

6.3 IMPORTANT R&D NEEDS

11. Modeling and Simulation: Development of methodologies and tools for understanding the behavior of complex information systems.

One of the best methods for understanding the behavior of complex systems is to create modeling and simulation environments. Currently our understanding of the effects of various attacks and defenses on large scale networks is in its infancy. Research into methods for graceful degradation and recovery, methods for determining critical nodes and resources, measuring the value of building in certain levels of redundancy, and many other issues can be explored at both the micro and macro levels with properly constructed modeling and simulation systems. Furthermore, the loss of portions of the communications and information infrastructure should be analyzed as to their impacts on other areas

such as energy and transportation. Modeling has the advantage of allowing experimentation which cannot be performed in realistic environments of any appreciable scale. Tools and techniques to validate models and simulation are necessary.

12. Risk Management: Development of methodologies and tools to evaluate and manage risks in the communications and information infrastructure.

Development of methodologies and tools are needed to identify and minimize the impact of risks to the infrastructure and information. Research areas would include: evaluation of threats and vulnerabilities; methodologies for formulating management decisions based on operational missions and information value; methodologies for dealing with uncertainties in or incomplete knowledge of threats, vulnerabilities, and protection measures; and managing risk across the multiple components and organizations involved in the infrastructure.

13. Encryption Technologies: Development and evaluation software, firmware, and hardware encryption technologies.

Research is needed to develop a comprehensive methodology and criteria for evaluating and weighing the many types of cryptography, as well as updated information about the features and limitations of implemented encryption as it applies to software, firmware, and hardware. Other research issues include development of technologies such as scalable encryption and very fast digital signature, which is critical, for example, for packet authentication in network-level security.

7.0 SUMMARY AND CONCLUSION

Significant research and development is needed to assure that the communications and information infrastructures are secure from natural disasters or attacks. This report has outlined some of the areas which should receive priority effort and resources to provide the infrastructures with continuing reliability, integrity, confidentiality, and access control. The R&D topic areas are summarized in Table 3, along with a ball-park estimate for each of the required investment by industry and/or government.

TABLE 3: TECHNOLOGY R&D PRIORITIZATION AND CHARACTERIZATION[a]

R&D Programs (by Topical Area)	Applicable Assurance Objective(s) [b]	Technological Potential/Risk [c]	Development Timeframe	Federal R&D Role	Estimated Investment [d]
Characterization and Notification of Threats	P, M, I	M	L	H	$300M
Detection, Analysis and Prevention	P, M, I	H	L-H	H	$100-150M
Definition of Security Architectures	P, M, I, R	H	L-H	M	$500-700M
Response, Recovery, and Reconstitution	M, I, R	M	L-M	M	$50-100M
Advanced Concepts and Theory	P, M, I, R	M-H	M-H	H	$50-100M
Management of Information Protection	P, M, I, R	M	L-M	L-M	$30-50M
Characterization of Infrastructure Req. for Minimum Essential Serv.	M, I, R	H	L	H	$50-75M
Valuation of Information	P, M, R	H	L-M	M-H	$20-40M
Indication and Warning	P, M, I	M-H	L-M	H	$50-75M
Cost-Benefit Analysis	P, M	L-M	L-M	M	$20-40M
Modeling and Simulation	P, M, I, R	L-M	L-M	H	$100-200M
Risk Management	P	L-M	L-M	H	$100-200M
Encryption Technologies	P	H	L-H	M	$300-500M

[a] The authors considered R&D resources required only for the next five years. R&D will, of course, be required beyond that timeframe.

[b] P, M, I, and R = Prevention, Mitigation, Incident Management, and Recovery

[c] H, M, and L = High, Medium, and Low

[d] Estimate (rough order-of-magnitude range) of the overall investment required to complete the R&D to the point of commercialization.

Technical Information Department • **Lawrence Livermore National Laboratory**
University of California • Livermore, California 94551