CONF-9204136--1

LA-UR- 92-1389

Title: RESULTS OF THE FIRST UNICOS SECURITY SURVEY

LA-UR--92-1389

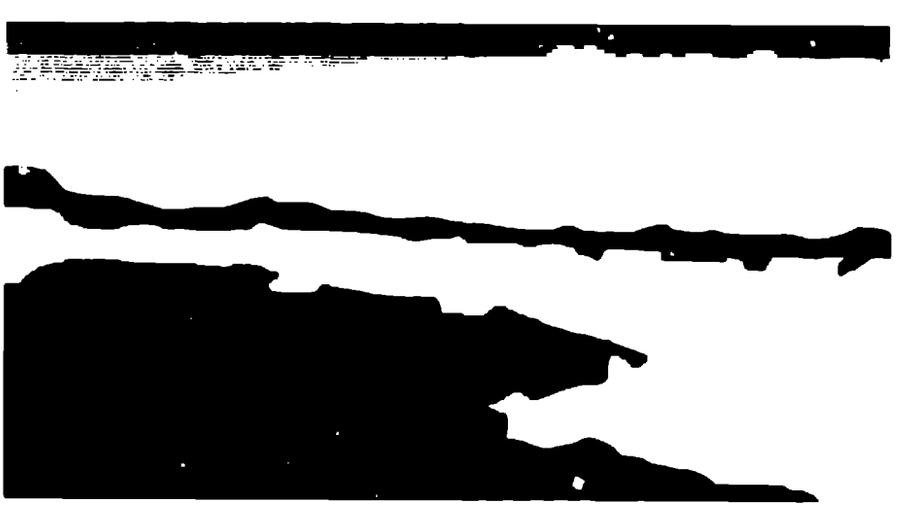
DE92 013429

MAY 07 1992

Author(s): G. G. Christoph, C-8

Submitted to: 29th Semi-Annual Cray User Group Meeting
Berlin, Germany
April 6-10, 1992

MASTER



Los Alamos
NATIONAL LABORATORY

Form No. 836 R5
ST 2629 10/91

Results of the First UNICOS Security Survey

Gary G. Christoph, Ph.D.
Computing and Communications Division
Los Alamos National Laboratory
Los Alamos, NM 87544

Abstract

At the Santa Fe CUG, in September, 1991, a brief survey was distributed to attendees in order to begin developing a database of sites interested and active in using UNICOS security protections and features. Forty-two individuals attended a Security BOF session; their responses comprised about three-quarters of the forty-six sites (representing 62 installed machines) who completed and returned the survey questionnaire. Although the sample is clearly biased--most of those responding had already evidenced interest in security by attending the BOF--the broad range of sites, industrial and academic as well as government and military, that were represented was surprising. Fully 50% of the 62 installed machines were actively running UNICOS Secure Mode. This talk will provide an overview of the results of the survey, which will be repeated at least annually by the new Security MIG. A tabulation of the sites that have some experience with running Secure Mode UNICOS will be made available to all sites, in keeping with the goal of disseminating such hard-won experience with UNICOS security.

Introduction

This paper reports the results of a survey of CUG sites in September, 1991. This survey was undertaken because the author found that field experience in implementing and using various UNICOS security features was not being disseminated. Indeed, there appears to be no formal way for collecting and distributing such information. CUG sites are largely on their own, with only CRI manuals and a telephone connection (usually highly filtered through their CRI on-site Analyst) to CRI Tech Support in Eagan, to figure out how to configure, install, and put into production UNICOS security features. In some cases, the site would also contend with unpublished dependencies or bugs, problems that had been fixed only in more recent revisions.

Sites that have had a history of performing much of their own system maintenance, I believe, were only in slightly better shape than those sites that relied upon CRI on-site analysts to configure and install their systems. Unless an analyst (and I do not here restrict myself to CRI analysts, but include myself in

this category) was trained to be alert for security holes, and unless some breach occurred and brought itself to the attention of the analyst, the system might run for considerable periods of time with quite large vulnerabilities, including the potential complete capture of the machine.

Such vulnerabilities derive from three types of errors, the first two of which legitimately fall under the responsibility of the site manager to control, with the last being the responsibility of the vendor:

1. Vulnerabilities that derive from users improperly using UNIX (TM) system features. Examples of this are access permissions on user files and directories that have been set unacceptably wide open, namely, `rwx` for each of owner, group and world.

2. Vulnerabilities that derive from the system being improperly configured or installed. Examples of this are network configuration tables or features that are installed with defaults that are inappropriate for the site's environment, such as `"IP_FORWARDING ON"`, which allows the Cray to serve as a transparent gateway to other machines, networks or workstations, to which users may not otherwise have legitimate access.

3. Vulnerabilities that derive from system software that is not perfect. An example of this is a system `setuid` utility, such as the UCBerkeley command, `rdist`, which (until recently fixed) permitted a user to change the ownership and access rights of any object on the system (and thereby capture root and secadm privileges).

My point here is not that such vulnerabilities exist, but that the knowledge of them is poorly disseminated and hard to come by. This is complicated by the fact that UNICOS and UNICOS Secure Mode have been under constant evolution for the last several years, so that sites have had their hands full just trying to keep up with installing and administering this complicated system. And CRI has had its hands full in communicating the many changes: it is my understanding that between Release Level 6.0 and 6.1.5a, there are on the order of 2000 mods. Thus, an important objective for developing this security survey was to engender a customer network for discovering and disseminating UNICOS security information. For several good reasons, which will be discussed below, we sites should not rely entirely upon CRI for communication of such information.

Finally, the main stimulus for carrying out the survey was this author's personal experience in trying to learn how to implement a Secure Mode UNICOS feature, namely, compartments.

Last Summer, in the course of trying to understand UNICOS compartments, to see if Los Alamos could safely and reliably use this feature to separate groups of users, I discovered just how difficult getting this knowledge can be. The documentation, including the more extensive CRI Training Manuals, does not warn of any problems. But the documentation does not go very far beyond a

description of the security policy involved and the various relevant commands and how they are supposed to work. With the exception of ACL's, no algorithms are explicated in the documentation. Our previous experience with implementing UNICOS multiple security levels at Los Alamos suggested to us that a number of unexpected problems would be found. It was therefore important, if disruption to users was to be kept to a minimum, to try to anticipate and head off as many of these as possible before bringing up compartments.

After reviewing the available documentation, I attempted to obtain from CRI the names of sites that were actively using compartments in production. In this, CRI was not particularly informative, but for a good reason. As a vendor, CRI is severely limited, legally, in what information about one customer can be released to another customer. The most that CRI could do on my behalf was to try to contact a site that was using compartments and to ask them if they would be willing to call me. This avenue failed utterly. I also discovered that CRI is, or seems, relatively unaware of how sites are using UNICOS. One cannot assume that site analysts are feeding field experience back into Eagan. Tech support was, as I later learned, completely unaware of a number of North American sites that were actively using compartments in production with real users. However, even my extensive telephoning to other sites, even to CUG officers, failed to uncover these sites. The information I needed simply was not available. I thus erroneously concluded that Los Alamos would have to learn how to make compartments work the hard way, by groping and testing out the code.

Now, some months later, we at Los Alamos have done just that, and we have compartments in production. But it was not easy. I am sure that the other sites that also have compartments in production, who we discovered through this Security Survey, went through the same travail, also alone, thinking they were the first. Hopefully, by utilizing the contacts listed in the Appendix, other sites will not have to proceed alone but may build on the experience others have already struggled to obtain.

First Security Survey –General Response

The Security Survey questionnaire is reproduced as Appendix A. It consisted of eleven questions about the site, its CRAY equipment, what security features were in use, and why. The raw tabulated results of the Survey comprise Appendix B. For the benefit of sites interested in contacting other sites that have experience with various UNICOS Secure Mode features, Appendix C tabulates the contact persons and telephone numbers for these sites.

It is of interest to discuss some of the statistics, although it must be understood that the way the questionnaire was distributed means that the sample is biased. Simply, those sites most interested in UNICOS security were most likely to return a response.

Forty-eight (48) sites responded. The number of machines represented by these sites is sixty-two (62); many of the responding sites have several machines. At the

time of the survey, there were 192 Cray sites, so the response was 25%. Although questionnaires were distributed to the CUG site folders, this was not done until fairly late in the CUG, and many sites were unaware that the survey was being taken. This poor procedure will be corrected in the future.

The responding sites are easily broken down into three categories, with the representation shown in Table I.

Table I. CUG Sites by Category

	Non-Secure Mode	Secure Mode	Totals
Government and Defense Contractors:	10 sites	20 sites	30 sites
Business and Industrial:	9 sites	3 sites	12 sites
University:	5 sites	1 site	6 sites
Totals:	24 sites	24 sites	48 sites

Who Runs Secure Mode?

Fully one-half of the respondent sites are running Secure Mode. Because of the bias of the sampling, this is unlikely to be representative of the proportion of all sites running Secure Mode, but it is nonetheless striking, because the Secure Mode sites responding to this survey represent about 12% of all sites. It is therefore not unlikely that perhaps 20-25% of all Cray sites are running Secure Mode. This will be investigated more fully on future surveys, when more attention will be paid to getting a less biased sampling.

That government and defense contractor sites should be interested in security is no surprise. This is borne out by the distribution of sites that are running Secure Mode UNICOS. Interestingly, of the sites running Secure Mode, I inferred that fifteen of the them have machines connected to the internet. Of these, twelve were government sites. Yet of the reasons given by the Secure Mode sites for running Secure Mode, only eleven cited "government requirement" as a primary reason for doing so. The reason given most (15 times) for running Secure Mode UNICOS was to have the "security logging" that comes with Secure Mode. While 13 sites felt that protecting the integrity and sanctity of users' data was reason for running Secure Mode, not a single site felt that "protecting the operating system" was a primary rationale for running Secure Mode.

Only nine of the Secure Mode sites run their machines as "system high", i.e., electrically isolated from external users. This extreme security measure is usually justified when classified or extremely sensitive business proprietary information is being handled on the machine. When machines are run system

high, it means that access to the machine is strictly limited to a chosen set of "trusted" users. That Secure Mode is being run on "system high" machines, despite the additional administrative burdens and costs implicit in running Secure Mode, indicates that those sites are extremely security conscious.

Revision Levels and Security

One of the questions we were interested in was whether the sites running Secure Mode are able to keep up with the latest UNICOS revisions and releases. At least those sites that are required to run Secure Mode are generally required to perform some sort of integration/validation testing before installing a new release. Depending upon the degree of testing required, installing even a new minor release can consume several man-months for several staff. This is true at Los Alamos, where we have a significant number of local mods that also need to be revalidated. Thus, one would expect a tendency amongst such sites to skip alternate releases, because of the extra overhead of revalidation. Table II shows the revision levels for the responding sites, for each reported machine.

Table II. Machine System Revision Levels

Release Level	5.1	6.0	6.1	7.0
Non-SecureMode	6	9	10	0
Secure Mode	13	8	12	1
Totals	19	17	22	1
Percentages	32%	29%	37%	2%
All CUG Sites	101	45	39	1
Percentages	54%	24%	21%	0%

The table also shows the revision levels reported, by site (not by machine), for all the CUG sites. The results were surprising, in that it appears that the Secure Mode sites are, if anything, slightly ahead of the general population. This suggests that the Secure Mode sites rather than putting off upgrading to the latest revision, may be somewhat more sensitive to making sure that they install the most recently available revision to ensure having the latest fixes to security holes. Although CRI announced at the Santa Fe CUG that they would be supporting previous revision levels up to a year after introducing a new major revision, a few sites have commented to me that critical bugfixes, including security bugfixes, have not always been pushed back into earlier

releases.

What Security Features are Being Used?

Only respondents actively running Secure Mode were asked to answer. In retrospect, this was a mistake, because it assumed that all sites interested in running securely would surely be running Secure Mode. Table III shows the responses.

Table III. Security Features in Use

	Sites	Machines
Only standard UNICOS protections (no Secure Mode)	24	26
Secure Mode (default level 0, default null compartment only)	15	18
Multiple Security Levels (or MINSLEVEL > 0)	4	7
Compartments	5	6
Kerberos (non-CRI)	2	5
SecureID™, SmartCard™, etc.*	7	10

*Includes four (4) non-Secure Mode sites

Half of the sites do not run Secure Mode; they rely primarily upon the basic protections (owner/group/world access rights) to protect the system from users and users from each other. The biggest surprise is that most of the sites running Secure Mode do not have the features (security levels and compartments) turned on, but they run with the default minimum security level (zero) and no compartments. In general, the sites that have turned on the more restrictive features have been government sites that have special need for security levels; about half of the machines that are run system high also fall into this category. Even when run system high, these machines are run with the additional protections afforded by the features.

A small number of sites have installed SecureID™ or similar features to protect access to their machines. A few sites have decided they cannot wait for CRI to release Kerberos as a feature (available in release 7.0), and have installed Kerberos on their own. It is of interest that one of these sites, with four machines (release levels 5.1, 6.0, 6.1 and 7.0), is CRI Eagan. SNLA (Sandia National Laboratories, Albuquerque) is to be commended for their substantial effort in bringing Kerberos into operation in a real supercomputer production environment.

Reasons for Running/Not Running Secure Mode

The responses are tabulated in Appendix B, questions 8 and 10. Some of the reasons why sites run Secure Mode have already been touched on above. The reasons why sites chose not to run Secure Mode are equally interesting. The most frequently cited reason (by 13 Sites) is that "Basic [UNICOS] protections are good enough for our needs." Six sites felt that Secure Mode was too hard to manage, and four sites felt that Secure Mode had too many outstanding problems, that it was too immature. Given that many sites <u>are</u> significantly concerned about security, these responses can be interpreted as a general perception that Secure Mode is harder to run and administer than vanilla UNICOS. Unfortunately, we who have been running Secure Mode have probably helped perpetuate this perception, by explaining loudly in public how much trouble we have encountered in getting Secure Mode features operational. While it is true that some Secure Mode features do make administration more complicated, Secure Mode (with no levels or compartments) by itself adds relatively little to the administrator's burden, while adding quite a bit to security by providing auditing.

Sources of Hole/Fix Information:

I personally have felt frustrated in getting the latest news of system security problems. I am aware of several sites that have discovered "holes" but refuse to communicate such information, even to CRI. These sites try to fix the "hole(s)" locally, protecting themselves, but leaving other sites vulnerable. Their explanation is that information of such vulnerabilities is so sensitive that it must be protected very carefully -- were such information to come into the possession of a hacker, they argue, the hacker could capture their machine. But this of course leaves all other sites unknowingly vulnerable to the same attack. Thus it is of interest to find out how CUG sites learn about such vulnerabilities. Nearly all of the vulnerabilities I am aware of have been discovered by users and reported to CRI, usually as an SPR. CRI then responds with a mod to fix the problem. Such mod-fixes are communicated by the same channels as for normal bugfixes, namely, field alerts and a monthly bulletin sent to the designated site contact.

Of the sites running Secure Mode, by far most depend upon their CRI Site Analyst for alerts about system security problems or "holes" (Table IV). Discovery of security holes by a site's own staff was the next most frequently cited source of such information. Sites overwhelmingly rely almost exclusively on CRI for fixes to such vulnerabilities, learning of the fixes either from their local CRI Analyst or from CRI Eagan communications. CRI thus carries a great deal of responsibility for such communication, both for alerting sites to the existence of problems (which it has learned of from customers) and for providing and alerting sites to fixes.

Table IV. Sources of Security Problem Information (Secure Mode sites only) (numbers of sites using the indicated source--many multiple responses)

Source of information	About Holes	About Fixes
Site CRI Analyst	11 Sites	16 Sites
A site's own Staff	8 Sites	4 Sites
CRI Eagan (field alert, etc.)	6 Sites	9 Sites
CERT/CIAC Internet alerts	6 Sites	2 Sites
Other Sites	2 Sites	none

It would be of interest to know how much time elapsed between the discovery and reporting of a security hole, and the dissemination of a fix, and how much time elapses between the dissemination of a fix and the installation of the fix (how long do sites run with publicized vulnerabilities?). Unfortunately, the way the survey question was posed precluded answering these questions. Responses varied from "prompt" to "abysmally slow." Clearly, much depends on how well a given site keeps up with the most recent release, and on how diligent the local CRI Analyst is at watching for field alerts and Service Bulletin notices of security problems. Until recently, most sites had little or no direct access to the CRI SPR and Field Alert databases (CRInform).

Is There Interest in SIC/MIG formation?

Perhaps the most surprising conclusion is suggested by the 81% favorable response to the question "Should CUG form a Security SIC?" Given the bias in the sample, one would expect that those sites already concerned about security , and therefore already running Secure Mode would vote overwhelmingly to create a SIC or MIG. But it was a revelation to see almost the same percentage of support for creation of a SIC/MIG by the sites not running Secure Mode.

This result, taken together with comments made to me by a number of sites, and the responses to question 10 (Reasons why a site is <u>not</u> running Secure Mode), indicates that the CUG sites <u>are</u>, in general, significantly concerned about the security of their systems. In the Security BOF, several sites admonished me for focusing mostly on Secure Mode features, while there is such concern in the broader community about trying to run Non-Secure Mode UNICOS securely. The newly formed Security MIG, accordingly, will seek to serve this broader interest.

Appendix A.

UNICOS SECURITY SURVEY

Security BOF

Santa Fe CUG -- Sept. 25, 1991

The goal of this survey is to collect information on which sites have experience running Secure Mode UNICOS to assist other sites in locating expertise and experience which may be helpful in their administration and configuration of Secure Mode UNICOS.

Sites which are "black" are encouraged to return a form -- the statistics would still be useful to the rest of the community -- but please clearly indicate "Black" at the top if you do not wish names and telephone numbers to be available to the CRAY UNICOS community (such names and numbers will be held in confidence).

Questions:

1. Site Name/Your name: _____/_____

Contact for Security Adm:_____/phone/emailaddr:_____

2. UNICOS Hardware (type & quantity, e.g., two YMP8/128): _____

3. At UNICOS Release Level (e.g., 6.1.4): _____

4. Running Secure Mode: YES NO

   If YES, How long (months)? _____

5. Are you:
   Running True Multi-Level:
   (i.e., real user levels .gt. zero) YES NO
   Running Compartments:
   (5.1 TFM only doesn't count!) YES NO

6. Is machine run "System-High"? (i.e., physically/ electrically isolated from world): YES NO

7. If un-isolated (e.g., on Internet), system is protected by (circle letter, all that apply):

   (a) Limited passthrough (e.g., secure gateways or routers)
   (b) Restricted (e.g., encrypted or secure) network
   (c) Kerberos or RSA encrypted authentication mechanisms
   (d) SecureID (tm), Smartcard (tm) or similar authentication mechanisms.
   (e) System is untrusted, we trust network logon/authentication
   (f) Only UNICOS protections

   (g) Other: _____

8. If running Secure Mode, reasons for doing so are (circle letter, all that apply):

   (a) For Security Logging Features.
   (b) Required by Gov't Order (DoD, DOE, Security Agency, etc.).
   (c) Needed to protect company's/customers'/users' proprietary info.
   (d) To protect operating system privileged functions and info.

   (e) Other:_____

9. If running Secure Mode, what is your primary source of information about security vulnerabilities(holes)/fixes (circle one letter of most appropriate in each left column and rank (1-5, 1=best) on promptness and usefulness (content) of the sources--rank all of them if you have had experience with them):

holes	fixes		prompt quick>>>late	useful good>>>>useless
(a)	(a)	Local Site CRI Analyst	1 2 3 4 5	1 2 3 4 5
(b)	(b)	CRI--vendor alerts/prob. rpts.	1 2 3 4 5	1 2 3 4 5
(c)	(c)	CERT/CIAC	1 2 3 4 5	1 2 3 4 5
(d)	(d)	Our own systems staff	1 2 3 4 5	1 2 3 4 5
(e)	(e)	External contractor/consultant	1 2 3 4 5	1 2 3 4 5
(f)	(f)	Other:_____	1 2 3 4 5	1 2 3 4 5

   Do you have suggestions as to how to improve communication of holes/fixes?

10. If not running Secure Mode, why not ? (circle letter, all that apply):

   (a) Performance hit too much to accept.
   (b) Administration of Secure Mode too complicated/costly.
   (c) UNICOS Secure Mode has too many problems, not mature enough.
   (d) Basic protections good enough for our needs/don't need in our environment

   (e) Other: _____

11. Should the CUG provide a clearinghouse/forum for UNICOS security issues by formation of a CUG SIG (Special Interest Group) with its own sessions/meetings?

   YES NO Comments, Other Problem areas?:

_____ _____

If not returned at Conference, please send filled out survey to:

Gary G. Christoph
Group C-8, Mailstop B-294
Los Alamos National Laboratory
Los Alamos, NM 87545

(505) 667-3709 ggc@lanl.gov

Appendix B: Santa Fe CUG Security Survey -- Accumulated Results

Question	Responses					
2. **Hardware Types and quantities**	XMP	15	YMP	27	Cray 2	8
	XMPEA	3	YMP-E	5		
	XMPSE	2				
Totals	XMP	20	YMP	32	Cray 2	8

3. **Release Level**	5.1	6.0	6.1	7.0
Non-SecureMode	6	9	10	0
Secure Mode	13	8	12	1
Totals	19	17	22	1

4. **Running Secure Mode** Yes = 24 Sites 36 Machines Avg. Experience = 14 mos.
No = 24 Sites 26 Machines

5. **Running Multiple Levels** Yes = 4 Sites 7 Machines

Running Compartments Yes = 5 Sites 6 Machines

6. **Running System High** Yes = 13 Sites 18 Machines

7. System is on Internet, **we rely upon the following protections:**

a)	Secure gateways or routers to limit passthrough:	18 Sites	24 Machines
	(Running Secure Mode connected to Internet thru secure gateway:		11 Machines)
b)	Restricted (encrypted or secure) network	2 Sites	2 Machines
c)	Kerberos or similar authentication mechanism:	2 Sites	5 Machines
d)	SecureID(TM), Smartcard(TM) or similar authentication:	7 Sites	10 Machines
e)	(Item was ambiguous--responses could not be generally interpreted)		
f)	only UNICOS protections:	13 Sites	16 Machines
	of these, running Secure Mode:	9 Sites	11 Machines
g)	Other: Local filter utility ("jeeves", ORNL)	1 Site	1 Machine

8. **Reasons for Running Secure Mode** (only Secure Mode sites responding; multiple reasons given by many respondents):

a)	For Security Logging Features:	15 Sites
b)	Required by Government or military	11 Sites
c)	Needed to protect company's/customers'/users' info	13 Sites
d)	To protect operating system	none
e)	Other: "To deter hackers"	1 Site
	"Login attempt limit"	1 Site
	"To get ACL's"	2 Sites

9. **Primary Source of information about security hole/fixes:** (only Secure Mode sites responding; multiple responses -- question was poorly structured)	Holes	Fixes
a) Local CRI Site-analyst:	11 Sites	16 Sites
b) CRI vendor alerts and problem reports:	6 Sites	9 Sites
c) CERT/CIAC	6 Sites	2 Sites
d) Our own systems staff	8 Sites	4 Sites
e) External contractor/consultant	no Sites	no Sites
f) Other: "Other sites"	2 Sites	no Sites

Suggestions for improved communication of holes/fixes:

"Cray don't (sic) seem to want to admit to there being any holes."

"[We need] field alerts sent to site delegates (regular mail)"

"CRI should disseminate info to site Security/Sysadmins as soon as discovered/known. Could always email distribution (similar to CERT) list rather than paper notification. Some sites need this because they cannot rely upon a site analyst."

"Improve working of the CERT/First System; get more vendors involved"

"CRInform"

"No bugs have been pointed out. We do receive critical mods immediately, though." (This comment from a Black site!)

10. **Reasons why NOT running Secure Mode** (Secure Mode sites not responding; multiple responses from many sites):

a) Performance hit too great:	no Sites
b) Administration of Secure Mode too complex/costly:	6 Sites
c) UNICOS Secure Mode has too many problems, too immature:	4 Sites
d) Basic protections are good enough for our needs:	13 Sites
e) Other: "Too restrictive for "real" UNIX users	2 Sites
"Incompatible with applications we run"	1 Site
"We extensively use NFS on several machines"	1 Site

11. **Should CUG form a Security SIG/MIG:**	YES	NO	No Opinion
Secure Mode sites:	19	4	1
Non-Secure Mode sites:	11	3	10
Totals	30	7	11

Appendix C. Secure Mode Sites from the 1991 Santa Fe CUG Security Survey

Site ID (Region)	Release Level	Hardware	Secure Mode Features in use	Contact Name	Contact Phone/email
CEA-CEL (Europe)	6.0 6.0	XMP28 YMP8/8128	(12 mos.) (12 mos.)	Claude Lecoeuvre	(33-1) 45 95 61 85 (France)
CRI (USA)	5.1 6.0 6.1 7.0	C-2/4256 XMP48 XMP48 YMP2/32	Kerberos Kerberos Kerberos Kerberos		
DE-DEBIS (Europe)	5.1.11	YMP4/216	comparts (15 mos.)	Mr. Mueller	(49 711) 17-57654 (Germany)
DTRC (USA)	5.1.11	XMP216	(6 mos.)	Julie Wessel	(301) 762-2482 wessel@oasys.dt.navy.mil
ECMWF (Europe)	5.1	YMP8/64	(15 mos.)	Neil Storer	(44 734) 499353 neil.storer@ecmwf.co.uk
EGLIN (USA)	5.1.11	YMP8/2128	(12 mos.)	Ben McKinnon	(904) 882-3736 mckinnon@uv4.eglin.af.mil
EXXONRE (USA)	5.1.12	XMP116SE	(24 mos.)	Jill O'Neil	(908) 730-3108
FNOC (USA)	6.1	YMP-2E	(0 mos.)	Jim Powers	(408) 647-4378
FRAM (Europe)	6.0.13	YMP2/116	(6 mos.)	C. LaPlace	Internet: 47.96.13.07 (France)
KFA (Europe)	6.1.4 6.1.4	XMP416 YMP8/832	(18 mos.) (18 mos.)	Mr. Sichelschmidt	(49) 2461 61 6351 (Germany)
LANL (USA)	6.0.11 6.0.11 6.0.11	XMP48 YMP8/264 YMP8/264	multilevels(8 mos.) multilevels(10 mos.) multilevels(8 mos.)	Gary Christoph	(505) 667-3709 ggc@lanl.gov
LLNL (USA)	6.1.4	XMP48	multilevels soon (testing comparts)(12 mos.)	Chuck Athey	(510)422-7211 athey@ocfmail.ocf.gov
NASA-JSC (USA)	5.1.9	XMP464EA	comparts(24 mos.)	Jim Engel	(713) 483-5894
NAVO (USA)	6.1.4 6.1.4 6.1.4	YMP8/8128 YMP2E XMPSE	(7 mos.) (7 mos.) (7 mos.)	Frank Lovato	(601) 688-5091 lovato@pop.navo.navy.mil

Site ID (Region)	Release Level	Hardware	Secure Mode Features in use	Contact Name	Contact Phone/email
NTB (USA)	5.1 6.1	C2-2S/128 C2-4D/512	plan to SecureMode plan to SecureMode	Raymond Fleisleber	(719) 380-2281
ONERA (Europe)	5.1.12	YMP8/4128	(20 mos.)	J. P. Peltier	(33) 1-4657 11 60 x2094 (France)
ORNL (USA)	6.1.4	XMP14	(24 mos.)	Buddy Bland	aib@ornl.gov
SERC (Europe)	5.1.12	XMP416	(12 mos.)	G. T. Folkes	gtf@ib.rl.ac.uk (Great Britain)
SNLA (USA)	6.1.4	YMP8/864	multilevels(17 mos.) Kerberos v.4	W.Vandevender	(505) 844-4802 whvande@sandia.gov
SNLL (USA)	5.1.12 6.0beta	YMP8/264 XMP28	multilevels(30 mos.)	Diane Gomes	(415) 294-1479
WSRC (USA)	6.1.4	XMP132EA	(33 mos.)	James C. Jensen	(803) 725-5147

Notes:

This Table does not contain any "Black" sites, nor sites which requested anonymity.

CRI machines have been included to indicate that several machines at Eagan, MN, are actively running Secure Mode, at different release levels. The appropriate contact points for CRI are the local site analyst and/or CRI Tech Support.

Explanation of column entries: All data was current as of September 1991. Entries under "**Secure Mode Features**" are: (**months**): the number of months that Secure Mode (security level=0, compartments=0) have been in production. If the number of months is preceded by **multilevels**, it means that multiple Secure Mode security levels, or a non-zero minimum level, has been in production for that number of months; if preceded by **comparts**, it means that multiple Secure Mode compartments have been in use for that number of months. **Kerberos** means that Kerberos authentication has been locally implemented on the indicated Cray machines at that site.