

# **Secure Unix Workstations for Distributed Computing**

James A. Rome  
Oak Ridge National Laboratory  
jar@ornl.gov

Presented to  
ESCC-DCCC Joint Meeting  
CEBAF, Newport News, VA  
September 29, 1995

## ***We all know security is important . . .***

---

As I write this,

- ▣▣▣▣▶ A Russian broke into Citicorp's computers and illegally transferred \$8 million.
- ▣▣▣▣▶ The Netscape SSL 40-bit code that was supposed to be used for secure VISA and MasterCard transactions was broken by a French student in a week. California students broke the seed for the random key in a minute.
- ▣▣▣▣▶ Over \$40 trillion is transferred electronically each year. This will grow rapidly when credit card transactions on the Internet become a reality.
- ▣▣▣▣▶ Our electric grid, air space, financial markets, phone system, . . . are all controlled by large computer networks.
- ▣▣▣▣▶ We are embarking on large distributed collaborative research efforts.

**Are we secure enough?**

## ***Security can be applied to three main areas***

---

- ▣▣▣▣▶ The network
  - ▶ Cryptography and inter-realm authentication
  - ▶ ESNNet is using DCE + Kerberos 5
- ▣▣▣▣▶ The network/LAN interface
  - ▶ Firewalls
  - ▶ Proper router programming

*Most computer attacks come from within rather than without . . .*

- ▣▣▣▣▶ The computer nodes
  - ▶ Hidden password files
  - ▶ Discretionary access control (DAC)  
File access by owner, group, world
  - ▶ Audit trails
  - ▶ Security patches

These are all “band-aids” to patch up a system with many security vulnerabilities.

**Compartmented Mode Workstations (CMW) provide a significantly higher level of security.**

## ***Ideal venues for a CMW-based system***

---

### **The DOE-OSS Fileroom Project**

- ▣▣▣▶ Millions of pages of documents need to be searched and retrieved electronically.
- ▣▣▣▶ Some of the data are classified.
  - ▶ Reclassification is required.
- ▣▣▣▶ Eventually, the non-sensitive data may be available to the public.

### **Tech Center 2020**

- ▣▣▣▶ Lockheed-Martin “incubator” company for high-tech startup companies.
- ▣▣▣▶ One high-end workstation used by different companies.
- ▣▣▣▶ Proprietary information protection must be guaranteed.

### **“Big science” database**

- ▣▣▣▶ New data are stored in the same table as old data and are held confidential until papers are published.
- ▣▣▣▶ Data can be retracted.

## Summary of “Orange Book” security features

Criterion	C1	C2	B1	CMW	B2	B3	A1
Identification and Authentication (IAA)	Blue	Dark Blue	Light Pink	Red	Light Pink	Magenta	Green
Discretionary Access Control (DAC)	Blue	Dark Blue	Light Pink	Red	Light Pink	Magenta	Green
System Architecture (Least Privilege)	Blue	Dark Blue	Light Pink	Red	Light Pink	Magenta	Green
Security Testing	Blue	Dark Blue	Light Pink	Red	Light Pink	Magenta	Green
Auditing	White	Dark Blue	Light Pink	Red	Light Pink	Magenta	Green
Object Reuse	White	Dark Blue	Light Pink	Red	Light Pink	Magenta	Green
Labeling	White	White	Light Pink	Red	Light Pink	Magenta	Green
Label Integrity and Label Export	White	White	Light Pink	Red	Light Pink	Magenta	Green
Multilevel Export	White	White	Light Pink	Red	Light Pink	Magenta	Green
Single-Level Export	White	White	Light Pink	Red	Light Pink	Magenta	Green
Printout Labeling	White	White	Light Pink	Red	Light Pink	Magenta	Green
Mandatory Access Control (MAC)	White	White	Light Pink	Red	Light Pink	Magenta	Green
Sensitivity Labels	White	White	White	Red	Light Pink	Magenta	Green
Device Labeling	White	White	White	Red	Light Pink	Magenta	Green
Trusted Path	White	White	White	Red	Light Pink	Magenta	Green
Covert Channel Analysis	White	White	White	White	Light Pink	Magenta	Green
Trusted Facility Management	White	White	White	Red	Light Pink	Magenta	Green
Configuration Management	White	White	White	Red	Light Pink	Magenta	Green
Trusted Recovery	White	White	White	Red	White	Magenta	Green
Trusted Distribution	White	White	White	Red	White	White	Green
Information Labels	White	White	White	Red	White	White	White
Authorizations	White	White	White	Red	White	White	White

## ***Why not start with a more secure system?***

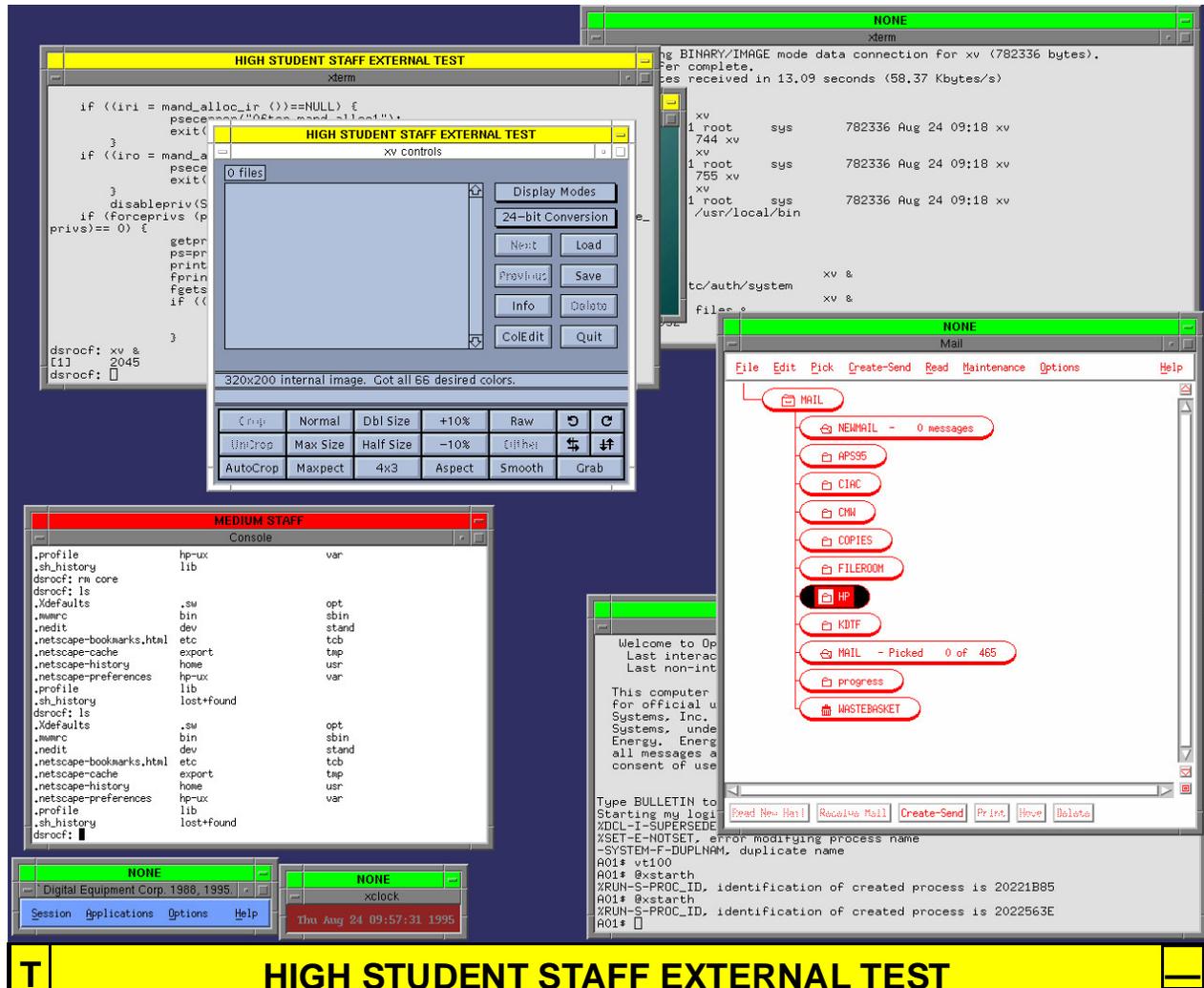
---

The compartmented mode workstation (CMW) Unix systems are now ready for deployment.

- ▣▶ Developed by DoD and NSA for multilevel classified work.
- ▣▶ Rated *B1* in the NSA Orange Book with many features of the higher *B2* and *A* levels. This is significantly higher than the *C1* or *C2* rating of most conventional systems.
- ▣▶ There are CMW versions for Sun, IBM, HP, DEC, Data General, SCO (Intel) platforms.
- ▣▶ The major database (Oracle, Informix, Sybase, Ingress) vendors have multilevel-secure versions of their products.

**These systems have now emerged from being “bleeding edge” technology to being useful technology.**

# What does a CMW system look like?



*Hewlett Packard HP-UX 10.09 screen*

- Every window is labeled
- Trusted stripe (on bottom) can't be occluded
- Read-down/write-up policy enforced by window manager

## ***Aside: The previous screen shot was secure***

---

The program *xv* worked perfectly and captured a shot of the screen. But,

▣▣▣▣▶ All windows were black holes.

The CMW Motif Window Manager is much more protective than on a usual Unix system where the screen can be read relatively easily by determined hackers.

To capture the screen, as ISSO I had to

▣▣▣▣▶ Modify a file that gives programs privileges. I gave *xv* the *WindowManager* privilege.

▣▣▣▣▶ I rebuilt the database that checks program privileges using the above file.

▣▣▣▣▶ I set *xv* to have a *System High* security label.

Thus, I could only run it from a *System High* session. Otherwise, the screen shot would declassify information. The resulting TIFF file was automatically labeled *System High*.

## ***What makes a CMW system more secure?***

---

In addition to the usual Unix features, CMW systems add

▣▣▣▶ **Mandatory access control:**

All files and subjects on the system are labeled with a classification and one or more compartments or “need to know” categories.

- ▶ The file system is different. The inodes contain the labels.
- ▶ Access to any system resource is automatically controlled according to the subject’s clearance, and the program’s privileges.

▣▣▣▶ **Root privileges are split up:**

On conventional Unix system programs run with a *uid* of 0 (root) which gives them all privileges. On a CMW system, the operating system routines have been rewritten.

- ▶ Programs do not run at *uid* 0.
- ▶ They only assume privileges when needed and drop them when no longer needed. This is called the *principle of least privilege*.

## ***CMW security features (continued)***

---

- ▣▣▣▣ **System administration is split up into roles:**  
Administrator, Information System Security Officer (ISSO), Operator, and Network Security Officer (NSO).
- ▣▣▣▣ **Two man rule:**  
It takes two people to set up a user account, the Administrator and the ISSO.
- ▣▣▣▣ **Enhanced audit trail:**  
Every action of individual users, groups, or combinations thereof can be audited.
  - File access and modification
  - Success or failure of system operations
  - Usage of system resources
- ▣▣▣▣ **Sysadmin tools:**  
Security-sensitive system administration tools can only be run from the console.
- ▣▣▣▣ **Communicates with selected hosts only:**  
Connections are refused unless the other host is listed in the *M6RHDB* database.
- ▣▣▣▣ **External non-CMW hosts enter at one label.**

## *Is it really secure?*

---

- ▣▶ Certified by the National Computer Security Center.
- ▣▶ Unaffected by a Satan attack.

But, the administrator must carefully evaluate new software and hardware to maintain this level of security. Some issues to be considered are:

- ▣▶ What was the “certified configuration?”
- ▣▶ Does commercial off-the-shelf software (COTS) run without special privileges? At any security level? By any user?
  - ▶ Used to be a problem. Now COTS usually works “out of the box.”
- ▣▶ How do you interface with other CMW and non-CMW computers?
- ▣▶ What privileges do you give to the average user?

## Example of a trusted program

---

```
/* This trusted program changes the */
/* level of a user coming from a */
/* unlabeled host (if authorized) */

/* gcc flevel.c -o flevel -lsecurity */

#include <prot.h>
#include <stdio.h>
#include <sys/types.h>
#include <sys/secdefines.h>
#include <sys/security.h>
#include <mandatory.h>
#include <unistd.h>

main (int argc, char **argv)
{
    mand_ir_t *iri, *iro;
    char string1[200];
    char *ps;
    privvec_t eprivs;
/* Initialize security parameters and allocate security arrays */
    set_auth_parameters (argc, argv);
    initprivs();

    if ((iri = mand_alloc_ir ())==NULL) {
        exit(1);
    }
    if ((iro = mand_alloc_ir ())==NULL) {
        exit(1);
    }
/* Make sure auditing is on !! */
    disablepriv(SEC_SUSPEND_AUDIT);
/* Turn on only privileges needed to allow user to change levels */
    if (forceprivs (privvec(SEC_CHSUBJSL,
        SEC_CVTLABEL,-1), save_privs)== 0) {

        /* Get user's desired level */
        fprintf (stderr,
            "Enter desired sensitivity label: ");
        fgets (string1, 199, stdin);
/* Convert from named level to internal representation */
        if ((iri = mand_er_to_ir (string1)) == NULL) {
            exit(1);
        }
/* Set user's desired level. Will fail if not dominated by user's clearance */
        if (setlabel (iri)) {
            fprintf (stderr, "Not authorized\n");
            psecerror("Error");
        }
        else {
/* Check and be sure it worked */
            getlabel (iro);
            fprintf (stderr,
                "New sensitivity level for process: %s\n"
                mand_ir_to_er (iro));
        }
/* Restore privileges user had on entrance */
        (void)seteffprivs(save_privs, NULL);
/* Free memory */
        mand_free_ir (iri);
        mand_free_ir (iro);
/* Exec a shell for user with new level */
        execl ("/bin/ksh", "-", NULL);
    }
/* or tell user why it failed... */
    else {
        psecerror("Forceprivs failed");
    }
}
```

## *Advantages of CMW systems*

---

In addition to the resistance to attack CMW systems offer other advantages.

- ▣▶ Compartments automatically protect proprietary information with no additional programming, and can't be subverted.
  - ▶ *Problem:* The employee evaluation program requires that the fitness reports for every employee are in one directory, but they should only be accessible to each employee's supervisory chain.  
*Solution:* Label each employee's report with the supervisor's compartment. The supervisor's boss is a member of all his sub-supervisors compartments.
  - ▶ *Problem:* Protect proprietary data from an industrial partner in a CRADA, but be able to look at the data from several partners at once.  
*Solution:* Put each partner's data in a separate compartment
  - ▶ *Example:* Tech 2020 (startup incubator) uses CMW on the shared computer.

## *Advantages of CMW systems (cont.)*

---

- ▣▶ Enhanced auditing allows more fine-grained actions.
  - ▶ Be able to tell who has accessed a table on a row-by-row basis to allow for data retraction. (Trusted database)
  - ▶ Create “citation” index to evaluate worth of data. (Trusted database)
  - ▶ Track activities of public to be able to prove that they did or did not find something on the computer.
- ▣▶ More flexible database administration.
  - ▶ Labels apply to rows, not just to tables.
    - ◆ Two people making the same query of the same table get different answers according to their clearances.
  - ▶ Compartments eliminate need for separate query tools for each group to segregate data.
  - ▶ Classification levels allow users to select the reliability level of data. All data will be seen at a high classification. Only old data at a low level.

## *Networking issues*

---

CMW systems were designed to operate in secure network environments.

- ▣▣▣▣▶ *rlogin* may or may not require a password. If so, it is sent in clear text.
- ▣▣▣▣▶ Multilevel hosts exchange labeled packets.
  - ▶ Many protocols: CIPSO, RIPSO, MAX6, TSIX,...
  - ▶ Applied at both network and application level.
  - ▶ Issue: how to translate levels from site to site. Manufacturer's group (TSIG) made up standards, but still "Tower of Babel."  
<ftp://ftp.sterling.com/tsig/tsig.html>
- ▣▣▣▣▶ NFS extended to labeled file systems. Another CMW host will automatically apply all MAC and DAC access restrictions to an imported volume.
- ▣▣▣▣▶ Sun uses Yellow Pages (NIS) to administer a network of CMW machines as a single entity. (It is even accredited as a distributed system.)

## *Networking issues (continued)*

---

CMW platforms do not yet support

- ▣▣▣▣▶ AFS
- ▣▣▣▣▶ DCE
- ▣▣▣▣▶ Kerberos
- ▣▣▣▣▶ Smart Cards

It would violate the system security to replace the usual daemons with the Kerberized versions.

As these systems become more widely used in the commercial world, enhanced network security features will surely be added. (Sun has a CMW http daemon.)

For now, we hope that these systems will be able to connect to ESNet.

## Conclusions

---

- ▣▶ Today's CMW systems are usable
  - ▶ COTS programs usually work without privileges.
  - ▶ Enhanced tools make the task of system administration reasonable. (But, it is still harder to administer these systems than conventional Unix . . .)
- ▣▶ These systems are much more secure than conventional systems. This level of security is needed.
- ▣▶ It is time to start using these systems for security-critical tasks.
  - ▶ Kerberos server
  - ▶ Time card server
  - ▶ Medical data
- ▣▶ CMW workstations make the most secure form of server for databases.
- ▣▶ Enhanced networking features that work on CMW platforms are still required.