LA-UR- 01-3334

Approved for public release;
distribution is unlimited.

c.1

Title:

INFORMATION BARRIERS AND AUTHENTICATION

Author(s):

D. W. MacArthur and J. K. Wolford, Jr.

Submitted to:

42nd Annual INMM Meeting
Indian Wells, CA USA
July 15-19, 2001
(FULL PAPER)

Los Alamos
NATIONAL LABORATORY

LA-UR-01-3334

INFORMATION BARRIERS AND AUTHENTICATION

Duncan W. MacArthur
Los Alamos National Laboratory, MS E-540
Los Alamos, NM 87545 USA
505/667-8943

James K. Wolford Jr.
Lawrence Livermore National Laboratory
P.O. Box 808
Livermore, CA 94550 USA
925/422-7236

Presented at the
Institute of Nuclear Material Management
42nd Annual Meeting
Indian Wells, California
July 15-19, 2001

INFORMATION BARRIERS AND AUTHENTICATION

Duncan W. MacArthur
Los Alamos National Laboratory, MS E-540
Los Alamos, NM 87545 USA
505/667-8943

James K. Wolford Jr.
Lawrence Livermore National Laboratory
P.O. Box 808
Livermore, CA 94550 USA
925/422-7236

ABSTRACT

Acceptance of nuclear materials into a monitoring regime is complicated if the materials are in classified shapes or have classified composition. An attribute measurement system with an information barrier can be employed to generate an unclassified display from classified measurements. This information barrier must meet two criteria: 1) classified information cannot be released to the monitoring party, and 2) the monitoring party must be convinced that the unclassified output accurately represents the classified input. Criterion 1 is critical to the host country to protect the classified information. Criterion 2 is critical to the monitoring party and is often termed the "authentication problem." Thus, the necessity for authentication of a measurement system with an information barrier stems directly from the description of a useful information barrier. Authentication issues must be continually addressed during the entire development lifecycle of the measurement system as opposed to being applied only after the system is built.

ATTRIBUTE MEASUREMENT SYSTEMS

Verification measurements on declared quantities of unclassified plutonium are relatively straightforward. Standard neutron and gamma measurement techniques can be used to verify the mass and isotopic ratio of the plutonium. However, these measurements are very intrusive and will contain classified information if classified items are being measured. Thus for measurements of classified items, an information barrier (IB) must be added to the system to conceal the classified information. The stated intent of an IB is to allow meaningful radiation measurements to be performed on potentially classified objects without display of any classified data. To perform this task successfully, the IB must satisfy two basic constraints:

1) First and foremost, the IB should prevent the release of classified information.
2) However, in conjunction with the first constraint, the IB should also allow the inspecting party to reach credible and independent conclusions concerning the objects being monitored.

Information barriers are discussed more detail in Refs {1} through {3}.

An attribute measurement system with information barrier is used to verify that an item possesses certain attributes without disclosing classified information. Very accurate neutron and gamma measurement systems are used to measure the potentially classified characteristics of an item. These potentially classified measured values are compared with mutually agreed unclassified thresholds to generate a series of binary outputs indicating agreement or disagreement with the agreed thresholds. These binary results pass through an output data barrier and are displayed as a series of green (agreement) or red (disagreement) indicator lights. The output data barrier ensures that no classified information can be passed to the display, and that data flows only from inside the enclosure to the outside. Attribute verification systems are described in more detail in Refs. {4} and {5}.

A simple schematic realization of this type of attribute measurement system is shown in Fig. 1. All potentially classified information is contained within a protective shell, and only unclassified results are displayed outside the shell. In this case, the shell characteristics are more important than the characteristics of the internal elements in determining the protection afforded by the complete system.

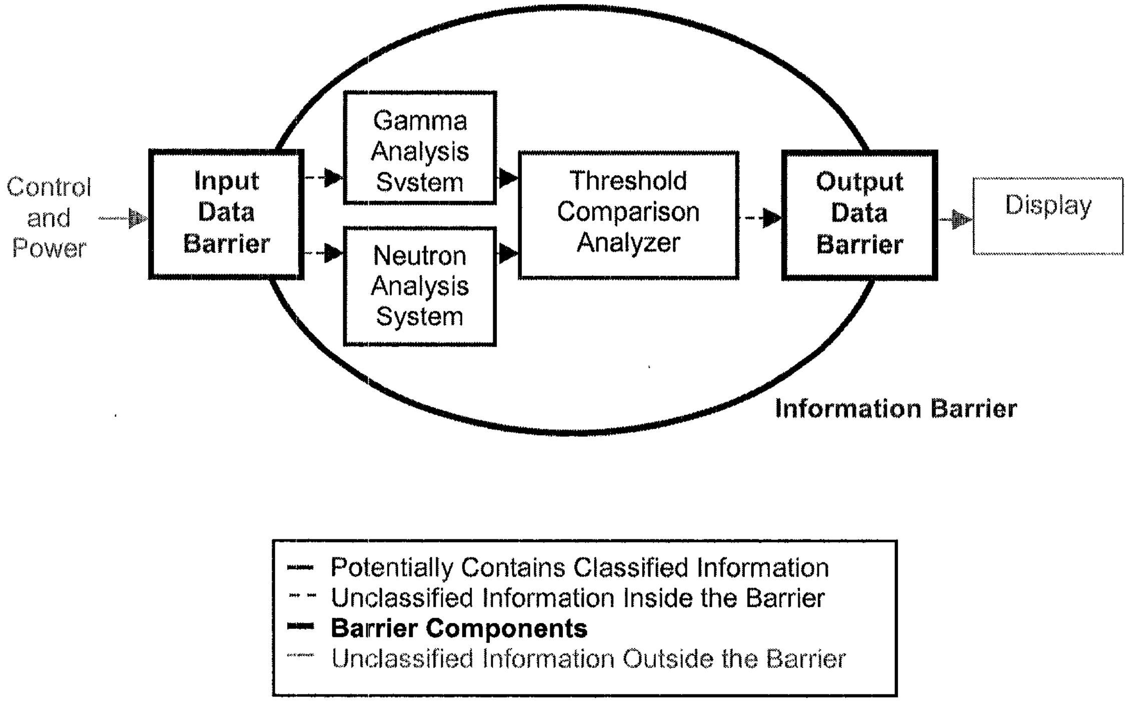
Control and Power
Input Data Barrier
Gamma Analysis Svstem
Neutron Analysis System
Threshold Comparison Analyzer
Output Data Barrier
Display
Information Barrier
— Potentially Contains Classified Information
- - Unclassified Information Inside the Barrier
▬ Barrier Components
--- Unclassified Information Outside the Barrier

Fig. 1. Core concept of an attribute measurement system. The data barriers are the only points of contact between the internal computing systems (potentially containing classified information) and the external environment.

THE TWO REQUIREMENTS FOR THE INFORMATION BARRIER

Although the primary purpose of an IB is to prevent the release (either accidental or intentional) of Host Country classified information, the implementation of the IB should allow the Inspecting Party to have confidence that the measurement system is producing meaningful results. Protecting classified information is relatively straightforward if that is the only goal. Strict access control is one method that is in widespread use. However, this type of information protection, while it completely satisfies the first criterion for an IB, totally ignores the second.

Similarly, if authentication is the only concern, then the solution is again straightforward. Standard safeguards techniques, although highly intrusive, are quite acceptable and effective for monitoring unclassified material. In this case, the Monitoring Party can observe the detector signals, the intermediate results, and anything else that will increase confidence in the veracity of the measurement. However, this type of intrusive monitoring is not acceptable for verifying classified material. This solution may satisfy the second criterion for an IB, but it totally ignores the first.

To be useful, an IB must simultaneously satisfy both criteria. We agree that security cannot be compromised. However, a measurement system that does not incorporate methods for authentication does not fulfill the requirements of the Monitoring Party and cannot be considered a useful IB.

HOST AND MONITORING PARTY CONCERNS

The most significant, although not the only, Host Party concern with the IB is the first criterion—data security. The host is primarily interested in the requirement that "the IB should prevent the release of classified information" and in the elements of the attribute measurement system that contribute to this protection. Thus the Host is most concerned with the IB itself. This includes the threshold comparison analyzer, the data barrier, and the enclosures and shields that make up the remainder of the physical aspect of the IB.

The threshold comparison analyzer compares the classified measurement results with unclassified thresholds to generate the binary outputs that eventually drive the unclassified indicator display. The output data barrier controls the flow of information between the computational block and the unclassified indicator display. If this element is designed so that it cannot pass classified information, then overall information security is enhanced. Finally, the enclosure and physical protection add to Host assurance that no classified information is being lost.

On the other hand, the primary interest of the Inspecting Party is in the second criterion, i.e., "the IB should also allow the inspecting party to reach credible and independent conclusions concerning the objects being monitored." The primary elements of the measurement system that impact this requirement are the data acquisition, analysis, and display systems. The correct operation of the data acquisition elements is important to the reliability of the output data. These elements of the system must function correctly, and as expected, if the Inspecting Party is to believe the indicator outputs.

We do not mean to imply that the only concern of either party should be in the areas specified above—only that these are the areas of greatest concern.

DESIGN FOR AUTHENTICATION

Many of the problems associated with authentication of systems including information barriers are discussed in detail elsewhere at this conference {6}, {7} and {8}. One problem of particular concern is the interface between IB design and later authentication of the entire measurement system. Although the primary purpose of the IB is protection of information, the IB design must take account of authentication requirements.

One of the most powerful authentication tools available is input into the design of the measurement system. Many design choices can be made that will enhance the authenticatability of the system (such as open operation modes {4}, reference source measurements, and modular electronic design) without reducing the level of data protection offered. Conversely, if all of the design choices are made without regard to authentication, the resulting measurement system may be nearly unauthenticatable. (Examples include multiple computer types, extraneous functionality, and required access controls.)

ACKNOWLEDGMENTS

We acknowledge the contributions of Thomas Gosnell, Richard Kouzes, Douglas Mayo, Karl Pitts, and Rena Whiteson to this paper. This work was sponsored by the U.S. Department of Energy and Defense Threat Reduction Agency/Cooperative Threat Reduction.

REFERENCES

{1} Duncan W. MacArthur and Rena Whiteson, "Comparison of Hardware and Software Approaches to Information Barrier Construction," *Nucl. Mater. Manage.* **XXIX** (Proc. Issue/CR-ROM) July 2000.

{2} Joint DOD/DOE Information Barrier Working Group, *Functional Requirements and Design Basis for Information Barriers*, PNNL-13285, PNNL, Richland, WA, May 1999.

{3} Duncan W. MacArthur, Rena Whiteson, and James K. Wolford, Jr., "Functional Description of an Information Barrier to Protect Classified Information," *Nucl. Mater. Manage.* **XXVIII** (Proc. Issue/CD-ROM) July 1999.

{4} Rena Whiteson and Duncan W. MacArthur, "Fissile Material Transparency Technology Demonstration Attribute Measurement System with Information Barrier: Functional Requirements," Los Alamos National Laboratory document LA-UR-99-5634 (Rev), February 2000.

{5} Duncan MacArthur, Rena Whiteson, Diana Langner, and James Wolford, Jr., "Proposed Attribute Measurement System (AMS) with Information Barrier for the Fissile Material Transparency Technology Demonstration: System Overview," Los Alamos National Laboratory document LA-UR-99-5611 (Rev), February 2000.

{6} J.K. Wolford, Jr., et al., "Software Authentication," to be presented at the INMM 42nd Annual Meeting, Indian Wells, CA, July 15-19, 2001.

{7} Richard Kouzes, et al., "Authentication Procedures," to be presented at the INMM 42nd Annual Meeting, Indian Wells, CA, July 15-19, 2001.

{8} Douglas Mayo et al., "Hardware Authentication," to be presented at the INMM 42nd Annual Meeting, Indian Wells, CA, July 15-19, 2001.