LA-UR- 00-5631

Approved for public release; distribution is unlimited.

Title: **INFORMATION BARRIERS**

Author(s): **D. W. MacArthur**

Submitted to: **Arms Control and Nonproliferation Technologies**

(Article)

Los Alamos
NATIONAL LABORATORY

Form 836 (8/00)

INFORMATION BARRIERS

Duncan MacArthur
Los Alamos National Laboratory
Los Alamos, NM 87454 USA

ABSTRACT

Many of the radiation attributes specified in international treaties, initiatives and agreements can be measured using traditional nondestructive assay methods. However, such measurements become problematical if the item being measured is classified. An information barrier, as described in this paper, is required to protect any classified information while displaying meaningful unclassified results.

Information Barriers

Many of the attributes discussed under "Treaties, Agreements, and Initiatives" can be measured using traditional nondestructive assay methods. These measurement techniques are well established and documented. However, such measurements become problematical if the item being measured is classified (as it is in many of these cases). Since useful radiation data generated from a classified item is generally classified itself, the data must be protected and not displayed directly. The information barrier (IB) that protects the classified information must perform two functions.

1) The IB must prevent the release (either accidental or intentional) of classified information.
2) At the same time, the IB must provide confidence that the measurement systems are functioning correctly and that the unclassified display is causally related to the classified measurements. (This is often referred to as the "authentication problem.")

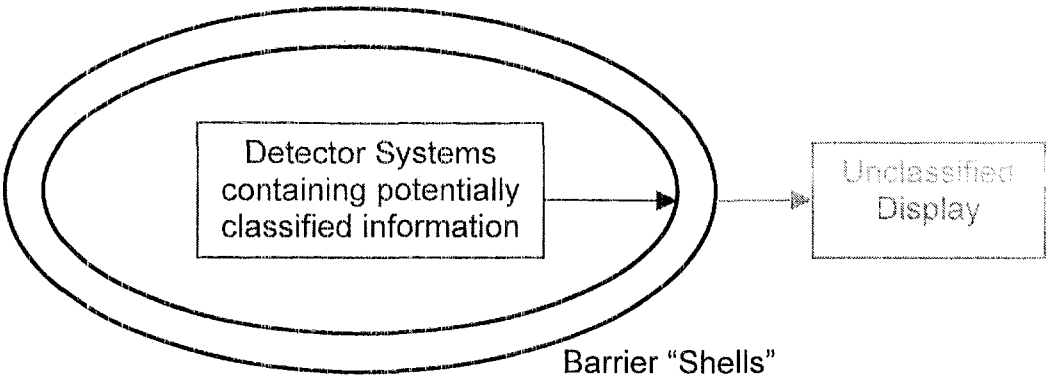
The IB is a combination of procedures and technology (both hardware and software) and, as such, cannot be easily identified in a photograph. The entire attribute measurement system, from detectors to display, is designed to address both requirements of the IB.

In order to prevent the release of classified information, the IB system is designed to eliminate the possibility of "single point" failures. Failure of any individual element of the IB will not result in the loss of classified information. An effective IB can be thought of a series of moderately strong protective shells as opposed to a single, very strong, shell. Each shell can be procedurally or technologically based or formed of a combination of the two.

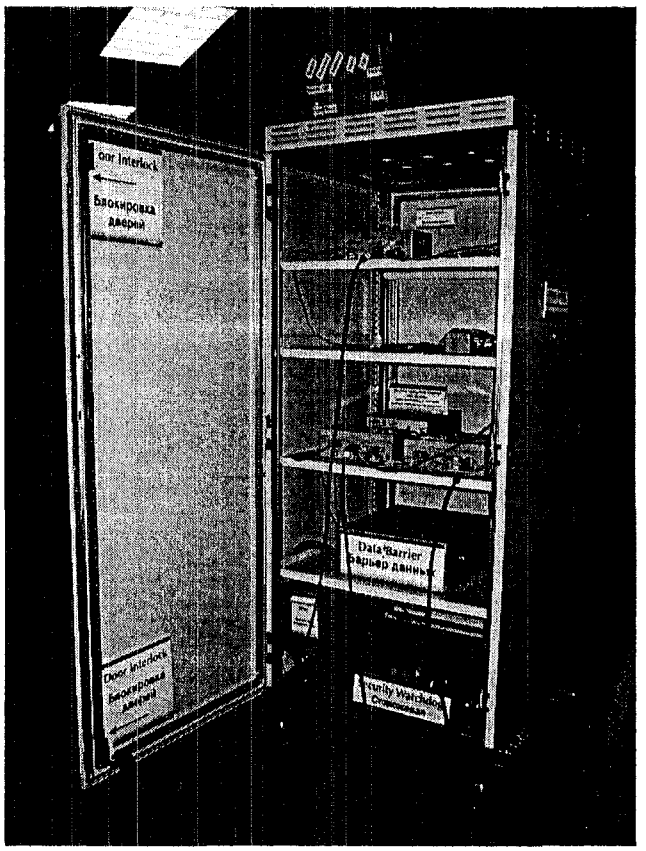
The IB must also be designed with the needs of authentication in mind. Each element of the measurement system (including the IB) should be simple and easy to inspect and should not have any extraneous functionality. If the measurement system composed of simple building blocks, or modules, the function of each element can be well-defined. Similarly, if each of the protective shells is simple, then it will be straightforward to verify that the information protection functions of the IB are operating as specified.

The closed shell(s) model is appealing from a security perspective, but some information must pass through the shell(s) if the measurement system is to function. Another key function of the IB electronics is to allow such transfer while ensuring that only unclassified information is transferred. Also, a security "shell" that is always closed is difficult to authenticate. An "open" mode of operation is required to allow inspection inside of the IB. The mode of system operation is monitored by an electronic circuit to ensure that classified information is not present when the doors are opened.

Attribute measurement systems incorporating IBs were demonstrated for a joint US/Russian Federation/IAEA audience in June 1999 (see Trilateral Initiative paper) and for a US/Russian Federation audience in August 2000 (see FMTTD paper). In addition, the IB concept was demonstrated as part of the PPRA workshop in November 2000.



Conceptually, an information barrier can be viewed as series of nesting shells separating the classified information from the surrounding area. If all classified information is contained within this barrier, the level of protection depends more on the shells themselves and less on the details of the measurement systems within.



Although many of the technological elements of the information barrier are contained in a single shielded cabinet, it would be incorrect to identify this cabinet as **the** information barrier. Rather, the cabinet contains a series of electronic modules that are critical to both the measurement and security functioning of the complete system.