Conf-9010304--2

UCRL-JC--105099

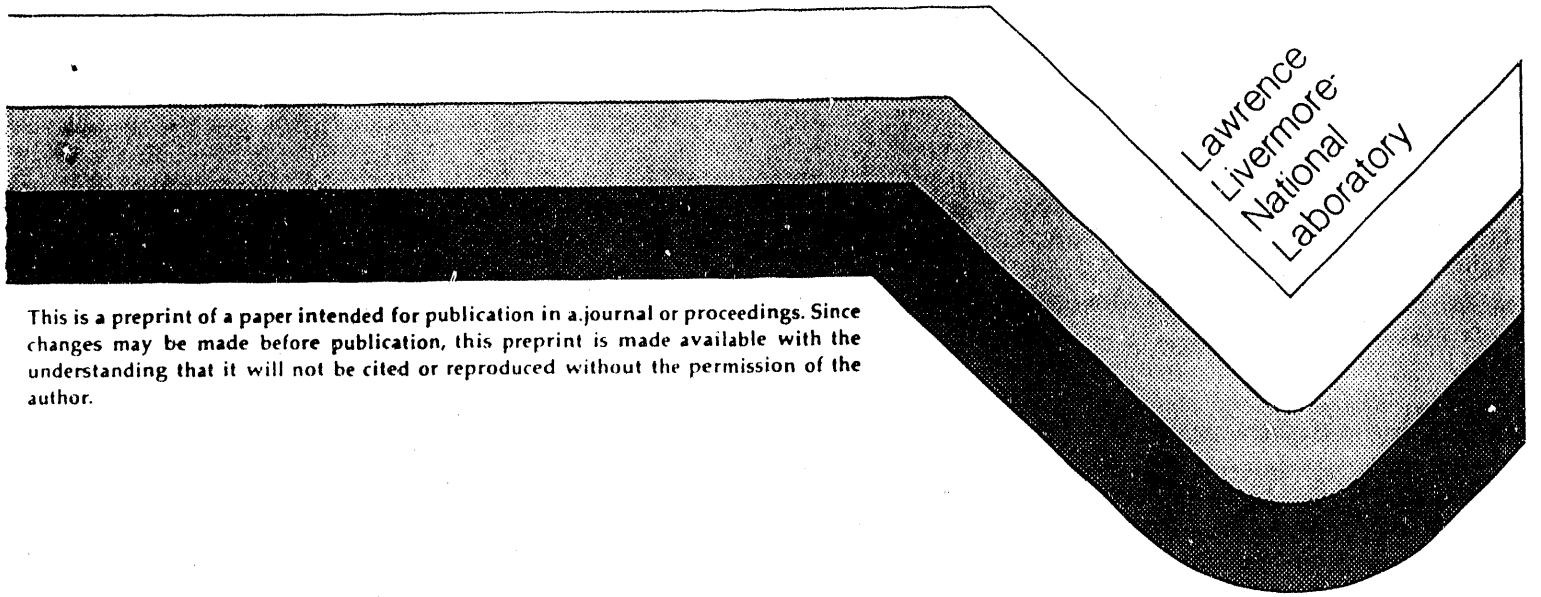
DE91 007136

DOE's Computer Incident Advisory Capability (CIAC)

Eugene Schultz

This paper was prepared for submittal to
the Office Information Management
Conference (OIM)
New Orleans, LA
October 24-26, 1990

September 1990



DOE's Computer Incident Advisory Capability (CIAC)

Eugene Schultz

University of California
Lawrence Livermore National Laboratory

Abstract

Computer security is essential in maintaining quality in the computing environment. Computer security incidents, however, are becoming more sophisticated. The DOE Computer Incident Advisory Capability (CIAC) team was formed primarily to assist DOE sites in responding to computer security incidents. Among CIAC's other responsibilities are gathering and distributing information to DOE sites, providing training workshops, coordinating with other agencies, response teams, and vendors, creating guidelines for incident handling, and developing software tools. CIAC has already provided considerable assistance to DOE sites faced with virus infections and worm and hacker attacks, has issued over 40 information bulletins, and has developed and presented a workshop on incident handling. CIAC's experience in helping sites has produced several lessons learned, including the need to follow effective procedures to avoid virus infections in small systems and the need for sound password management and system administration in networked systems. CIAC's activity and scope will expand in the future.

The theme of the year's Office Information Management Conference is "Quality in the DOE ADP Environment." One important aspect of quality is establishing and maintaining secure computing systems. It is difficult to envision quality in the computing arena under conditions in which systems are accessed by intruders, files are deleted or altered by unauthorized users or malicious code, or viruses or worms deteriorate system performance and/or prevent normal access to data. In many respects the worst thing that can happen in a computing system is loss of trust by users. Network users who learn that their accounts have been compromised by an intruder or small systems users who lose important files because of a virus can easily lose trust in their systems and motivation to operate their systems to accomplish their work. Computer security is a vital ingredient in helping to maintain user trust and to keep systems available to users, so that users can productively use these systems.

Computer security has become an increasingly complex field since the early days of computing. Not only have computing systems become considerably more sophisticated, but the types of threats and their potential consequences have also changed substantially. Until a few years ago most computer security incidents could be described as cases of unauthorized use of systems and/or insider attacks. The advent of viruses in the small system arena posed a new level of technical challenge. Network attacks such as sophisticated intrusions, e.g., the attacks on DOE and other machines by a West German described by Stoll (1989) and the 1988 Internet Worm exemplify even higher levels of computer security threat.

*This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract No. W-7405-Eng-48.

Traditionally, computer security involves planning and implementing protections against malicious or unwanted code, procedural failures, intrusions into systems, and fraud, waste and abuse. Incidents in recent years, however, demonstrate that traditional computer security measures are insufficient to deal with the magnitude of threats facing computer systems. *Incident handling* is an additional, necessary element, because virtually no set of protections is sufficient to safeguard any system against every threat. The goal of incident handling is to return attacked systems to normal or mission status as quickly as possible with minimal damage, loss and disruption.

In 1988 the Department of Energy, recognizing the need to have an incident response team, committed to supporting such an effort at Lawrence Livermore National Laboratory. Early the next year, the Computer and Communications Security Group at LLNL launched the CIAC (Computer Incident Advisory Capability) Project. CIAC currently consists of four computer scientists charged with the primary responsibility of assisting DOE sites faced with computer security incidents (e.g., hacker attacks, virus infections, worm attacks, etc.). This capability is available to DOE sites on a 24-hour-a-day basis. CIAC is currently co-sponsored by Information Resources Management (IRM) within Administration, the Office of Safeguards and Security (OSS) within Defense Programs, and Energy Research Programs.

CIAC's Charter

CIAC is a project with a large variety of goals and objectives (Schultz, 1989). The CIAC team was formed primarily to provide a centralized incident response capability (including technical assistance) for DOE. This assistance is provided at no cost to DOE sites (unless travel on the part of CIAC team members is necessary). Part of CIAC's charter is to deal proactively with computer security issues by keeping sites informed of current events and vulnerabilities in operating systems and vendor products. This enables site computer security personnel to respond to threats in an appropriate and timely manner. Similarly, CIAC provides training on incident handling to share sound incident handling procedures, technical information, and lessons learned. CIAC has developed guidelines for incident handling to help sites with their contingency response plans. CIAC was also established to maintain liaison with other response teams and agencies. CIAC team members, for example, frequently communicate with the FBI concerning network attacks, coordinate actions with other national incident response teams, and work with vendors to obtain patches for vulnerabilities in vendor products. Part of CIAC's purpose is to serve as a clearinghouse--a central source of information--for data on threats, known incidents, and vulnerabilities. Another facet of CIAC's charter is to develop software for responding to events/incidents. For example, CIAC team members are currently developing a tool to determine whether patches have been made in SunOS computing systems. Finally, CIAC was established to analyze events and trends to help keep the DOE computing community aware of long-term threats and to update incident handling procedures and technical requirements (e.g., tools needing to be developed).

Accomplishments

Since its inception CIAC has assisted over 70 DOE sites on over 300 separate occasions. For example, last Fall CIAC team members helped individuals at DOE sites respond to a five week long DECNET worm attack. After disassembling the worm, we developed scripts to eliminate the worm from infected systems and to immunize systems from attack. At the same time we helped individuals who requested assistance in recovery procedures. An encouraging result was that relatively few DOE computing systems were

affected by this worm. CIAC has coordinated responding to numerous other network intrusions. During a rash of such intrusions earlier this year, CIAC team members identified compromised systems, notified cognizant personnel, and provided assistance when requested. The evidence we gathered and submitted to the FBI helped result in the arrest of several suspects. We have also assisted many users in recovery from virus infections on MS-DOS and Macintosh computers.

CIAC has also distributed over 40 information bulletins to DOE sites describing threats such as operating system vulnerabilities needing to be patched, ongoing hacker and worm attacks, and viruses with potential for massive disruption of small systems. Our bulletin board, containing useful information and many freeware/shareware packages, has been widely used throughout DOE. We have developed a two-day workshop on responding to incidents. Some of the topics covered include an overview of incident handling, responding to viruses, worms, and hacker attacks, major operating system vulnerabilities, and tools for improving security and responding to incidents. The very popular simulation at the end of the workshop requires attendees to play the role of a system manager who needs to set appropriate protections and adopt sound response strategies to fend off hacker attacks. We have already presented this workshop on 12 separate occasions.

In addition to dealing with daily operational matters, CIAC team members engage in special projects. We are developing a patch checking tool for SunOS systems. This tool will indicate to system managers exactly which vulnerabilities within any given system are and are not fixed. This effort will be a major impetus to closing vulnerabilities frequently exploited by attackers. We are also researching UNIX and UNICOS vulnerabilities, and are developing incident handling guidelines.

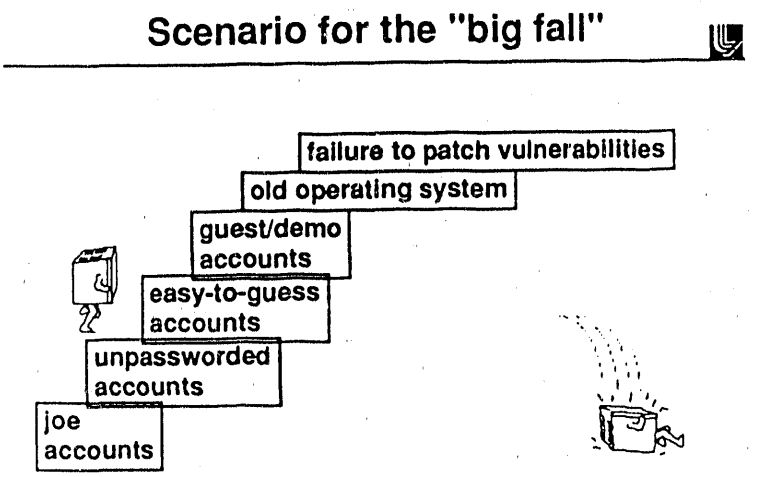
Lessons Learned

There have been many lessons learned concerning CIAC operations. We have, for example, learned a great deal about requirements for gathering legal evidence for prosecution of computer crime. Most relevant to this conference, however, is lessons learned about computer security practices within the DOE community. Because CIAC responds to incidents, CIAC is in a position to evaluate what is and is not working with respect to present computer security practices and policies, and what needs to be done.

The most prevalent problem within the DOE computing community is viruses. In fact nearly 40 percent of our dealings with sites involves viruses in some manner. Small systems users too often fail to practice safe computing procedures (Schultz et al., 1990). They risk virus infections by neglecting to check removable media and vendor software before introducing them into their own machines. Vendor demos are a major source of virus infections. Electronic bulletin boards are another source of risk to virus infections. When viruses infect systems, it is too often true that users are unaware of procedures to follow; users often do not know who to call in case of a virus infection. Fortunately, a relatively small percentage of computing systems become infected by a virus. In addition, most viruses are non-destructive, and are more of an annoyance than a grave threat to the integrity of small systems. Nevertheless, viruses (and the panic they too frequently cause) require manpower and disrupt computing systems, and, thus, are a serious detractor to the quality of the automated data processing environment.

Another concern is intrusions into networked systems. The main problem is that users of such systems often use weak passwords, allowing intruders and/or automated attack

scripts to penetrate the network. In one recent study between four and 60 percent of a subset of systems connecting to the Internet had passwords that could be cracked by a program with a dictionary consisting largely of common words and simple permutations of account names (Klein, 1990). System managers frequently do not patch system vulnerabilities, allowing intruders to bypass authentication procedures (i.e., user login) to access systems and gain privileged user status. Default accounts with presupplied passwords and guest/demo accounts are some other avenues of attack. The following slide from CIAC's workshop on incident handling provides an excellent illustration of the problem:



Finally, although DOE has made admirable efforts in defining computer security requirements, there is widespread uncertainty within the DOE computer security community concerning exactly what these requirements are. DOE Orders 1360.2A and 5637.1, applicable to unclassified and classified computing, respectively, are not sufficiently comprehensive to give clear guidance. We need a more precise and complete set of requirements for computer security.

CIAC's Future

CIAC's mission and capabilities are changing. CIAC is growing in size to deal with increasingly complex incidents, and is putting more emphasis on proactive activity. Our workshop, for example, helps us expand our ability to serve the DOE community by teaching others to respond the way we would respond. We hope to develop a variation of our workshop for managers only, to help managers coordinate better with technical personnel during incidents, and to help managers plan for incident handling more effectively. In a similar vein we would like to develop a more technically intensive workshop with "hands-on" training for system managers.

In the past CIAC team members have occasionally been called on to travel to sites to provide direct technical assistance. Because of the increasing complexity of incidents, we predict that we will be engaging in more activity of this variety. We would like to assist DOE in developing a definitive set of security requirements for classified and unclassified

computing systems. Finally, CIAC will be developing predictive threat models to help guide responses to future threats.

How to Contact CIAC

CIAC's business hours phone number is (415) 422-8193 or FTS 532-8193, and the off-hours/emergency number is (415) 971-9384. FELIX, CIAC's bulletin board, can be accessed at (415) 423-4753 or FTS 543-4753. CIAC's e-mail address is ciac@tiger.llnl.gov

References

Klein, D. V., "Foiling the cracker": A survey of, and improvements to, password security. UNIX Security II Workshop Proceedings, 1990, pp. 5 - 14.

Schultz, E.E., The Computer Incident Advisory Capability (CIAC). Center for Computer Security News, 1989, vol. 8, pp. 13 - 15.

Schultz, E.E., Brown, D.S., & Longstaff, T.A. Responding to Computer Security Incidents: Guidelines for Incident Handling. University of California Technical Report UCRL-104689, 1990.

Stoll, C., Tracking a Spy through the Maze of Computer Espionage: The Cuckoo's Egg. New York: Doubleday, 1989.

END

DATE FILMED

02/19/91