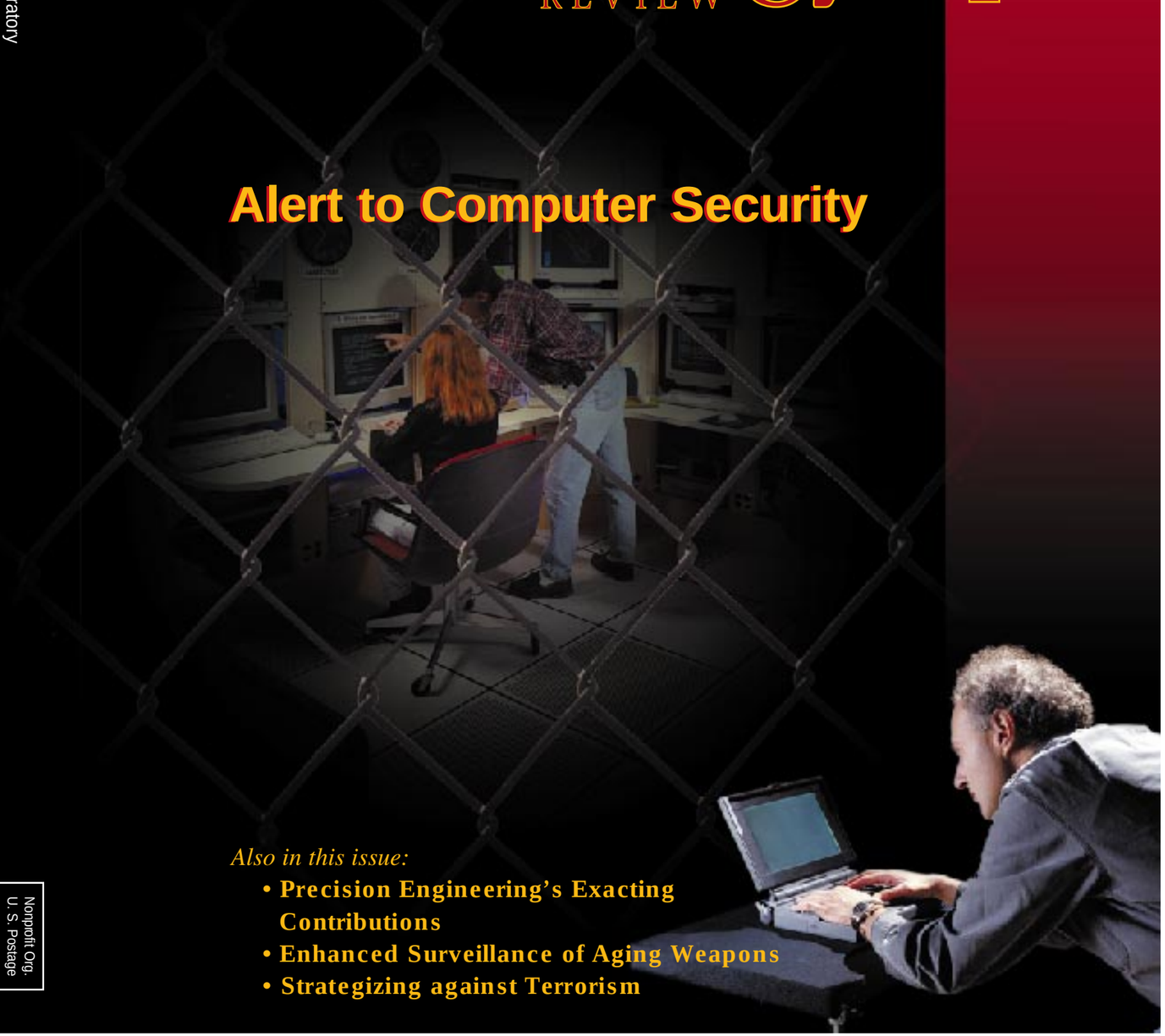
January/
February 1998

Lawrence
Livermore
National
Laboratory

Science & Technology REVIEW

Alert to Computer Security



Also in this issue:

- **Precision Engineering's Exacting Contributions**
- **Enhanced Surveillance of Aging Weapons**
- **Strategizing against Terrorism**

University of California
Lawrence Livermore National Laboratory
Science & Technology Review
P.O. Box 808, L-664
Livermore, California 94551

Nonprofit Org.
U. S. Postage
PAID
Albuquerque, NM
Permit No. 853

Printed on recycled paper.

About the Cover

The Department of Energy and the Laboratory have come to rely increasingly on advanced computer capabilities to fulfill their national security mission. In so doing, they have realized that one of their greatest strengths can also be vulnerable to intrusion and sabotage. Accordingly, they have developed capabilities and tools to secure and protect their invaluable computational resources. This month's cover shows Laboratory computer scientists Kathryn Call and Phil Cox at work protecting the computer systems and networks at Livermore and across the DOE complex. Call and Cox are part of the Computer Security Technology Center at Livermore. The center provides response to breaches in computer security and develops advanced security tools for computer systems. The article describing this work begins on p. 4.

Cover photos: Michael Anthony. Cover design: George Kitrinos

What Do You Think?

We want to know what you think of our publication. Please use the enclosed survey form to give us your feedback.

Electronic Access

S&TR is available on the Internet at *http://www.llnl.gov/str*. As references become available on the Internet, they will be interactively linked to the footnote references at the end of each article. If you desire more detailed information about an article, click on any reference that is in color at the end of the article, and you will connect automatically with the reference.

About the Review

Lawrence Livermore National Laboratory is operated by the University of California for the Department of Energy. At Livermore, we focus science and technology on assuring our nation's security. We also apply that expertise to solve other important national problems in energy, bioscience, and the environment. *Science & Technology Review* is published ten times a year to communicate, to a broad audience, the Laboratory's scientific and technological accomplishments in fulfilling its primary missions. The publication's goal is to help readers understand these accomplishments and appreciate their value to the individual citizen, the nation, and the world.

Please address any correspondence (including name and address changes) to *S&TR*, Mail Stop L-664, Lawrence Livermore National Laboratory, P.O. Box 808, Livermore, California 94551, or telephone (510) 422-8961. Our electronic mail address is *hunter6@llnl.gov*.

Prepared by **LLNL** under contract No. W-7405-Eng-48

S&TR Staff

Scientific Editor
J. Smart

Managing Editor
Sam Hunter

Publication Editor
Dean Wheatcraft

Writers
Lauren de Vore, Katie Walter, and Gloria Wilt

Art Director and Designer
Ray Marazzi

Internet Designer
Kitty Tinsley

Compositor
Louisa Cardoza

Proofreader
Al Miguel

S&TR is a Director's Office publication, produced by the Technical Information Department, under the direction of the Office of Policy, Planning, and Special Studies.

Printed in the United States of America

Available from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road
Springfield, Virginia 22161

UCRL-52000-98-1/2
Distribution Category UC-700
January/February 1998

Science & Technology REVIEW

January/February 1998

Lawrence Livermore National Laboratory

2 The Laboratory in the News

3 Commentary by David Cooper
Protecting the Global Connection

Features

4 **Making Information Safe**
Lawrence Livermore's Computer Security Technology Center is an important resource for information safety. It provides a response capability for computer incidents and has developed advanced tools to actively manage and defend system security.

12 **Engineering Precision into Laboratory Projects**
Livermore engineers are bringing greater precision to experimental physics ranging from the National Ignition Facility to linear accelerators to the lithography for making the next generation of computer chips.

Research Highlights

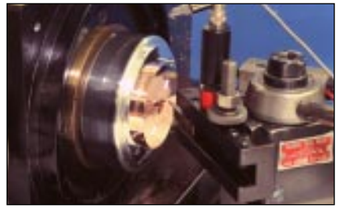
21 **Enhanced Surveillance of Aging Weapons**

24 **A National Strategy against Terrorism Using Weapons of Mass Destruction**

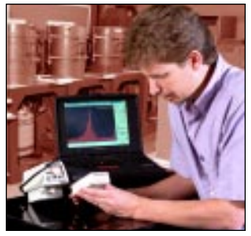
27 Patents and Awards

Abstracts

Page 4



Page 12



Page 24

Lab bugs vs old bombs

Nicknamed "Bugs against Bombs," a new research effort is aimed at turning explosive chemicals from old nuclear weapons into the same nonhazardous elements that make up water and air.

The University of California announced last September that its joint research with Lawrence Livermore has been so successful that a new plant based on the technology will be built later this year.

Biomedical scientists are feeding ethanol to microorganisms, causing them to produce enzymes that can neutralize toxic waste from old bombs, converting it to nitrogen, water, and carbon dioxide.

The technique has been applied in tests at the Department of Energy's bomb-dismantling plant in Amarillo, Texas. The next tests will be at an Army depot in Hawthorne, Nevada, where the new technique is expected to cut treatment costs in half.

Lawrence Livermore researchers John Knezovich and Jeffrey Daniels are working on the project with civil and environmental engineers at the University of California at Los Angeles. (See *S&TR*, July/August 1997, pp. 21–22.)

Contact: John Knezovich (510) 422-0925 (knezovich1@llnl.gov).

NIF, AVLIS, ASCI funded in new federal budget

The U.S. House of Representatives in September approved funding for the National Ignition Facility (NIF), Atomic Vapor Laser Isotope Separation (AVLIS), and the Advanced Strategic Computing Initiative (ASCI) at Lawrence Livermore. Funding for these programs was included in the Energy and Water Appropriations Act for Fiscal Year 1998, which was approved overwhelmingly by a vote of 404 to 17.

"Individually, the biggest winners are the 600-plus AVLIS employees who no longer have to fear being laid off within the next month," Representative Ellen Tauscher said in announcing the funding. "The other big winner is the NIF program, because we were able to secure the entire $229 million that was requested earlier this year."

For AVLIS, the total amount obligated by the DOE will not exceed $60 million. This provision will permit the continued development of the AVLIS technology until the United States Enrichment Corporation is sold.

The ASCI program received a total of $224.8 million for FY 1998, which represents a $20-million increase over previously approved allocations.

Contact: LLNL Media Relations (510) 422-4599 (garberson1@llnl.gov).

Labs to study ways to make explosions cleaner

Concern about the levels of pollutants released when outdated or excess munitions are destroyed has prompted the Department of Defense to ask Livermore's two national security laboratories—Sandia and Lawrence Livermore—to study ways to make those explosions cleaner.

So far, the U.S. Environmental Protection Agency has been satisfied that small quantities of toxic gases released when old or excess weapons are exploded are not making anyone sick. Last year, the Defense Department exploded 120,000 tons of unwanted munitions, compared to 60,000 to 80,000 tons in more typical years, and there is still an additional 500,000 tons to dispose of. As the disposal continues, the emissions could rise to unhealthy levels.

The Defense Department is investing $6 million per year for five years in experiments that may yield ways to completely neutralize the gases, which include small quantities of hydrogen cyanide and carbon monoxide.

A first round of experiments—in underground chambers last year at the old nuclear testing grounds in Nevada—was aimed at finding out what gases are being emitted in what quantities.

A second round, scheduled for late this winter, will include testing of possible solutions. For example, adding oxygen to the process could help all the gases burn completely, converting them to water and carbon dioxide rather than letting them waft away as smoke. Other solutions involve variations in the configuration and placement of the munitions when they are destroyed.

Contact: LLNL Media Relations (510) 422-4599 (garberson1@llnl.gov).

It's official: element 106 is named seaborgium

Ending a three-year controversy, the International Union of Pure and Applied Chemistry (IUPAC) approved the recommendations for names of elements 101 through 109, making the name seaborgium official for element 106. The element is named for Dr. Glenn Seaborg, who has been associated with the discovery of ten new elements.

The fourteenth transuranic element produced by human beings, element 106 was synthesized in the 1970s by collaborators at Lawrence Berkeley and Lawrence Livermore laboratories. Almost simultaneously, a group of Russian scientists claimed that they, too, had synthesized element 106. The American discovery later was confirmed to be correct, but the Russian discovery could not be confirmed.

The American group consisted of Seaborg, Al Ghiorso, J. M. Nitschke, J. R. Alonso, C. T. Alonso, and Matti Nurmia, from Berkeley, and E. K. Hulet and R. W. Lougheed from Livermore.

IUPAC's recommendations carry no legal force but are normally viewed as authoritative throughout the world. IUPAC President Albert Fischli pointed out that the process of proposing provisional recommendations, soliciting comments from the chemistry community, and making revisions where indicated has worked well. "Unfortunately, with conflicting claims and preferences, it has not been possible to devise names that are completely satisfying to all the laboratories involved in these discoveries," he said. "I believe that the final recommendations come close to achieving our goal and hope they will be used worldwide."

Contact: R. Lougheed (510) 422-6685 (lougheed1@llnl.gov).

Protecting the Global Connection

GLOBAL connectivity is a given. Every country in the world has some electronic capability that links it to vast worldwide communications networks. Information, in quantities unimaginable and in places unheard of, is instantaneously accessible merely by touching a few keys on a computer keyboard. The entire contents of the Library of Congress are a mere speck in the ocean of information available at our fingertips.

Our daily lives are inextricably tied to computers and communications networks. Financial institutions transfer trillions of dollars daily; much of the world's commerce is conducted electronically, including the trading of millions of shares of stock daily by stock markets in every major financial capital; transportation systems use global positioning satellites for guidance; electric power generation and distribution are computer-controlled; medical services, including intricate surgical procedures, are computerized; and industry uses automated assembly lines. The list goes on and on. With much help from networked computers and communications systems, we are fast becoming one global community, with all the attendant implications of alliances, cooperation, courtesy, dependence, restraint, and—perhaps most important—trust.

Imagine the chaos that could result from an extended disruption of networked services or in any one of those services—in fact, in any small subset of one of those services. We have had a few noteworthy examples—wake-up calls if you like—of the results of a short-term disruption: the East Coast power blackout a few years ago, the telephone outage in the Chicago region, the more recent shutdown of the power grid in the Northwest.

As early as 1979, the Department of Energy and Lawrence Livermore recognized the importance of protecting our unclassified computing environments from improper use, access, or disruption. While the focus in those early days was on protecting local computing installations, it was a relatively easy transition from that effort into a more universal, wide-ranging program that addresses the security implications of localized computing in the larger context of global connectivity. A number of computer security events in the late 1980s—notably the East German hacker incident discovered at Lawrence Berkeley National Laboratory and chronicled in Clifford Stoll's *The Cuckoo's Egg* and the Internet "worm" incident—helped focus the need for protection products and furthered the cause of computer security research efforts throughout the world.

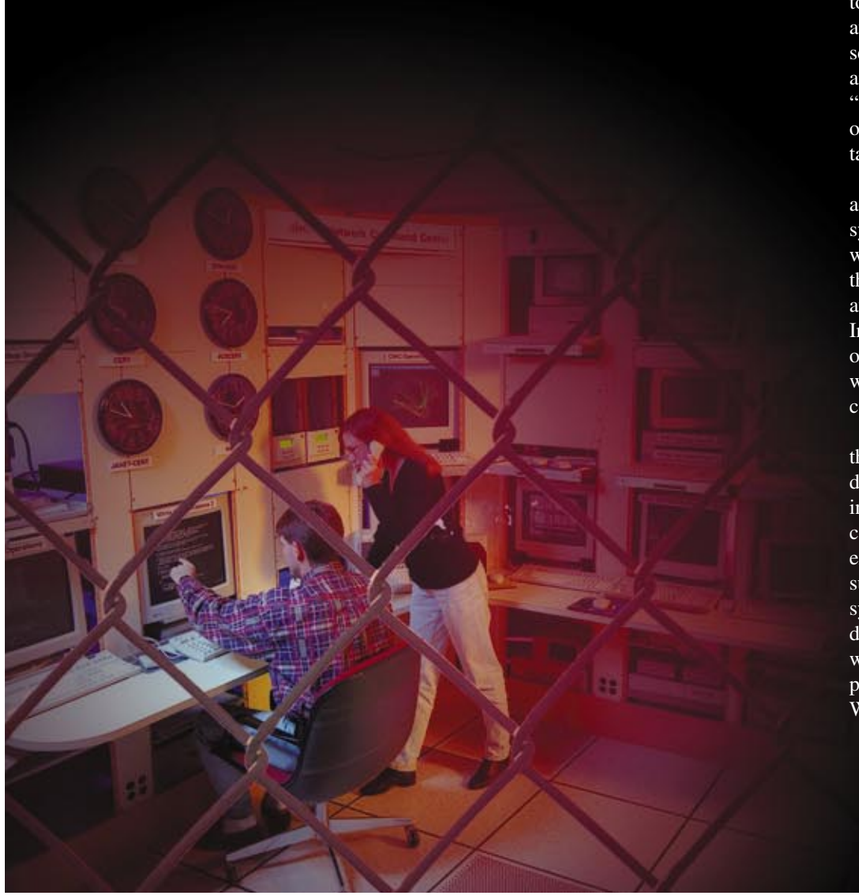
The Computer Security Technology Center at Lawrence Livermore was established to identify and develop computer and network protection methodologies and products that could help ensure the integrity and security of DOE computing resources. Products of the center have evolved over the years to keep pace with rapidly changing computing technologies. The following article describes a collection of products and services that DOE and its contractor community are using to help protect the vital computer systems and interconnecting networks that provide the computational underpinnings for Department of Energy programs.

The nation's growing dependence on computers and the networks that interconnect them places us at great risk. Threats range from simple annoyances, such as unsolicited advertising via e-mail, to much more sinister possibilities, such as intentional disruption by an adversary. The research efforts of the Computer Security Technology Center are vital to the future well-being of the global computer community of which we are a part.

■ David Cooper is Associate Director, Computation.

Making Information Safe

Our dependence on technology has made the Computer Security Technology Center's developments—electronic counterparts to guards, guns, and gates—crucial for protecting our nation's information assets.



VERY late one night in November of 1988, a warning appeared over the Internet: a virus was running loose in cyberspace. As it turned out, the warning was apropos but incorrect—it wasn't a virus but something worse. A computer virus needs the help of a user to activate and spread it; whatever was attacking systems on the Internet was seemingly able to search for and infect any location without assistance. It "wormed" its way through networks, overloading machines with invisible tasks and preventing their effective use.

As word spread, system administrators frantically shut off their systems from the Internet, hoping they weren't too late in defending themselves. They rested easier only after the worm was removed from the Internet. The worm's perpetrator was one Robert Morris, a graduate student, who eventually was convicted of computer fraud and abuse.

The Morris Worm will go down in the annals of Internet history as an early demonstration of how vulnerable and interdependent network-based systems can be. Even though it specifically exploited the weaknesses of a particular subset of UNIX systems, all Internet systems suffered days of service disruption and weeks of uncertainty while costly cleanup activities took place. The likelihood of more Morris Worm–like attacks led the Department of Energy to take two important steps to safeguard information on its computer systems: it created an incident response team to contain computer intrusions and prevent their recurrence, and it increased sponsorship of projects that advance the cause of computer security.

24-Hour-a-Day Security

As a direct result of the Morris Worm attack, DOE in 1989 formed the Computer Incident Advisory Capability (CIAC), an organization based at Lawrence Livermore that provides on-call incident response and transmits security incident information throughout DOE sites. Today, it is the oldest response team in existence funded by a federal civilian agency and is a recognized institution both nationally and internationally.

When CIAC receives notice of an incident, it assesses its extent, and determines if catching the intruder is possible. If the site where the incident occurred chooses to try to capture the intruder, CIAC monitors the break-in and coordinates with other sites and law enforcement to trace the intrusion back to its origin. After the intruder is caught or if the investigation determines that the intrusion cannot be traced, CIAC provides appropriate technical resources to contain the incident and fix the system's vulnerabilities. It collects and verifies information related to the incident and disseminates information about new vulnerabilities and patches (fixes for vulnerabilities) to the DOE community. CIAC's services are funded by the DOE and are available 24 hours a day, 7 days a week.

CIAC's incident handling capability is the central, reactive component of a larger security service that also provides awareness training and education. It does so through comprehensive, customized workshops tailored to a user group's specific information-security needs. Workshop subjects include threats and countermeasures, firewalls, connecting to the Internet securely, legal issues, and even briefs on how to use CIAC effectively.

As part of its work, CIAC keeps close ties with other response teams, commercial vendors, law enforcement agencies, and other government agencies to track the latest technology trends and the latest known information about network security threats and vulnerabilities. It publishes a well-recognized security Web site on the Internet (http://ciac.llnl.gov/).

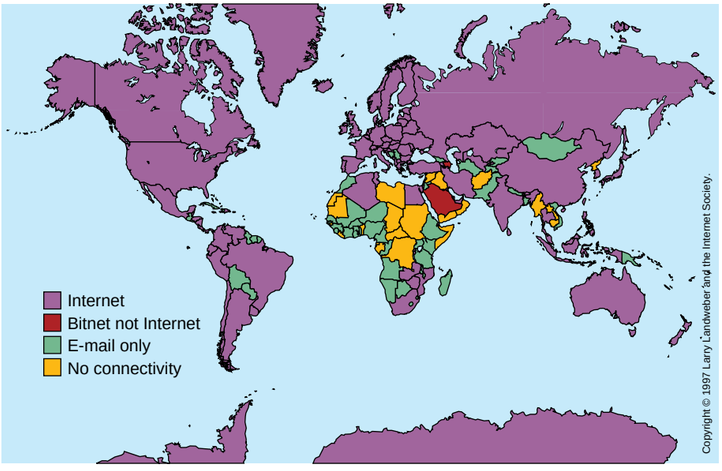
To extend CIAC services to all other federal civilian agencies, the U.S government funded a new joint effort with a sister team called the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University in Pennsylvania. This new virtual team is called FedCIRC (Federal Computer Incident Response Capabilities).

Integrated Protection

The Morris Worm incident occurred at a time when awareness of computer security issues was beginning to grow. In 1986, Congress enacted a Computer Fraud and Abuse Law, following it in 1987 with the Computer Security Act that established a national framework for addressing computer security issues and required federal agencies to plan and train for security incidents. Since then, awareness of computer security has increased because worldwide connectivity is increasing at exponential rates (Figure 1), and computer security compromises are increasing in parallel with it. In 1995, for instance, an estimated quarter of a million computer intrusions occurred on Department of Defense computers alone. Trends indicate that the number of intrusions doubles each year, so that by the end of 1997, it is estimated that DoD computers were attacked one million times.

Computer intrusions into DOE and other computers can range from annoyances such as chain letters (make your lucky day luckier by sending this message to a dozen friends) and hoaxes (don't open this file or read this e-mail message because it will destroy your system) to malicious attacks that deprive computer users of service, destroy files

(a) International Connectivity, June 15, 1995



(b) International Connectivity, June 15, 1997

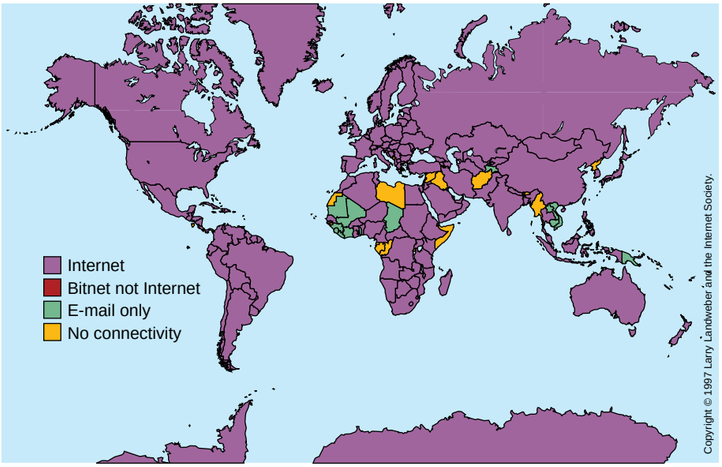


Figure 1. Comparison of (a) and (b) reveals an exponential increase in worldwide computer connectivity in just two years. Computer security issues have increased at a similar rate.

and hard drives, or steal sensitive or proprietary information.

What has particularly worried computer security specialists is the growing number of hackers, the growing technical sophistication of their attack tools, and the leveraging of their expertise. Hackers have begun sharing automated hacking tools with each other, enabling many more hackers, including less-experienced ones, to attack computer systems with impunity, exploit arcane system flaws while fully covering their own tracks. And they can do all this without necessarily understanding how the tools work (Figure 2).

In this context, the second response DOE had to the Morris Worm attack was to sponsor the establishment of the Computer Security Technology Center, or CSTC, at Lawrence Livermore. Kernels of CSTC had existed at the Laboratory since the 1970s, when prescient computer specialists such as Chuck Cole and, later, Doug Mansur (now the program manager of CSTC) began working on computer security research and development projects. Cole, who recently retired as Deputy Associate Director of Operations in Livermore's Computation Directorate, was such a strong champion of computer security that he was as much a factor as the Morris Worm attack in convincing DOE to create a formal entity dedicated to information security. Once formed, the CSTC combined the incident response work of CIAC with two other important components: advanced security research and development projects, and outreach consulting services. This integration of capabilities has proven to be powerful, and the CSTC has become an increasingly influential focal point for information protection throughout the federal community.

Security through Penetration

Among the consulting and professional services that CSTC staff provide is one they dub the White Hat review, a friendly attack of a client's information systems. These systems are likely to be complex, with global computing functions, telecommunications, open architectures, and diverse platforms and protocols that span geographic boundaries and time zones. Their interdependencies put all components at risk if any one fails, thereby jeopardizing the security of the total system. At the same time, system complexity exceeds the protection capabilities of most safeguard mechanisms.

As a way to actively manage the risks of complex systems and improve information protection, a client can request that a White Hat team perform system and network penetration tests and acquire a snapshot of security strengths and weaknesses. Members of the White Hat team are Top Secret–cleared, information security specialists, armed with current intruder techniques and tools, who attempt to penetrate an information network and learn the state of protection measures in the system. They really are just the other side of the coin of CIAC response personnel—generalists who use their computer skills to root out security problems.

White Hat activities generally comprise three phases and use methods previously negotiated with client management: scan and map a network to determine its topology and identify its vulnerabilities, intrude and compromise systems by exploiting the discovered weaknesses, and analyze results to recommend protection improvements. Unlike organizations whose systems suffer hostile attacks, the clients requesting a White Hat team always maintain complete and continual control of their systems and the intrusion process.

Advanced Security Tools

The specialized research and development work performed by CSTC staff has led to the development of security tools now in use in DOE and other federal environments. A number of the tools have been used to catch intruders, and one of them made national news while doing so.

Detection Sets Court Precedent

In early 1996, federal investigators charged an Argentinean student with illegally accessing U.S. military computers. The student apparently had broken into his university's Internet-linked computers to steal passwords and then used the network to penetrate computer systems at the National Aeronautics and Space Administration, the U.S. Navy, the U.S. Army, and systems in Taiwan, Mexico, the United Kingdom, and South America. He had managed to get access to a variety of sensitive government information before the U.S. Navy traced the culprit and nabbed him. To apprehend this hacker, the Navy used the Network Intrusion Detector (NID) software developed by Lawrence Livermore computer scientists and based on earlier work with the University of California at Davis.

NID is a suite of tools that detects and analyzes unauthorized computer access. Working within a network of host computers called a security domain, NID runs undetected by the intruder as it collects information packets (data packaged for transmission) and statistics across the domain. First, it uses a tool called

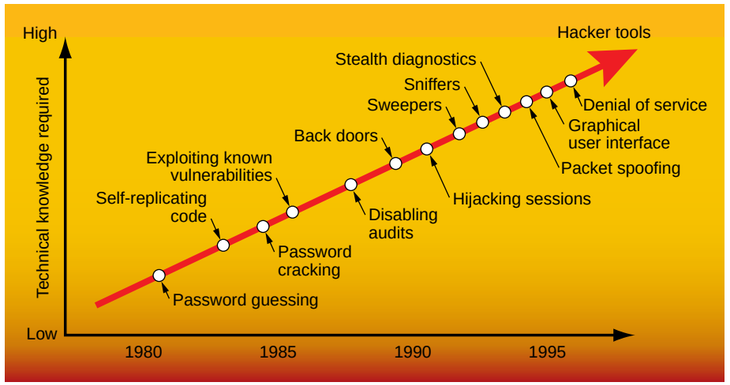


Figure 2. As technical knowledge increases, so do the number and sophistication of hackers' tools. Alarmingly, hackers without detailed technical understanding of those tools are still able to use them.

iDetect to look for evidence of an intrusion by examining information packets for intrusion signatures (that is, a string of characters known to be used for attacks). Collected evidence is presented to an authorizer that approves the transition to iWatch, NID's second evidence-gathering phase. iWatch scans a network for connections that contain the same signatures found by iDetect. If iWatch provides compelling evidence, then a third subset, iScript, is used to convert the packets of data into a transcript suitable for use in court.

Before NID software could be used against the Argentinean student, the FBI had to convince a judge that NID would not violate privacy standards such as those imposed on wiretaps. Accordingly, NID was modified to address the issue of civilan computer privacy. The modifications took into account the conflicting values of information protection versus privacy and made use of an evidence-gathering model that searches for specific patterns. If the data search detects an apparent specific pattern, permission could be obtained to continue with specific data collection.

On March 29, 1996, Attorney General Janet Reno announced on national television that an arrest warrant had been issued for the student. "We are using a traditional court order and new technology to defeat a criminal, while protecting individual rights and constitutional principles that are important to all Americans," Reno said. The case set a precedent for evidence gathering on the Internet.

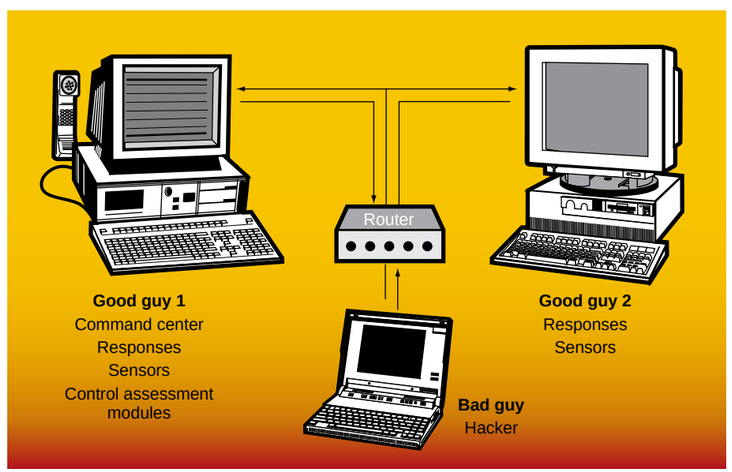
Detection in Near-Real Time

Had Automated Information System (AIS) Alarms been available when the Argentinean hacker was breaking into the network, he might not have gotten as far as he did. An intrusion detection program that is in development, AIS Alarms works much like a building security system connected to a police or security station. It uses sensors distributed throughout a network to detect specific suspicious events. Sensor information is fed to a central assessment module (CAM), which is outfitted with a set of rules for interpreting the information and determining the state of system security. The assessment triggers a number of possible system responses, such as turning on more sensors to get more security data; notifying a system administrator of abnormal or improper activity on the network; or reconfiguring a firewall, router, or other network protection device to isolate particular users, addresses, or network services (Figure 3).

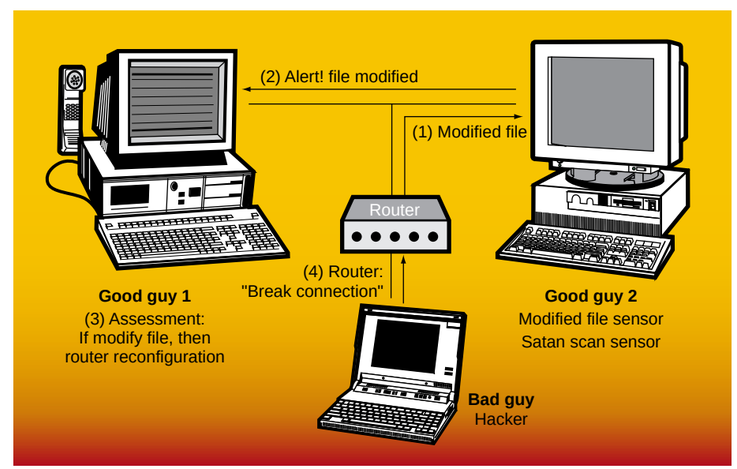
AIS Alarms recognizes a security incident in near-real time and with great flexibility. Its three parts—the sensors, central assessment engine, and response agents—are all planned as "plug-and-play" elements that can be configured and reconfigured easily (even "on the fly") in the computer architecture. This feature allows users to tailor the system for different networks, local policies, and threat environments. Sensors can be ramped up when a threat has been detected (the response agents can turn more sensors on) or are disabled to conserve computing resources. The rules used by the CAM can be changed to redefine what constitutes a computer attack, thus giving system administrators great leeway in specifying what should be detected and how responses should be formulated. The CAM may be made to merge information from any number of sensors, and it may be linked into hierarchical systems to protect local, regional, and national computer networks. Whatever the configuration, the AIS Alarms remains automatic: it can run unattended and will, on its own, take evasive action against attacks.

The AIS Alarms project is a collaboration of the Lawrence Livermore, Los Alamos, and Sandia laboratories. The tri-lab team has designed the software as a continually evolving system. Because there is a constant leapfrogging of security solutions and new attack methods, the team's approach has been to develop a prototype system quickly and then fine-tune it through real application and experience. The result is ever-improved security, better understanding of risks, and minimized computing resource overhead.

(a) The AIS Alarms setup allows hacker recognition.



(b) Recognition and assessment by AIS Alarms trigger flexible responses.



A Network SPI

DOE commissioned the Security Profile Inspector (SPI) analysis program specifically to counter attacks like the Morris Worm and was joined by DoD's Defense Information Systems Agency in sponsoring its development. Developed at Livermore, the program is now being used throughout DOE and DoD; the transfer of its technology to the private sector is being pursued.

SPI simultaneously assesses the security of all machines in a designated security domain. Users and system administrators can run SPI on demand or on a set schedule. Either way, they are actively defending their systems from hackers and even from insiders trying to escalate an attack to more sensitive parts of the system.

SPI has six modules that are used to collect and report system security information. They are installed on every host computer in the security domain. The modules query the status of a system's files, users, and groups; look for common security problems and known vulnerabilities (the list of which is constantly updated); uncover poorly chosen passwords; create a database snapshot of important user, group, and file information that can be used to detect unauthorized changes or additions; test the access controls; and ensure that the system contains only up-to-date, authentic software (that is, no Trojan horses) with the latest patches for detected flaws.

The computers installed with these modules communicate, via secure channels, with a command host computer that aggregates, processes, and integrates all acquired information and generates reports assessing the state of the system. The command host becomes, in effect, the "system administrator" of the security domain.

A centralized system administration is crucial for safeguarding networks. Yet, when computing resources are distributed to myriad users, tasks, and workstations, this function is usually left to end users with little or no system administration experience. SPI addresses this problem by providing for uniform, expert security management across many machines from a central workstation.

Ways to Practice Deterrence

Computer security starts with a system in which a user can place complete faith: it is "clean," is properly configured, and has had all upgrades and recommended security patches installed. These are prerequisite to effective access control, account monitoring, and appropriate network services. But

(c) Notification of intrusion and response is almost instantaneous.

Figure 3. Currently under development by the Computer Security Technology Center, Automated Information System (AIS) Alarms allows (a and b) recognition of and (b and c) response to security incidents almost as they are happening.

keeping an electronic house in order is not as easy as it sounds, because operating system software changes constantly and system administrators must deal with many systems and heterogeneous environments. As upgrades arrive for both the core software and security patches, the versions to which they apply are difficult, if not impossible, to track. Worse, their intended applications (the system, type, version, or architecture to which the upgrade applies) are not readily apparent. Sometimes, upgrades and patches do not do what they are intended to do or arrive with incomplete or erroneous installation packages. Sometimes, they even arrive security-flawed straight out of the box. Part of the Morris Worm attack was, in fact, based on exploiting one such flaw to gain illicit access to systems.

System administrators will have some housekeeping help from Lawrence Livermore's Secure Software Distribution System (SSDS), which is currently in development. This practical, automated tool can be used to query, maintain, and upgrade the software integrity of hundreds of individual systems from a central point, through largely automated means. When completed, the SSDS tool will quickly, automatically, and regularly assess and authenticate system software, collect vendor upgrades and patches, determine the applicability of upgrades and patches to specific systems, install them and related critical system software, remove patches if for some reason a system must be restored to its previous state, detect instances of subsequent tampering, and collect sitewide software statistics or metrics.

David Crawford (left), a member of the Computer Security Technology Center's incident response team, works with tools developer Stephen Wong to refine the products and services that protect Laboratory computer systems from unauthorized penetration.

SSDS works through two components: an SSDS server that resides in one computer and an SSDS agent in each computer being monitored. The server performs the key functions of tracking vendor upgrades and patches, converting any new ones into standard formats and storing them in a database, and comparing database information against local system files to determine what has been installed and what still needs to be installed.

Patching tools similar to SSDS attempt to keep track of the patches that they have installed by building a "patch history" file. However, because these tools do not have the capability to survey the local file system, they can be easily fooled into reporting erroneous information. In contrast, the SSDS server queries the agents about the file owner, access control list, and cryptographic "hash" and compares this information with its database to ascertain what patches are actually installed on the local file system. SSDS bypasses reliance on the local patch history file, which may be incorrect or compromised.

The SSDS can be configured to support a variety of environments, whether small homogeneous networks or large heterogeneous ones. A simple configuration was described above: one server serving agents installed on all target systems. When, as at Lawrence Livermore, hundreds or thousands of systems running a variety of operating systems and architectures are in use, multiple servers will be used to collect patches and upgrades. The functions of evaluating and installing them are delegated to another subset of the system, with the number of systems performing these functions determined by the size of the security domain. The SSDS has great flexibility for supporting a variety of systems by distributing different workloads without duplicating effort.

Identifying Classified Information

Many government agencies and other organizations need to be sure that the electronic documents on their open computers are free of classified or other sensitive information. Also, since World War II, DOE, its predecessor agencies, and their contractors have generated billions of pages of classified materials. Various recent laws and court decisions now require DOE to swiftly declassify and release many of these documents. Declassification is not an easy task, because two authorized classifiers, at least one of whom must have additional training and authorization as a declassifier, must determine that a document no longer needs the protection of classification.

CSTC, through the Text Analysis Project (TAP) funded by the DOE Declassification Productivity Initiative, has been developing software tools to assist in identifying classified information for proper electronic or hard-copy storage, deletion, or declassification.

TAP works by reviewing documents against a rule set based on classification or other guidance. A TAP rule is a collection of words and phrases along with conditions based on proximity such as "within the same sentence" or "within eight words" and, in some cases, quantitative constraints on individual items such as "later than 1980" or "mass greater than 5 kilograms." Synonym lists induce multiple variants of most rules. The rule set leads to a table of rule words and to other tables specifying constraints and relating words to phrases and phrases to rules.

To process a document, TAP "reads" through it looking for rule words and tracking their locations. When TAP finds all the words for a particular rule and has determined that they meet that rule's conditions and constraints, it declares a match, or hit, assigns it a hit number, and specifies the applicable rule number and the precise location of the hit in the document being analyzed. The user can now display the document with the hits highlighted. Jumping from one hit to the next, an authorized classifier or declassifier will see additional information for each hit—the classification guide and topic on which the rule was based and the associated classification level.

TAP can batch-process large numbers of documents and provide a summary report to be used by a classifier to prioritize documents for review or by an administrator to assign documents to appropriate reviewers.

Classifiers and declassifiers are currently using TAP to support systematic reviews in which documents are separated into two categories (classified and unclassified), but no sanitization is done to turn classified into unclassified documents. Later, as DOE produces and refines rule sets targeted at various types of information, TAP may be able to support sanitization efforts and to replace one of the two reviewers required for declassification.

Solution Is a Moving Target

Tools to fend off attackers and safeguard our information have not, as we know, completely protected us from computer intrusions. They might never do so, because attack methods change and software flaws continually appear—they are moving targets. Nevertheless, the work of the Computer Security Technology Center is vital in protecting the Laboratory's and DOE's information assets; its staff will continually search for more and more advanced solutions. Doug Mansur says, "There's hope for containing these problems. For even the most perplexing security problems today, we can offer at least partial solutions."

—Gloria Wilt

Key Words: AIS (Automated Information System) Alarms, Computer Incident Advisory Capability (CIAC), Computer Security Technology Center (CSTC), computer intrusions, document classification, hacker, incident response, Internet, Morris Worm, Network Intrusion Detector (NID), Secure Software Distribution System (SSDS), Security Profile Inspector (SPI), software patches and upgrades, Text Analysis Project (TAP), virus, White Hat review.

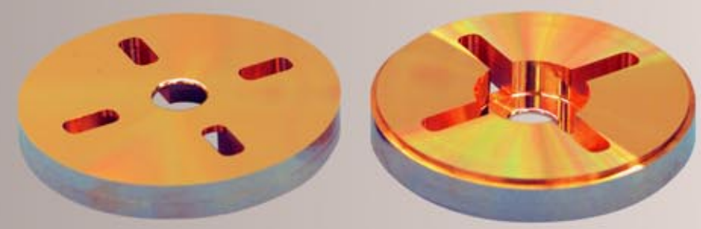
For further information contact Douglass Mansur (510) 422-0896 (mansur1@llnl.gov).

About the Center

Lawrence Livermore's COMPUTER SECURITY TECHNOLOGY CENTER (CSTC) is composed of 32 computer scientists led by Douglass Mansur, center manager (pictured at left). He is assisted by Harry Bruestle, deputy center manager; Sandra Sparks, head of the incident response team; and John Rhodes and Lauri Dobbs, co-leaders of tools-development projects. CSTC got its start in 1989 with the Computer Incident Advisory Capability (CIAC), an organization begun by DOE at Livermore to identify and respond to breaches in computer security throughout the DOE complex. This 24-hour-a-day incident-response capability is made possible by a variety of new and evolving tools developed by CSTC personnel to monitor and protect computer systems and networks, to respond to and deter penetration of those research and development resources, and to identify and secure the unclassified and classified information stored in and handled by Laboratory, DOE, and civilian government computers.

Engineering Precision into Laboratory Projects

From nuclear weapons in the Laboratory's early days to the advanced optical systems of the upcoming National Ignition Facility, Livermore projects regularly "push the envelope" for precision.



ALMOST since the inception of the Laboratory, Livermore engineers have been working to make manufacturing processes more precise. With the goal of building a more effective nuclear weapon, they developed new instruments that brought greater accuracy to measurements of dimensions, shapes, densities, and surface finishes than was possible with existing instrumentation. They also worked to develop manufacturing processes for machining and finishing that were more precise than anything commercially available.[1] The science of measurement (known as metrology) and precision engineering go hand in hand, because without the ability to measure a dimension or other quantity, one can never know whether a given level of precision has been achieved.

As measuring capabilities improved, components for nuclear weapons were designed to tighter tolerances, leading to an increased emphasis on precision manufacturing. In fact, Livermore's creative weapon designs produced a precision engineering capability that was unique in the U.S. weapons complex and that endures to this day. Precision engineering at Livermore in those early days laid the foundation for the effectiveness of today's nuclear arsenal.

As the Laboratory's mission broadened in scope, projects in lasers and astronomy, among others, also put demands on Laboratory engineers to design optics and other parts to tolerances that could not be met by commercial manufacturers. With no commercial suppliers available, ultraprecise manufacturing systems had to be developed, many of which were later transferred to the private sector. Today, the Laboratory would have no difficulty commercially obtaining many of the instruments and manufacturing systems it developed as prototypes 10 years ago. But the demand for precision at the Laboratory continues to increase, keeping Livermore's precision engineers busy.

Livermore scientists do not shy away from projects that require precision. The National Ignition Facility (NIF), which is now under construction, is perhaps the premier example. Upon completion, NIF will be the world's largest laser and most sophisticated optical instrument, with over 7,500 high-precision optical components larger than 40 centimeters in diameter, including amplifier slabs, lenses, mirrors, polarizers, crystals, windows, and shields. It will also incorporate more than 40,000 smaller optical components. Lawrence Livermore is one of the few organizations in the world with the capabilities necessary to execute a project requiring the level of precision demanded by NIF. As Laboratory Director Bruce Tarter said in a speech at a recent symposium on precision manufacturing, "Precision engineering is on LLNL's short list of core competencies." It has been for 40 years and probably always will be. And today, it is one of the capabilities helping to make the National Ignition Facility a reality.

Pioneers in Precision

Livermore was a pioneer when it started its work in precision engineering in the 1950s. Private industry did not then have the economic incentive to carry out the necessary developmental work. Today, many commercial firms are concerned with conforming to tight tolerances and specify that their manufacturing machinery be designed accordingly. But they seldom have the analytical skills needed to both improve the precision of their manufacturing processes and embody that improvement in the design of their machinery.

As one of just a few organizations in the world that combines expertise in both process development and machine design, Lawrence Livermore brings something unique to the precision engineering table. Livermore has an in-depth understanding of physical phenomena, equipment, and processes and employs this understanding in both developmental work and practical applications.

Livermore's precision engineers tend to be generalists who attack a whole problem rather than specialists who work only on one aspect of it. At Livermore, precision engineers take a systems view of how to gain higher precision—or high precision for less cost—than is currently possible. Many disciplines work together to meet the demands of Laboratory programs.

As experts in dimensional metrology, machine design, and material removal processes,

Livermore's precision engineers have developed an impressive array of state-of-the-art tools, some of which are described in the box on pp. 16–17.

Greater Precision for Less

Much of today's precision engineering work reflects a change in philosophy that first appeared some 15 years ago. Absolute accuracy used to be the objective. But as cost has become a greater factor in most projects, the goal has changed to one of constantly improving the precision-to-cost ratio.

Meeting NIF Challenges

This new goal is perhaps nowhere more important than at the National Ignition Facility where the cost of all components must be about one-third of today's typical cost, with precision and tolerances equal to or exceeding present capabilities.

One of the critical precision engineering tasks for NIF is the development of new manufacturing processes that will be used by commercial vendors to machine KDP (potassium dihydrogen phosphate) crystals for NIF's laser system. KDP crystals are also used in the Nova laser and are produced by a commercial supplier, but NIF's tighter tolerances call for the KDP to have a surface quality higher than that currently available commercially (Figure 1).

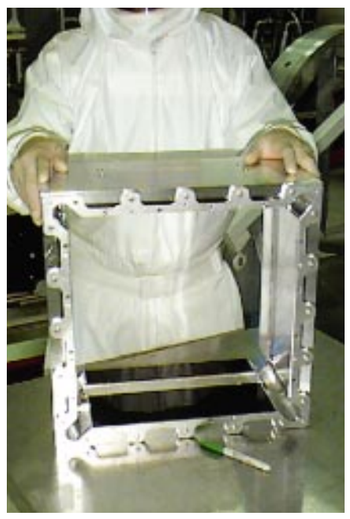


Figure 1. Large KDP (potassium dihydrogen phosphate) crystals, such as the one shown here in its final optical mount, will be used in the National Ignition Facility. Precision engineers at Livermore have developed the methods for machining these crystals to NIF tolerances. They are also developing an instrument to ensure that the crystals are manufactured to specification and are aligned so they will function properly within the NIF laser.

Several years ago, Livermore scientists won an R&D 100 Award for a method to accelerate the growth of KDP crystals.[2] Livermore precision engineers are developing methods for machining these new crystals to NIF tolerances. They have modified a Laboratory machine for initial rough cutting of the crystals and have shipped it to the vendor who will produce the crystals. They have also developed a process for crystal finishing and have written the specifications for the finishing machine. During 1998, the vendor will assemble the finishing machine at the Livermore site. The best news is that the best way to manufacture the crystals to specified tolerances meets NIF's cost requirements.

Livermore is also developing the instrument that will be used to align the crystals. Known as Crystal Alignment and Verification Equipment (CAVE), this tool ensures not only that the crystals are manufactured to specification but also that they are properly aligned and function in accordance with the specification.

Improved Accelerator Cells

Cost is also a major issue for a new linear electron–positron collider for basic physics research that is currently in the developmental stage. Lawrence Livermore has teamed with the Stanford Linear Accelerator Center and Lawrence Berkeley National Laboratory on its design, which calls for 1.9 million accelerator cells designed to submicrometer tolerances.

In the current baseline design, groups of 204 cells are bonded into 1.8-meter-long structures. To improve accelerator performance, these cells are designed to vary gradually over the length of each structure. Ninety-two hundred of these structures are to be installed and aligned over the 21 kilometers of the beamline.

Manufacturers of high-end optics could supply these parts, but the cost would be unacceptably high. In an effort to reduce the current estimated cost, Livermore precision engineers are exploring less expensive alternatives for manufacturing these components (Figure 2), including developing prototypical manufacturing processes. Many trade-offs are being considered to minimize cost while achieving the required accelerator performance in a reasonable fabrication time. The project manufacturing plan will be part of the conceptual design report that will demonstrate why this new collider should be built.

System Development

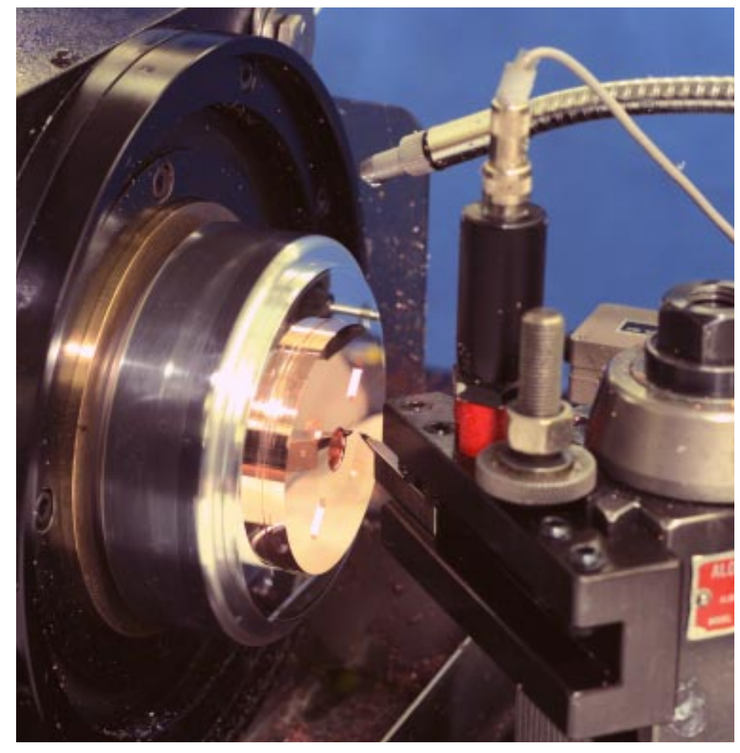
Precision engineering requires, among other things, a systematic approach to determining dimensional errors. When measurements are made, precision engineering requires a quantitative assessment of the total uncertainty of the measurement. During the manufacture of a component, it requires an "error budget"—a comprehensive estimate of what errors may affect the tolerances of the component. Meeting these requirements means that the Laboratory's precision engineers must become good at system integration. Two examples where precision engineering has been integrated into Laboratory projects are advances in extreme ultraviolet (EUV) lithography for printing computer chips and the development of a workstation for the femtosecond laser cutter.

Measuring Optical Surface Errors

Earlier Laboratory work on multilayer reflective coatings for inertial confinement fusion produced part of the technology that has enabled development of EUV lithography for printing computer chips. With this technology, computer chips will be 100 times faster and able to store 1,000 times more information than those made using current lithographic methods. To meet these performance demands, the next generation of computer chips must have circuit line widths that are 0.1 micrometer or less. The manufacturing process for these chips will obviously demand extremely tight tolerances.

EUV lithography uses laser light with a very short wavelength—shorter than ultraviolet but longer than x ray—to project the circuit pattern by reflection onto each chip. The system that can do this requires mirrors, cameras, and other devices with some of the most accurate optics ever made. Thus, developing EUV lithography is essentially an exercise in precision

Figure 2. A prototype accelerator cell being machined to submicrometer tolerances by a small diamond-turning machine at Livermore for the proposed new electron–positron collider at the Stanford Linear Accelerator Center in Menlo Park, California. The collider will require almost 1.9 million of these cells, and Lawrence Livermore is developing a manufacturing plan for minimizing fabrication costs.



Metrology and Machining at Livermore

Advances in Metrology

Livermore has invented a number of new metrological devices in response to programs that have needed parts fabricated or measurements made beyond the limits of existing instruments. Several of them have won R&D 100 (earlier known as IR 100) awards, and many have been commercialized. These include the laser heterodyne profiler, developed in the 1970s, and an amplifier to increase the resolution of a linear variable differential transformer (LVDT), which was developed in 1990 with Lion Precision of St. Paul, Minnesota.* Both of these tools are used to measure errors in the surface of optical elements such as mirrors and lenses.

A recent invention takes the measurement of optical errors to the atomic level for the first time. The absolute interferometer, shown in Figure 3 on p. 18, produces measurements of optical surfaces to within just one or two atoms, or less than 1 nanometer.**

In the early 1980s, Livermore scientists combined an LVDT with a hydrostatic spindle and a computer. Called the Compuron, this tool can measure the roundness of parts with an accuracy of 2.5 nanometers and is still in use today at Livermore.

Diamond-turning machine 3 (DTM3) is large enough to machine a cylinder 2.1 meters (84 inches) in diameter by 1.1 meters (44 inches) long. DTM3 is kept at a constant temperature by a shower of light machine oil that flows at 400 gallons per minute. The horizontal *x* axis carries the spindle, which holds the part, and the *z* axis carries the tool perpendicular to the part. DTM3 has been used to produce many types of optical surfaces.

Metrology tools find many uses. The most obvious is to measure shape errors in the part being produced. But they also can measure the errors arising in the equipment used to manufacture the part, a practice known as machine tool metrology. And they are often used to measure a process—for example, to characterize a grinding wheel.

Livermore has also continually supported the development of standards that are important to precision engineering. Most of this work has been with the American Society of Mechanical Engineers and American National Standards Institute in such areas as surface texture, dimensional measurement, measurement procedures for acceptance testing of machine tools, and symbology and tolerances for drawings. Livermore scientists are also active in working with the International Standards Organization to establish international metrological standards.

An example of the importance of standards arises in what seems at first to be a simple operation—measuring the dimensions of an object. Because temperature affects an object's shape, lengths are, by international agreement, specified at 20°C. But few such measurements are performed at exactly that temperature, so engineers use an equation that considers the coefficient of thermal expansion of the part's material to describe the change in length. Even then, errors may occur if the length measurement at ambient temperature is not made carefully or if the temperature difference from 20°C is determined incorrectly. If a seller and a buyer of a component perform the calculation differently, they will compute different lengths for the part. Thus, the procedures for assessing length must be carefully prescribed so that all parties get the same result.

Designing High-Precision Machines

At the same time that Livermore scientists were improving the science of metrology, they were also making major advances in developing high-precision machining tools.

A key ingredient in the design of any precision machine is the error budget, which delineates how much uncertainty or nonrepeatability can be tolerated at each step in the production process. Predictability and repeatability must be maximized in these machines if they are to consistently produce parts with tolerances of fractions of a micrometer.

Most of the machine tools that Livermore has developed are for turning, primarily diamond turning, but advances have also been made in grinding. Turning is a point-defined process that draws a single tool across a surface in a highly controlled manner. Grinding is an area-averaging process that moves tiny abrasive particles across a surface in a less predictable manner. Turning excels in producing precise size and contour, whereas grinding can produce a smooth surface finish on selected materials.

Since the 1960s, Livermore has continually experimented with and refined the science of diamond turning, which uses a specially designed precision lathe and a single-crystal diamond tool to machine metals to a mirror-like finish and extremely close dimensional tolerances. Livermore designed and produced several large diamond-turning machines, each with greater contour accuracy than its predecessor. Most designs incorporate fluid bearings of either air or oil to reduce friction and increase stiffness, strict temperature control, and as much vibration isolation as possible. (See figure on p. 16.)

One of the finest achievements of precision engineering at Livermore is the Large Optics Diamond Turning Machine (LODTM, pronounced "loddem"), the world's most accurate machine tool. (See figure at right.) Built in the early 1980s to machine prototype large-diameter mirrors made of copper, electroless nickel, and other metals for the Department of Defense, LODTM can machine workpieces as large as 1.5 meters (5 feet) in diameter and 46 centimeters (18 inches) in height to an accuracy of greater than 30 nanometers rms (root mean square). LODTM has also been used to produce secondary mirrors for the Keck Observatory in Hawaii and continues to be used to develop prototype optics.

Diamond turning is ideal for machining certain nonferrous metals such as copper, gold, aluminum, and nickel. Livermore has extended its use to machining of such brittle materials as the nonlinear crystal KDP (potassium dihydrogen phosphate), which is used in the Nova laser and the upcoming National Ignition Facility. The Laboratory is also evaluating diamond turning for the finishing of silicon as a mirror substrate for high-energy lasers.

But some materials, including steel, titanium, and beryllium, react chemically with the diamond point, causing it to wear excessively. Livermore has experimented with single-crystal cubic boron nitride (cBN), which is stable and strong to high temperatures, as an alternative to a diamond tool, but early trials have shown that single-crystal cBN is too delicate for use in machining. Instead, we are developing turning tools that are diamond with coatings of cBN and other hard materials, which allow the tool to maintain its sharp edge.

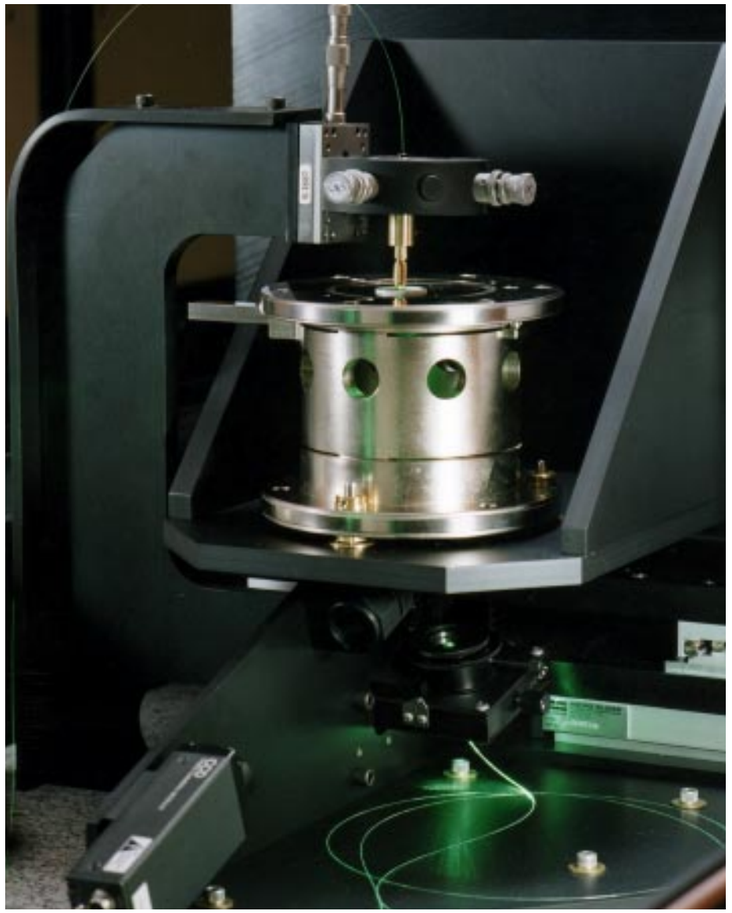
Ductile grinding emerged in the 1980s as a possible analog to diamond turning for finishing ceramics, glass, and other brittle materials. It differs from other types of grinding in that the surface being ground is smeared rather than cracked. The process uses an extremely fine grit (less than 20 nanometers) and requires careful control of the force of the grit to minimize its penetration into the surface. An acoustic-emission sensing system developed at Livermore assists with controlling the process by detecting the proximity of the grinding wheel to the workpiece and supplying in-process measurements for monitoring grinding quality. Still under development at Livermore and elsewhere, ductile grinding produces a finer, higher quality finish than ordinary grinding. In glass, for example, grinding typically produces a frosty surface, but ductile grinding produces a shiny surface.

*"High-Precision Low-Noise LVDT Amplifier," *Energy & Technology Review*, Lawrence Livermore National Laboratory, Livermore, California, UCRL-52000-94-11 (November 1994), pp. 6–7.

**"New Interferometer Measures to Atomic Dimensions," *Science & Technology Review*, Lawrence Livermore National Laboratory, Livermore, California, UCRL-52000-97-10 (October 1997), pp. 6–7.

The Large Optics Diamond Turning Machine (LODTM) machining a workpiece. Many of the LODTM's parts are made of a special steel alloy (Super Invar), which has an exceptionally low coefficient of thermal expansion. Air cooling for the area around the machine keeps temperature changes to within about 10 millidegrees Celsius, and a water cooling system for the metrology system keeps changes to less than 1 millidegree over a day.

Figure 3. Developed at Livermore and winner of a 1997 R&D 100 Award, the absolute interferometer can measure errors in the surfaces of optical parts to the thickness of just a few atoms. This metrological exactness is helping to make possible the next generation of high-power computer chips, produced using extreme ultraviolet lithography.



engineering. For example, the surface of the optical parts in the camera must be accurate to within just a few atoms, because the smoothness of the surface finish determines how much of the light will be scattered and lost. Less scatter translates into a shorter exposure time for each chip and a higher production rate. The overall shape of the optical surface must also be accurate to improve the accuracy with which the pattern is projected.

Existing metrology could not measure surface shape with sufficient precision, so Livermore developed the absolute interferometer, which can measure errors of a surface to just a few atoms (Figure 3).[3] This new ability to measure surfaces of optical parts to the required tolerances removes one of the roadblocks to further development of EUV lithography.

Exploiting Laser Cutter's Precision

In another project, Livermore engineers are developing a workstation for the femtosecond laser cutter, a breakthrough manufacturing process that also spun off from inertial confinement fusion work. This laser cutter delivers pulses lasting just 50 to 1,000 femtoseconds (quadrillionths of a second), ionizing the material and removing it atom by atom. The precision engineer's job was to design and construct a machine tool to a precision that can exploit the femtosecond laser's capabilities to cut materials, whether they be steel or soft tissue, very exactly and with little or no collateral damage. In the workstation, ultrasonic sensor technology is used to locate and mark the cut. The cutting takes place in a vacuum chamber with diagnostic cameras measuring the cut.

The cutter's first application was to disassemble nuclear weapons at DOE's Pantex plant.[4] Several major manufacturers are interested in incorporating this new cutter into their manufacturing process. With the workstation, this precision cutting technology can make the move to industry.

The Impact of Precision

The precision work at Lawrence Livermore has had an impact not only on the Laboratory itself, but also on everyday products. Because so many precision manufacturing methods developed at Livermore have been transferred to the private sector, companies and individuals outside Lawrence Livermore can obtain many machines, parts, and materials of a higher quality and at a lower cost than was previously possible.

An example of Livermore's effect on the private sector involves the diamond turning of infrared optical components for heat-seeking missiles. Because the Department of Defense wanted to be able to obtain the components commercially, it paid Livermore to transfer the diamond-turning technology to the private sector in the early 1980s. The technology that produced those components was the forebearer of the methods used today to produce precision components for bar-code scanners, video cassette recorders, compact disc players, laser printers, and copy machines.

A few breakthrough technologies, such as the laser interferometer and the personal computer, have revolutionized how machines are designed, but most advances in precision engineering today are incremental. This in no way dilutes their importance, however. It has been estimated, for instance, that modest improvements in the accuracy of fabricating the skins and spars for a Boeing 747 jet would reduce the weight of the aircraft by 10,000 pounds. If those minimal changes were made to all 747s in use today, the net result would be a fuel cost savings of about $600 million every year for U.S. airlines.

Precision manufacturing is also expected to reduce hydrocarbon emissions from combustion engines. Figure 4 shows how these emissions were reduced from 3.2 grams per mile to 0.9 gram per mile when the catalytic converter was introduced in the mid-1970s and then to about 0.4 gram per mile when electronic controls were added. With present engine designs and manufacturing technologies, automobile manufacturers cannot meet demanding new emission standards. But the same manufacturers predict that new combustion chamber designs using precision engineering technologies will drive the next major advance in emissions reduction.

A Leader in the Field

Although precision engineering has been a core competency at Livermore Laboratory for four decades, it was not a cohesive discipline in the U.S. private sector until about 20 years ago. Livermore's long-standing leadership in the field of precision engineering has prompted it to take a leading role in broadening the recognition and application of the discipline. In the mid-1980s, several Livermore engineers helped to establish the American Society for Precision Engineering, which has become an active international organization, with more than 700 members from industry, universities, and government.

Today, precision engineering is a recognized technology that is used regularly to respond to a range of challenges. The Laboratory, manufacturers, and others are relying increasingly on precision engineering to meet future demands and reduce costs.

Precision engineering will have a place at Livermore as long as physics experimentation continues. Physics experiments cry out for perfection. While perfection is seldom possible in an engineered system, increasing the system's precision brings it as close to perfection as possible.

—Katie Walter

Key Words: diamond turning, extreme ultraviolet (EUV) lithography, femtosecond laser cutter, KDP (potassium dihydrogen phosphate), Large Optics Diamond Turning Machine (LODTM), machine design,

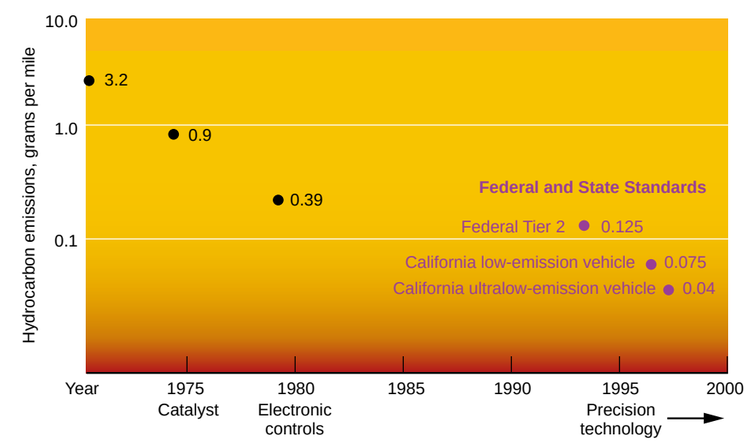


Figure 4. The use of precision engineering in the manufacture of internal combustion engines is expected to reduce hydrocarbon emissions to levels that meet new federal and state standards.

National Ignition Facility (NIF), optical systems, precision engineering, process development.

References

1. For more information on the early days of precision engineering at Livermore, see articles in *Energy & Technology Review*, Lawrence Livermore National Laboratory, Livermore, California, UCRL-52000-87-9 (September 1987). Many of the advances in precision metrology discussed in these articles have become commercial instruments.
2. See "Growing High-Quality KDP Crystals Quickly," *Energy & Technology Review*, Lawrence Livermore National Laboratory, Livermore, California, UCRL-52000-94-11 (November 1994), pp. 3–5.
3. "New Interferometer Measures to Atomic Dimension," *Science & Technology Review*, Lawrence Livermore National Laboratory, Livermore, California, UCRL-52000-97-10 (October 1997), pp. 6–7.
4. See "A New Precision Cutting Tool: The Femtosecond Laser," *Science & Technology Review*, Lawrence Livermore National Laboratory, Livermore, California, UCRL-52000-97-10 (October 1997), pp. 10–11.

For additional information please contact Kenneth Blaedel (510) 422-0290 (blaedel@llnl.gov) or Daniel Thompson (510) 422-1915 (thompson7@llnl.gov).

About the Precision Engineers

KENNETH BLAEDEL is leader of the Precision Systems and Manufacturing Group (formerly the Machine Tool Development Group), part of the Engineering Directorate's Manufacturing and Materials Engineering Division at Lawrence Livermore. He is a specialist in material removal processes, particularly the grinding of brittle materials, and in the design of machines to conduct these processes. He has been involved in the design and application of many of the precision diamond-turning machines at the Laboratory. He holds both a B.S. and Ph.D. in mechanical engineering from the University of Wisconsin and is an active member of the American Society for Precision Engineering. He has extensive experience in dimensional metrology and currently chairs the Environment for Dimensional Measurement Committee for the American Society of Mechanical Engineers/American National Standards Institute.

DANIEL THOMPSON has been associated with precision engineering at Livermore since joining the Laboratory in 1975. He is currently Program Leader for the Energy Directorate's Precision Engineering Program and previously led Livermore's Machine Tool Development Group for 11 years. He received a B.S. in mathematics from the University of Colorado and an M.E. in mechanical engineering from the Thayer School of Engineering at Dartmouth College. He is past president of the American Society for Precision Engineering and serves as associate editor for *Precision Engineering*. He received the Federal Laboratory Consortium award for excellence in technology transfer and has received two IR-100 (now R&D 100) awards for developments in precision engineering.

Enhanced Surveillance of Aging Weapons

Figure 1. The relative size of the vacuum-tight microextractor assembly (left) and the coated microextraction fiber (right) compared to a quarter. The fiber is less than 400 micrometers in diameter.

WITHIN the Department of Energy, the word "surveillance" has a meaning closely akin to the word from which it derives—"vigilance." For years, the DOE has had an ongoing surveillance program to verify the safety and reliability of U.S. nuclear weapons. Surveillance has always dealt with the possible effects that aging may have on weapon materials and components. The study of aging effects is even more important now that nuclear testing has ceased, no new weapons are being developed, and the existing arsenal is growing older. Current plans call for many of the weapon systems in the arsenal to be in the stockpile well beyond their design lifetimes, and scientists must be able to predict the behavior of these systems as they age.

DOE's enhanced surveillance program is just one facet of science-based stockpile stewardship.[1] Since the program began in 1995, it has been managed by DOE's Office of Defense Programs. But the work is actually being done by the seven DOE facilities that designed and fabricated the weapons in the first place—Livermore, Los Alamos, and Sandia national laboratories as well as the Y-12, Kansas City, Pantex, and Savannah River plants.

The objective of the enhanced surveillance program is to develop diagnostic tools and predictive models that will make it possible to analyze and predict the effects that aging may have on weapon materials, components, and systems. With this information, program participants will be able to determine if and when these possible effects will impact weapon reliability, safety, or performance and thus will be able to anticipate needs for weapon refurbishment. Because the DOE weapons complex has been reduced in numbers of plants and personnel, the lead time necessary to manufacture critical components must be as long as is practical. Enhanced surveillance is crucial to providing the longest lead time the DOE complex can afford to provide.

Specifically, the program's goals are to predict component and material failure mechanisms; predict the service lives of materials, components, and overall systems; determine the feasibility of monitoring critical components in place, in real time, nondestructively; and develop diagnostics for failure mechanisms when time to failure cannot be adequately predicted.

Surveillance of Thermonuclear Weapons

The seven participating facilities are working on 110 tasks in three focus areas: primaries, secondaries, and nonnuclear components. Livermore has only minor involvement with project work related to nonnuclear components, which is Sandia's specialty. However, the Laboratory is heavily involved in the first two areas because its specialty has always been the development of primaries and secondaries, where the fission and fusion processes occur in a thermonuclear weapon. For the work at Livermore, Jeffrey Kass and John Kolb are leading a multidisciplinary team that includes physicists, engineers, materials specialists, and technicians from several directorates.

For weapon primaries, the Livermore team is evaluating changes that occur over time to the pit's special nuclear materials and to various types of high explosives. For example, plutonium irradiates itself and, given enough time, may change shape ever so slightly. Other tasks involve developing sensors, imaging devices, and diagnostic techniques for nondestructive evaluation of a primary. The team is also developing methods for studying the dynamic properties of primaries through small-scale testing.

Similar work is under way for weapon secondaries, characterizing materials in detail and developing material aging models to predict material life. Livermore staff are also

developing diagnostic technologies to verify material and system predictability.

The Livermore project contributes to the work of the Surveillance Information Group, which includes representatives from all the DOE laboratories and plants. The Surveillance Information Group has conducted pilot projects in support of the DOE-wide Nuclear Weapons Information Group,[2] whose mission is to develop a secure, Web-based, electronic archive of old and new classified documents and other information on weapons design, production, and testing.

Nondestructive Evaluation

Livermore is leading a task to develop a technique called microextraction for nondestructive evaluation of the weapon primary. Microextraction is one of several technologies under development that will be used to determine how aging and the environment may affect the stability of a weapon's components.

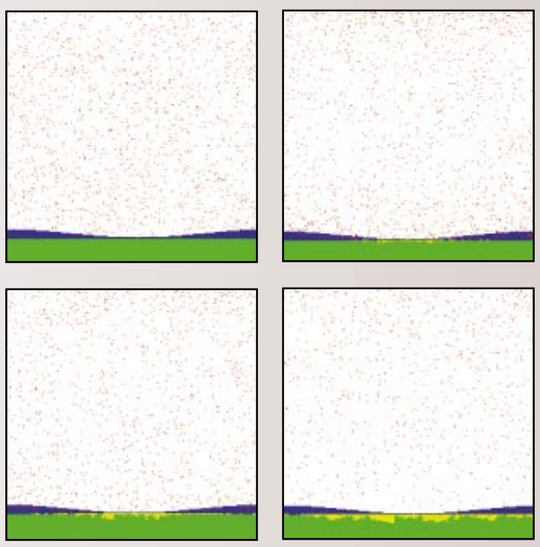


Figure 2. A two-dimensional model of the hydriding of a material surface inside a mock thermonuclear weapon's nuclear explosive package in the presence of a layer of oxide. Red particles represent hydrogen, the purple overlayer is metal oxide, green is pure metal, and yellow is the hydrided metal. The sequence is from left to right and top to bottom.

Initial work with microextraction analyzed the primary's headspace gases. Studies show that primaries outgas at significant levels. To study these outgasses, Laboratory scientists exposed a microfiber coated with a solid-phase adsorbent to the weapon headspace gas to collect any chemical species. They then analyzed the microextraction fiber using gas chromatography and mass spectrometry. They have also developed methods to move the fiber as close to the weapon's purge valve as possible to permit essentially direct sampling of the weapon headspace and obtain more accurate data (Figure 1).

The Livermore team then characterized the material standards associated with various weapon systems. It found that many of the compounds absorbed in some high explosives may be traced to the use of other materials. For example, significant levels of toluene arise from its use as a solvent in the synthesis of the high explosive TATB. Data analysis thus far demonstrates that the outgassing and absorption processes observed on the core samples would not have significant effects on other materials in the near term because the outgassed species are nonreactive. The next step, which is still under way, is to complete an initial survey of systems and associated materials developed at Livermore.

Livermore is also leading an effort to implement microextraction to assess the aging of organics in closed environments. Valuable baseline information on new and aged weapons components has been obtained at DOE's Savannah River and Kansas City plants, with Livermore providing guidance on the effort.

Another task that Livermore is leading addresses modeling of material aging in the nuclear explosive package (NEP) of thermonuclear weapons. The NEP is a closed environment that contains exceptionally pristine and dry materials. It is enclosed in a can that prevents the interaction of the materials in the NEP with the outer atmosphere.

Livermore's goal is to develop a comprehensive computer model of the chemistry of this closed environment. Models are being developed of the interaction between the materials and between the materials and the gases left in the NEP during assembly. The time it will take for significant interaction to occur is important for the question of when these components will need to be refurbished or remanufactured.

The team is developing models for the reaction of gases with materials and for the diffusion of gases through the NEP. The reaction of gases with metals is a complicated process. Frequently, a layer of oxide on the metal causes the reaction to occur nonuniformly. As shown in Figure 2, a two-dimensional model demonstrates the pitting that may occur during this reaction.

These reaction models must be incorporated into a larger model of the transport and reaction of gases in the system. The Livermore team has begun to do just that using TOPAZ, one of the computer codes developed at the Laboratory for calculating the mechanical properties of materials. The team has demonstrated that TOPAZ, which was designed to model thermal diffusion, can be adapted to calculate gas transport through the NEP system when the grid for TOPAZ is carefully developed. Detailed models of the transport paths in the NEP have already been produced.

Continuing work for this task includes creating advanced gas–solid reaction models and, more important, modifying the computer code to include these models.

A Look Ahead

Work on the enhanced surveillance program continues. By about 2002 or 2003, DOE hopes to have in place the models and diagnostic tools it needs to determine when weapon components need replacement and ultimately to predict a weapon's safety, reliability, and lifespan. This knowledge will be significant for effective management of our nuclear arsenal.

—Katie Walter

Key Words: diagnostics, enhanced stockpile surveillance, high explosives, nondestructive evaluation, nuclear explosive package (NEP), Nuclear Weapons Information Group, stockpile stewardship.

References

1. For more information on science-based stockpile stewardship, see "Keeping the Nuclear Stockpile Safe, Secure, and Reliable," *Science & Technology Review*, Lawrence Livermore National Laboratory, Livermore, California, UCRL-52000-96-8 (August 1996), pp. 6–15.
2. See "Preserving Nuclear Weapons Information,"*Science & Technology Review*, Lawrence Livermore National Laboratory, Livermore, California, UCRL-52000-97-5 (May 1997), pp. 18–19.

For further information contact Jeffrey Kass (510) 422-4831 (kass1@llnl.gov) or John Kolb (510) 422-6424 (kolb1@llnl.gov).

A National Strategy against Terrorism Using Weapons of Mass Destruction

THE World Trade Center and Oklahoma City bombings signaled a change in the character of terrorism in the U.S. Most of the previous acts of domestic terrorism have not involved mass casualties. However, recent incidents indicate an apparent desire of terrorists to injure or kill large numbers of innocent people—six people were killed and more than 1,000 injured in the World Trade Center bombing, and 168 people died in the bombing of the Alfred P. Murrah Federal Building.

As horrifying as these acts of terrorism were, damage and casualties could have been much greater if the terrorists had used weapons of mass destruction (WMD)—nuclear, chemical, or biological weapons. In March 1995, the Aum Shinrikyo cult demonstrated that terrorists can acquire WMD with its sarin nerve gas attacks in the Tokyo subway that killed 12 people and sickened more than 5,000.

An open society like ours in the U.S. is particularly vulnerable to WMD terrorism. Information on nuclear, chemical, and biological weapons is readily available on the Internet and in many how-to books. There is increasing evidence of illegal trafficking in nuclear materials. In addition, a number of countries hostile to the U.S. are known to be developing WMD capabilities, and some of them are known to support terrorist groups.

Livermore Study Group Formed

In June 1996, the Director of Central Intelligence and the Deputy Secretary of Energy chartered a study of the threat posed by terrorist groups using nuclear, chemical, or biological weapons in the U.S. Organized by Lawrence Livermore with Associate Director Wayne Shotts as the sponsor, the group was chaired by R. James Woolsey, former Director of Central Intelligence, and Joseph S. Nye, Jr., former Assistant Secretary for Defense for International Security Affairs. Known as the Livermore Study Group, it included eminent experts from the Central Intelligence Agency, the Departments of Defense and Energy, the Federal Bureau of Investigation, the Arms Control and Disarmament Agency, Congress, U.S. industry, and academia.

The study group examined the potential of terrorist use of WMD against the U.S., reviewed current U.S. capabilities, and made recommendations for enhancing the nation's ability to prevent and respond to this threat.

U.S. Poorly Prepared for WMD Terrorism

The study group concluded that the U.S. is ill-prepared to respond to a terrorist attack that uses WMD. According to co-chair Jim Woolsey, "Of all the threats that could inflict major damage to the U.S., terrorists using weapons of mass destruction is the threat for which the nation is least prepared." The study group notes that although existing capabilities work well for planned high-risk events like the 1996 Atlanta Olympics, no integrated system is in place to deal with a threat of the magnitude, complexity, and severity of WMD terrorism.

The study group recognized that a nascent national policy addressing the threat of WMD terrorism is in place, that it is being implemented at the level of the National Security Council (NSC) by a small staff, and that this high-level group's efforts are making progress in coordinating national resources to meet the challenges posed by WMD terrorism. However, much remains to be done.

Table 1. End-to-end strategy for responding to threats and acts of WMD terrorism.

Intelligence and warning	Prevention	Crisis management	Consequence management	Retaliation
• Strategic warning • Tactical warning	• Denial • Demotivation • Deterrence • Elimination	• Detection • Threat validation • Location • Weapon assessment • Impact assessment • Attribution • Demotivation and deterrence • Render safe	• Damage assessment • Evacuation and protection • Reconstitution • Cleanup	• Attribution • Prosecution • Military response

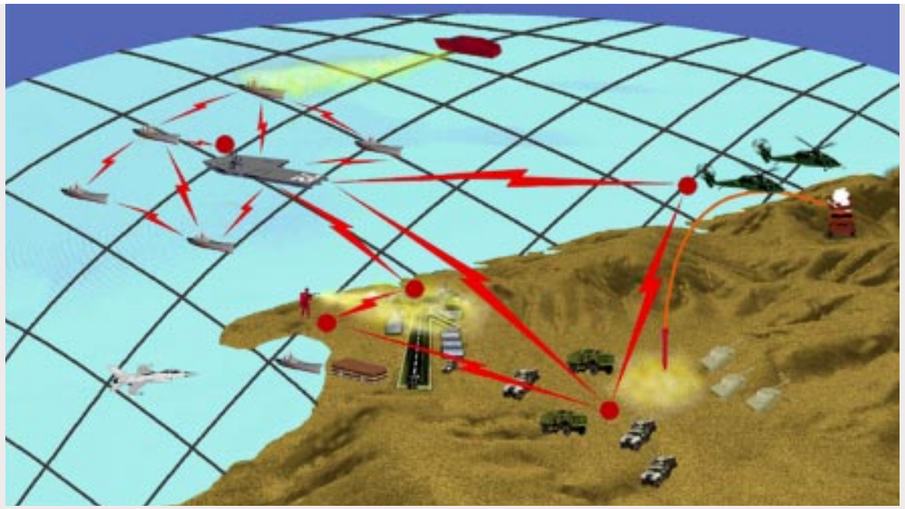


Figure 1. The Joint Biological Remote Early Warning System (JBREWS) is a system of networked sensors and communication links being developed to rapidly alert field troops of an attack with biological weapons.

National Strategy Recommended

The study group's overriding recommendation is, therefore, to give the threat of terrorism using WMD the highest priority in U.S. national security policy. Specifically, it recommends an accelerated and intensified national program, integrated across the entire federal system and managed as a program out of the NSC, to address comprehensively the threat of WMD terrorism.

The study group emphasized that an end-to-end systematic strategy is the best defense against WMD terrorism. Through an enhanced national program, an end-to-end systematic strategy could be implemented that integrates technology, operations, and policy and provides a framework for coordinated local, state, and federal emergency response. "We are not alone in our thinking," says Wayne Shotts, Laboratory Associate Director for Nonproliferation, Arms Control, and International Security and study sponsor. "A number of other studies related to the WMD threat have echoed the recommendation for a more robust national program." The Livermore Study Group takes these recommendations several steps further, urging an end-to-end strategy to provide a multilayered defense—from detection and prevention to reversal and response—in which all phases of a potential WMD terrorist attack can be addressed (Table 1).

Regarding the need for enhanced capabilities, the study group recognizes that many of the agencies responsible for counterterrorism have initiated significant new efforts to enhance U.S. capabilities in this arena. Nevertheless, in looking at an end-to-end strategy, the group identified a number of promising activities to improve the nation's ability to counter the threat of WMD terrorism.

For example, in the area of intelligence and warning, the study group's key recommendations are for more and better technologies and systems for tracking materials and activities indicative of WMD development, production, or transport and for policies and approaches that allow U.S. law enforcement agencies to function effectively in the modern communications-technology environment.

For the prevention phase, the study group calls for additional exploitation of diplomatic efforts, foreign policy, and treaties to promote WMD nonproliferation, strengthen international law enforcement, counter the conditions that foster terrorism, and facilitate the use of technology to counter WMD terrorism. They also note the need for better material control programs worldwide to prevent weapons materials from reaching the hands of terrorists and for expanded border protection programs to detect and intercept WMD materials.

To improve U.S. capabilities in crisis management, the study group urges accelerated development of new sensor systems (or improvement of existing systems) for detecting, identifying, and locating WMD materials and devices as well as technical capabilities for disabling and rendering WMD devices safe. Also required for more effective response and deterrence are better technologies, databases, and other means of forensic identification and attribution of the source, origin, and pathways of weapon materials and devices.

For consequence management, the study group stresses the need for intensified planning and preparation to enable emergency response personnel and medical communities to deal with mass casualties caused by WMD agents. The group also calls for faster and more accurate atmospheric transport and deposition models for determining the populations at risk if biological or chemical agents are released.

"The study group recognizes that implementing an integrated national program to deal with the constantly

changing threat of WMD terrorism will not be simple or straightforward," says Joe Nye, study co-chair. "However, we must not wait until a disaster of Pearl Harbor proportions forces us to recognize the severity of this threat and the need to mount an adequate defense."

Strategic Support from New Technologies

While the study group's charter does not extend beyond analysis and recommendations regarding WMD terrorism, Dennis Imbro, a Livermore scientist who served as liaison to the group, notes that "there must be a marriage of technology and policy to effectively counter this threat." The national laboratories are a valuable source of innovative and advanced technologies and thus can make important contributions to this critical aspect of national security. A number of technologies are being developed or refined at Lawrence Livermore that can address gaps in current U.S. counterterrorism capabilities.

One particularly promising technology with anti-WMD-terrorism application is the Wide-Area Tracking System (WATS) for detecting and tracking a ground-delivered nuclear device. Another is the Joint Biological Remote Early Warning System (JBREWS) for alerting U.S. field troops of an attack with biological agents (Figure 1). Both systems consist of a network of sensors and communications links, with information continuously evaluated by unique data-fusion algorithms. The sensors can be permanently deployed at chosen locations or mounted in vans for deployment on demand to protect specific areas for specific situations or events.

A portable radiation detector developed at Livermore to monitor and detect nuclear materials in the field at ambient temperatures also has potential uses to defend against WMD terrorism (Figure 2). The new system is based on a relatively new cadmium–zinc–telluride detector material and can separate gamma- or x-radiation energies to identify the isotopic signature of nuclear materials such as plutonium and uranium. The system has immediate applications, for example, in detecting and deterring nuclear smuggling through airports and shipping ports and in national and international nuclear materials safeguard operations.

To detect biological weapons, Livermore has developed immunoassay and DNA recognition-based sensors. Unlike most biodetection instruments, which are bulky and can only be used in laboratory settings, the mini-flow cytometer and the mini-PCR (polymerase chain reaction) instrument can be used in the field to identify specific biological warfare agents. (See *S&TR*, July/August 1997, pp. 14–16.) Both have been tested successfully at the U.S. Army's Dugway Proving Ground in Utah.

Livermore is also home to the Forensic Science Center, which uses a wide range of advanced chemical, biological, and nuclear analysis techniques to examine samples for the U.S. government and law enforcement agencies. Forensic science techniques are essential for identifying the source of WMD.

These Laboratory technologies and capabilities and others like them contribute greatly to meeting the monumental challenge of countering the threat posed by WMD terrorism.

—Lauren de Vore

Figure 2. The portable radiation detector being demonstrated by its inventor Anthony Lavietes can identify the precise isotopic signature of nuclear materials such as plutonium and uranium by detecting gamma radiation. It improves upon the large germanium-based detectors shown in the background and has a variety of applications, among them assistance with defense against terrorism using weapons of mass destruction.

Key Words: counterterrorism, cytometer, Forensic Science Center, Joint Biological Remote Early Warning System (JBREWS), Livermore Study Group, polymerase chain reaction (PCR) instrument, portable radiation detector, weapons of mass destruction (WMD), Wide-Area Tracking System (WATS).

For further information contact Dennis Imbro (510) 423-0220 (imbro1@llnl.gov).

Patents and Awards

Each month in this space we report on the patents issued to and/or the awards received by Laboratory employees. Our goal is to showcase the distinguished scientific and technical achievements of our employees as well as to indicate the scale and scope of the work done at the Laboratory.

Patent issued to	Patent title, number, and date of issue	Summary of disclosure
Thomas E. McEwan	**Time-of-Flight Radio Location System** U.S. Patent 5,661,490 August 26, 1997	An apparatus for measuring the time of flight of an electromagnetic pulse. A transmitter transmits a sequence of electromagnetic pulses in response to a transmit timing signal, and a receiver samples the sequence of electromagnetic pulses with controlled timing in response to a receive timing signal and generates a sample signal. A timing circuit supplies the transmit and receive timing signals. The receive timing signal causes the sampling by the receiver to sweep over a range of delays. An envelope detector converts the sample signal to a unipolar signal to eliminate effects of antenna-orientation mismatch. The envelope detector is an absolute-value circuit followed by a low-pass filter. A sample detection circuit indicates time of flight, from which the position of an electromagnetic pulse can be obtained.
Anthony M. McCarthy	**Method for Fabricating Transistors Using Crystalline Silicon Devices on Glass** U.S. Patent 5,663,078 September 2, 1997	A method for fabricating transistors on glass that overcomes the potential damage that may be caused during high-voltage bonding. A multilayer structure is formed on a silicon substrate and employs a metal layer that may be incorporated as part of the transistor. When the structure is bonded to a glass substrate, the voltage and current, because of the metal layer, pass through areas where transistors will not be fabricated. After removal of the silicon substrate, more metal may be deposited to form electrical contact or add functionality to the devices. By this method, both single and gate-all-around devices may be formed.
Stephen A. Payne Joseph S. Hayden	**Ultrafast Pulsed Laser Utilizing Broad Bandwidth Laser Glass** U.S. Patent 5,663,972 September 2, 1997	An ultrafast laser that uses a neodymium-doped phosphate laser glass characterized by a particularly broad emission bandwidth to generate the shortest possible output pulses. The laser glass is composed primarily of phosphate (P_2O_5), alumina (Al_2O_3), and magnesium oxide (MgO) and possesses physical and thermal properties that are compatible with standard melting and manufacturing methods. The emission bandwidth is greater than 29 nanometers and more, preferably greater than 30.5 nanometers. The broad-bandwidth laser glass can be used in mode-locked oscillators as well as in amplifier modules.
Chuen-Tsai Sun Jyh-Shing Jang Chi-Yung Fu	**Intelligent System for Automatic Feature Detection and Selection or Identification** U.S. Patent 5,664,066 September 2, 1997	A neural network that uses a fuzzy membership function, the parameters of which are adaptive during the training process, to parameterize the interconnection weights between layers of the network. As in a conventional neural network, each node in each level, except the input level, produces an output value. In a conventional neural network, all of the connection weights are adjustable and must be "trained." To reduce the number of parameters that need to be adjusted, a fuzzy membership function is used to define the interconnection weights between two of these layers. A tremendous reduction in the number of parameters for training is achieved because the field of connection weights being input to a node has been parameterized.
Daniel M. Makowiecki Alan F. Jankow	**Boron Containing Multilayer Coatings and Method of Fabrication** U.S. Patent 5,670,252 September 23, 1997	The production of multilayers containing thin boron, cubic boron nitride, or boron carbide films or coatings. The boron-containing multilayers may be deposited as hard coatings on surfaces, such as on tools or engine parts, and contain no morphological growth features. By alternating the formation of boron films or cubic boron nitride and boron carbide films, a multilayer boron/boron carbide, cubic boron nitride/boron carbide, or a boron/cubic boron nitride/boron carbide film or coating may be produced. The various layers of the multilayer may be diffused, blended, or graded to contain from 0 to 100% boron or cubic boron nitride or boron carbide, and the interfaces of the layers may be discrete or diffused.
John M. Gonsalves	**Pendulum Detector Testing Device** U.S. Patent 5,672,807 September 30, 1997	A testing device composed of several pieces of polyvinyl chloride tubing or pipe attached to a plastic holder. The test object, such as a weapon encapsulated in a protective cover, is secured in the holder. The holder and enclosed weapon are mounted in and swing through the archway of a walk-through detector system in a pendulum motion for any designated number of passes needed to complete the test. The components of the test device can be easily assembled and positioned in various locations of the detector facility archway, thereby simulating where the contraband might be concealed on a person walking through the detector system. The response of the detector system is observed.

Patent issued to	Patent title, number, and date of issue	Summary of disclosure
Joseph R. Kimbrough Nicholas J. Colella	**System Level Latchup Mitigation for Single Event and Transient Radiation Effects on Electronics** U.S. Patent 5,672,918 September 30, 1997	A power bus connected to a microelectronic circuit that is radiation susceptible. An ionizing radiation pulse detector detects a pulse of ionizing radiation and provides, at an output terminal, a detection signal indicative of the detection of a pulse or ionizing radiation. A current sensor is coupled to the power bus for determining an occurrence of excess current through the power bus caused by ionizing radiation. The current sensor has an output terminal that provides a control signal indicative of the occurrence of excess current through the power bus caused by a latchup condition in a microelectronic circuit connected to the power bus.

Awards

Two teams of Laboratory employees received **Hammer Awards** from the National Performance Review in recent ceremonies in Washington, D.C. **David Gutierrez**, from the Electronics Engineering Department, and colleagues **Kris Chubb** and **Pamela Harris**, provided technical support for creating the U.S. Business Adviser Web site, which was designed to make government information relevant to small and large businesses easily accessible. **Barbara Davis**, former manager of the Information Technology and Security Center, worked with **Joel Wong**, **Bill Silver**, and **Larry Moon** to create a process for collecting and disseminating lessons learned in environmental management, worker safety, and health across the DOE complex. The Hammer Awards were created by Vice President Al Gore to recognize special achievements in the efforts to reinvent government by cutting red tape and making government more efficient.

Don Lesuer has been elected a **Fellow** of the **American Society of Materials** (ASM). A Laboratory employee for 20 years, Lesuer is a group leader in the Engineering Directorate's Manufacturing and Materials Engineering Division. He was honored "for outstanding contributions as an inventor and leader in mechanical metallurgy related to advanced metal–matrix composites, metal-laminated composites, hypereutectoid (or high-carbon) steels and superplasticity."

Physicist **Seymour Sack** is a 1997 recipient of the **Fleet Ballistic Missile Achievement Award** from the U.S. Navy's Strategic Systems Program. The annual award recognizes significant contributions in science and engineering "which have been pivotal to the success of the Fleet Ballistic Missile Strategic Weapons Systems." Sack, who retired in 1990 and is currently a Laboratory associate, was nominated for the award by Laboratory Associate Director George Miller as "the preeminent designer of nuclear warhead primaries in the history of the U.S. nuclear weapons program." Sack joined the Laboratory in 1955 and, in 1973, won the prestigious E. O. Lawrence Award for his continuing influence at the Laboratory.

Abstracts

Making Information Safe

The attack of the Morris Worm one night in 1988 triggered the formation of the Computer Security Technology Center at Lawrence Livermore National Laboratory. One arm of this center, the Computer Incident Advisory Capability, manages and contains system intrusions while the other develops tools and employs strategies to safeguard systems against intrusions and pervasive hackers. Five of the advanced tools developed to deter, detect, and analyze computer security problems are described in the article.

Contact:
Douglass Mansur (510) 422-0896 (mansur1@llnl.gov).

Engineering Precision into Laboratory Projects

Since the 1950s, Lawrence Livermore has been using precision engineering to make manufacturing processes more effective. Livermore has developed a number of metrological devices and machine tools that first were used to build more effective nuclear weapons and more recently have been applied to such projects as the National Ignition Facility and extreme ultraviolet lithography for making the next generation of computer chips. Many of these tools have spun off to the private sector and are used in products that benefit us all. Livermore has long been at the forefront of precision engineering. Several Livermore engineers helped to found the American Society for Precision Engineering, and Laboratory precision engineers continue to participate in national and international efforts to establish metrology standards.

Contact:
Kenneth Blaedel (510) 422-0290 (blaedel@llnl.gov) or
Daniel Thompson (510) 422-1915 (thompson7@llnl.gov).

© 1997. The Regents of the University of California. All rights reserved. This document has been authored by the The Regents of the University of California under Contract No. W-7405-Eng-48 with the U.S. Government. To request permission to use any material contained in this document, please submit your request in writing to the Technical Information Department, Publication Services Group, Lawrence Livermore National Laboratory, P.O. Box 808, Livermore, California 94551, or to our electronic mail address*report-orders@llnl.gov*.

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

U.S. Government Printing Office: 1998/683-051-60039