UCRL-JC—111078

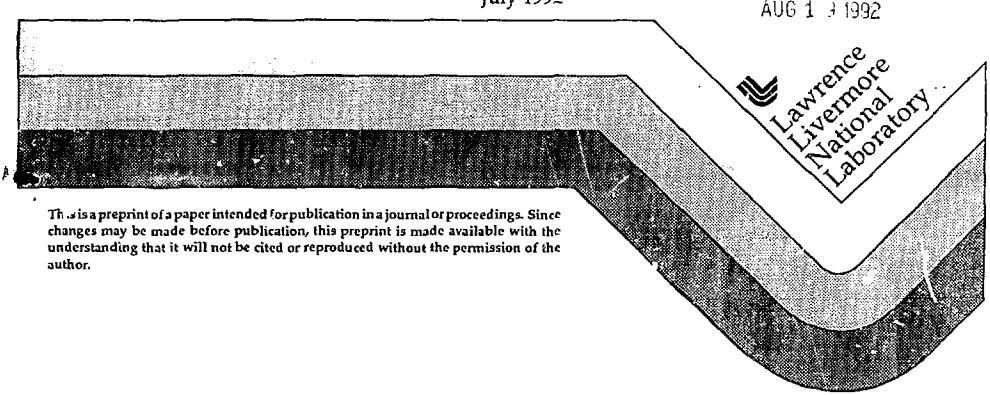
DE92 019536

Access Control Issues and Solutions for Large Sites

Fred E. Warren

This paper was prepared for submittal to the
Institute of Nuclear Materials Management
Orlando, Florida
July 19-22, 1992

July 1992



DISCLAIMER

Access Control Issues and Solutions for Large Sites *

Fred E. Warren
Safeguards and Security Engineering and Computation Division
Lawrence Livermore National Laboratory
Livermore, CA 94595

Abstract

The Lawrence Livermore National Laboratory (LLNL) operates an automated access control system consisting of more than 100 portals. We have gained considerable practical experience in the issues involved in operating this large system, and have identified the central issues to include system reliability, the large user population, the need for central control, constant change, high visibility and the budget. This paper outlines these issues and draws from our experience to discuss some fruitful ways of addressing them.

Introduction

In this paper we will consider some of the important issues associated with large entry control systems and what solutions have proven useful at the Lawrence Livermore National Laboratory. LLNL currently operates the Argus integrated security system that includes over 100 entry control portals. With a working population of more than 10,000 people and more than 20,000 entries through the portals each day, we have faced and solved many issues that present themselves to a large site where entry control is implemented on a large scale. As one might conclude, many of the issues arise from the sheer size of the system and represent a scaling up of issues that face all entry control systems. Other issues are unique to a large entry control system and a large user population. We will discuss both types of issues.

Reliability

The issue of reliability in an automated entry control system is very important in all installations, but becomes paramount in large installations. It also becomes more difficult to achieve as the size of the system and the number of components increase. At a large highly automated site such as LLNL the system is central to our ability to operate. In this environment it becomes impossible to duplicate completely the functions of the automated system with Security Inspectors (SI) or other manual means. The system is simply too large and there are not enough people available. The various programs underway at LLNL suffer extreme impacts if access to their facilities becomes unavailable. It inconveniences their workers, keeps visitors from their destinations and causes embarrassing incidents.

System failures increase non-

linearly with the number of pieces of equipment in the system and are associated with equipment wear, environmental damage, and subtle interaction between the components.

At LLNL we have approached these challenges in a variety of ways. With a large system it is critical that an in-house maintenance staff be available around the clock. We have a full time crew of highly skilled portal hardware maintenance technicians. To support them we maintain a large spares inventory, and a set of diagnostic tools. We additionally have an ongoing program of reliability engineering to improve our equipment. We also have staff who perform a similar function for the computer system and its associated software. We have found this computer system support very necessary to the successful operation of our large access control system.

Besides the maintenance of our equipment, we have found it vital to provide administrative methods for controlling the software installed on the system. We have established a System Problem Report (SPR) database to track and report on all problems or enhancements relating to the Argus system. This allows us to ensure that nothing falls through the cracks and that problems get addressed in an orderly way. We have also established testing procedures to ensure that the software installed on our system operates correctly before it is put into production.

The final point in automated entry control system reliability is actually the first point. The design of the system makes a major impact on its reliability. The Argus system is immune from total system failure. The portals continue to operate stand alone if there is a communications or power failure. The central computer is fully redundant and the software that controls the system is designed to be reliable and easy to maintain.

Large Population

Of course, a large user population brings with it many issues to resolve. Any problems with the system will have an impact on many people. This results in an increase in the need to handle "special cases" in an organized way. A large population requires more locations to serve people's needs and this results in such things as having multiple badge offices. The large population also forces activities that could be handled administratively with low volume to be done by automated methods.

At LLNL, our large user population has forced us to greater degrees of compartmentation. We have many "islands of security" spread across our site. This has resulted in the need to administer these security areas more easily. We have implemented the ability to assign people to groups of areas. We have also found the need to maintain increasingly complete audit trails and to provide software tools to do data reduction and reporting from the mass of data that the system keeps.

With a large population, there is more of a requirement to consider people who have problems with the system. It becomes harder to do a

"quick work-around" of the system by having SI or administrative intervention. This places a larger burden on the badge office staff and console operators to resolve problems for people. We also find a greater need to take people's special requirements, such as disabilities, in to account as there are more such people trying to use the system.

The computer system itself must also be properly sized to support the large population. Nothing frustrates a user population more than having to wait for the computer. Here the Argus system design helps by doing most of the access processing in the portal itself and filtering out unnecessary detail in the messages displayed to the console operators.

Central Control

Several requirements drive the organization of access control systems towards a centralized approach. One of the most important is the requirement to be able to stop the use of a badge immediately if a problem is detected. This stop must be transmitted to all access control points in a minimum time. Related to this requirement is the issue of lost badges. When a person loses a badge, further use of the badge must be prevented quickly.

At a large site, central control is important to avoid communication failures in potentially critical situations. An example of this is the dispatch of SI's to respond to an access control incident.

We have found several things that help to provide this needed central control. The Argus system provides a console that integrates all aspects of our access control and intrusion detection systems and provides for clear presentation of the important data to the console operators. The operators, in turn, provide the central clearing house for coordinating actions as needed. We have also found that having designated points of contact and clear lines of responsibility for each situation improves the number of successful responses. Documented procedures also play a key role in ensuring that information is accurately transmitted to the people who need it.

Change

At a large site like LLNL, the access control system is constantly undergoing changes. New portals are being activated, old portals are being deactivated, program requirements are changing, and DOE requirements are changing. It would be impossible to carry out the access control mission at LLNL with a static system. It is therefore critical that our system be able to change and adapt.

The Argus system design comes to our aid in this context as well as others. The system supports modular expansion and it is easy to add, subtract, or modify portals without disturbing the normal operation of the production system. We have documented procedures for these modifications and appropriate computer software to help make it easy. We also have in-house system development staff that allows us to

modify or enhance the system to conform to changing requirements. Current examples are implementing biometrics in the portal and adapting the system to use the new DOE common badge.

Visibility

When an access control system becomes as large and pervasive as it has at LLNL it has an impact on many people. Obtaining a badge to enter the site is often the first impression a visitor has of our facility. The second impression is often passing through an access control portal to get to his/her destination. Since the purpose of an access control system is to control access, it can become the focus of user frustrations should problems arise.

A large access control system represents a significant expense to the organization and is justified by its role in the protection of critical assets. Both the consumption of budget and the potential consequences of a access control failure make automated access control systems very visible to senior site management.

Our experience has led to the initiation of several activities to help manage the visibility issue. We have initiated regular meetings with our major users, for instance the badge offices, to facilitate communication and prevent problems from escalating. We have Safeguards and Security liaisons assigned to each of the major programs at the Laboratory to facilitate communication and the timely resolution of problems. We have also established an experienced engineering manager to supervise all the technical Safeguards and Security systems with a direct reporting relationship to the Director of Safeguards and Security. This has provided a management structure able to supervise the rapidly evolving and highly technical aspects of our Safeguards and Security organization.

The SPR system also performs an important function in managing the visibility of our system. It provides a formal way for our users to register problems they have found in the system and be able to track progress on their resolution.

Budget

Large automated access control systems are expensive. They are expensive to implement and they are expensive to operate. Often these systems are implemented by obtaining a Congressional line item. This approach provides the large initial funding required to install the system, but does not address the issue of ongoing maintenance and operation.

LLNL had the advantage of developing the Argus system in-house using line item funding. The initial approach was to develop the system, install it and then disband the development team. As we gained further understanding of the requirements of operating a large, very sophisticated access control system we modified this approach. We discovered that we needed a portion of the development staff to participate in the ongoing maintenance and enhancement of the system. Funding for this type of staff and providing them with challenging work is a very

important part of operating the Argus system at LLNL. We have also found, however, that other sites can operate the Argus system but it is better if our central team of experienced developers implement enhancements to the system. Unless a site is willing to invest heavily in expensive development staff and support them over the long haul, it is better to arrange for the system vendor to implement enhancements.

Obtaining funding to support ongoing system operation is a critical element to a successful access control system. The costs involved include purchase of equipment spares, new hardware and software required to support growth, and the labor cost for support personnel and their management. Depending on the size of the system, this can amount to a large piece of the operating organization's budget. Inadequate estimation of these costs can result in the inability to operate the system effectively and this can produce very serious results. Since budgets tend to be based on past estimates and are often cut, recovering from a poor guess about operating costs can be very difficult.

At our site the programs that require access control are responsible for paying for the purchase of the access control portals in their area and any associated central equipment required to support them. Over the last year we have also identified the requirement to include in these newpurchases funding to support the additional spares inventory required to support the new portals.

It is our experience at LLNL that we easily offset the operating cost of our automated access control system with savings in SI costs. We estimate that it would require ten times the current operating costs of our Argus system to duplicate the same level of access control capabilities using SI staff.

Conclusion

We hope that these experiences at LLNL with a large automated access control system will prove useful to others with similar systems. These systems provide many benefits to the sites that have them, but they also present many challenges to overcome. Perhaps by sharing our experiences we can all make better use of these marvelous products of the Computer Age.

---

* 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

Access Control Issues and Solutions for Large Sites

Presented to
the INMM Annual Meeting
July 22, 1992

Fred E. Warren

Introduction

LLNL Has a Large Access Control System

- 100 Portals
- 10,000 People
- 20,000 Entries

Three Years of Operational Experience

Issues

- Size of the system
- Size of the population

The Issue of Reliability

Critical in Large Systems

Harder to Achieve
- More components

Hard to Duplicate Functionality
- Not enough people

Failures Impact Programs

Solutions for Reliability

In-House Portal Maintenance Technicians

- 24 Hour coverage
- Spares inventory
- Diagnostic tools

Reliability Engineering

Computer System Support Technicians

- Computer hardware and networks
- Computer software

Solutions for Reliability

Administrative Methods

- SPR database
- Software testing procedures

System Design

- Argus access control system designed for reliability
- Booths operate stand alone
- Redundant central computers
- No single point of failure
- Software uses object oriented design in Ada

The Issue of Large Population

System Problems Impact Many People
- Need to handle "special cases"

More Locations Needed

Large Volume of Administrative Activity

More Compartmentation Required

More People - More Problems

Solutions for a Large Population

Special Cases Handling

Multiple Badge Offices

Areas of Areas of Compartmentation
- Software makes it easy

Better Audit Trails

Reliance on Badge Office and Console for Problem Resolutions

Provisions for Disabilities

Solutions for a Large Population

Automation Helps

- Automated badge processing

- Automated connection between badging and access control

- Automated support for administrative tasks
  - "late letters"

- Rapid response from fast computers

- Distributed system design
  - Portals operate with local data
  - Little communications overhead

The Issue of Central Control

The Requirement to Rapidly Stop a Badge

Communications Between Security Personnel

Centralized Reporting

LAWRENCE LIVERMORE NATIONAL LABORATORY

Solutions for Central Control

Central Computer - Distributed Portals

- One place to stop badges - instantly transmitted to portals
- Uniform information about clearances and accesses

Central Command Console

- Coordination of all incident responses
- Facilitates communications
- Only important information presented
- Based on maps - easy to understand

Administrative Control

- Clear lines of responsibility
- Documented procedures

The Issue of Change

Change is Constant

- New portals
- Old portals
- Program Changes
- DOE Changes

Adaptability is Critical to the Mission

Solutions for Change

Argus System Design

- Modular expansion
- Online modification of configuration
- Software support

In-house Development Staff

- Possible to change system as needed
- Biometrics
- DOE Common Badge

The Issue of Visibility

A Large Access Control System Has a Large Impact

Major Source of First Impressions

Major Expense to the Organization

Failures in Access Control are Very Visible

Solutions for Visibility

Regular Meetings with User Groups

Liaisons to Programs

Senior Technical Manager in Safeguards and Security

Database to Track Problems for Users

The Issue of Budget

Large Access Control Systems are Expensive

- to implement
- to operate

Operating Costs are Hard to Estimate Up Front

On-Going Development Costs

Who Pays for Upgrades and Expansions?

Solutions for Some Budget Issues

In-House Development Team - a Tradeoff

Operating Cost Estimates

- Equipment spares
- New hardware and software
- Support personnel
- Important to get right

He Who Uses Pays

- Programs who need the security pay the tab
- Spares must be factored in

We Save 10 Times the Operating Costs

Expensive but Worth It