LA-UR-01-5698
*Approved for public release;
distribution is unlimited.*

Title:

A Vulnerability Assessment of a General Attribute Measurement System

Author(s):

Karen Lewis Hirsch, Duncan W. MacArthur
and Rena Whiteson

Submitted to:

http://lib-www.lanl.gov/la-pubs/00796439.pdf

Introduction

A successful vulnerability assessment will enable a host nation to ascertain whether its classified information can be protected during a measurement regime. Specifically, vulnerability assessment is necessary to assure a host country that an intrusive measurement system will not be able to divulge classified information to an inspecting party. The vulnerability assessment must necessarily include a thorough analysis of the measurement system and the facility in which it is installed.

For the purposes of this document, an attribute measurement system is defined as a system that consists of a detecting system with an information barrier. The information barrier is defined as a physical and electrical boundary with very limited inputs and outputs. Figure 1 shows a simplified detection system with information barrier. The outputs must, by design, be unclassified – this is one of our operating assumptions. Some information barriers may be simple and allow only unclassified input and unclassified output, while others might be more complex. This second class of information barrier might allow for authentication of a subsystem output using unclassified inputs. For example, a switch that is always closed for classified measurements, but may be open for unclassified measurements. This switch would allow the information barrier to be open and permit additional inputs and show intermediate outputs, e.g. a spectrum on a screen.

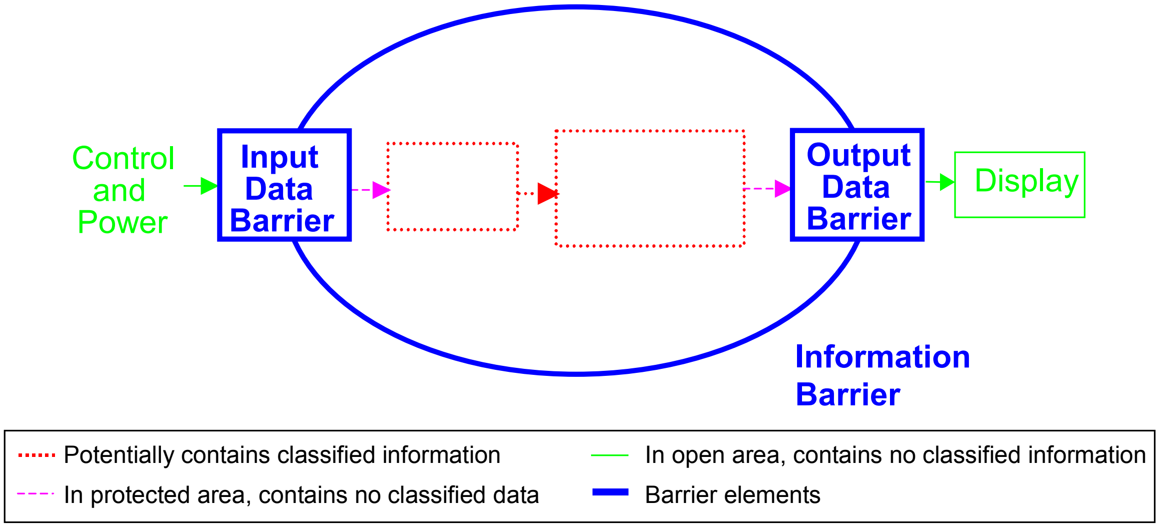
Control and Power
Input Data Barrier
Output Data Barrier
Display
Information Barrier
Potentially contains classified information
In open area, contains no classified information
In protected area, contains no classified data
Barrier elements

Figure 1. A simple detection system with information barrier showing that some components of a detection system are within the information barrier, while others must enter or exit the information barrier. Note that all measurements are taken within the information barrier, and that only processed, unclassified data can be seen outside the barrier.

A measurement system with information barrier may be designed or built by the host country or the monitoring organization.

- If the host country builds the measurement system, it must be assumed that they trust the instrument designers and builders to have no motivation for the release of classified data. Thus, the host country has less vulnerability if it designs and builds the measurement system.
- If the monitoring party has the responsibility for the design and fabrication of the measurement system, the host's vulnerability is increased. This can be mitigated by the use of commercially available and interchangeable components., This will increase the fidelity and decrease the time for the host country to assure itself that classified data will not be released. The host country must be confident that there are no hidden triggers that will cause the system to transmit data, that there is no possible method for data transmission, and that this is true both in the design and also in the final measurement system.

No matter who builds the system, the host country must be assured that it will not be releasing classified information by taking a classified measurement with the detection system. While this confidence is most easily achieved by the host country building the system, it is also achievable if the host country is able to physically inspect the system before measurements are taken. Only after the system has been validated by the host country, will it be used for measurements. It is assumed that the host country will have some control over the system after it has been built, meaning that it will not be shipped outside of the country or beyond an agreed upon location. Another assumption is that the host country has control over the samples being measured or monitored with this system. The facility is, by definition, under the control of the host country. This means that even though the inspecting party might be interested in acquiring the classified information hidden behind the information barrier, its ability to influence the release of that information is limited to methods they may carry into the facility. These would be constrained by the defenses that the facility puts in place.

Detection System

Detection systems generally include a power supply(s), a radiation detector, and some back end electronics (i.e. amplifiers to increase the signal output). There are three places where the monitoring party might attempt to gain access to signals: the inputs to the detector (including the power connections and/or object being detected), the output from the detector (assumed to be raw data), and any place where computation takes place. Assuming that the hosts control the detector(s) and inspectors have no physical access to them, then the only vulnerability associated directly with detectors is if they emit signals that are readable by inspectors (if they have appropriate devices for sensing these signals). Those signals could be used by inspectors to acquire sensitive information. Appropriate shielding can be used to prevent emissions of this sort. Protecting the wires coming out of the detector and entering the detectors by simple TIDs or seals should prevent tampering by the inspectors, who should be under surveillance while pursuing their inspections.

Information Barrier

An information barrier consists of physical, hardware, and software barriers to make the transmission of classified information impossible. There are several inputs to the system via into the information barrier, such as the power supply for the computers and hardware logic that are part of the information barrier. If the information barrier allows unclassified measurements in an “open mode,” to allow for more information to be transmitted, then a keyboard may be attached during “open mode.” This assumes that the system can recognize whether the sample being studied is sensitive or non-sensitive. Operator input can be limited to a button for initiating a measurement regardless of the mode in which the sample is to be measured.

The method of determining the mode of each measurement, *secure* or *open,* is a vulnerability. This method or mechanism must prevent unclassified measurements (i.e. measurements in open mode) of sensitive items or materials. The mechanism that determines whether a measurement must be in open or secure mode must be tested often. And it must be tested to assure that it cannot send covert signals through the switch and/or pushbuttons. This will be difficult to trace, as it could be either a hardware or a software signal.

An information barrier has an output of at least some lights. It is possible that it could also be sending signals in radio range. This is a vulnerability that must be analyzed both for continuous signal sending and for triggered signal sending. A triggered signal sending might be done by an inspector or by a signal being sent from outside the facility.

System interruptions could accidentally release classified information. It is important that the measurement system and the information barrier be designed such that no classified information can be stored. When a system interruption or error occurs, the system must immediately shut down. If it is possible, it should try to retain calibration information, but not any measurement data.

Calibration might be a vulnerability. This is the only time that information is being written to memory while data is being taken. It is important that the calibration procedure not allow classified information to be written to memory.

Emanations, tags and seals, and other concurrent measures

While none of the tags, seals and other devices that allow for the tracking of materials can prevent the release of classified information, it is important that all such items be scrutinized for ways that they could trigger emanations from within the information barrier. It is also important that they be analyzed for vulnerability if they are being used for assuring the host country that the inspectors do not have immediate physical access to the classified materials.

Summary

An intrusive radiation measurement system has several inherent vulnerabilities. These vulnerabilities could result in the inadvertent release of classified information by the host country or the intentional gathering of classified data by an inspecting party. Each component has to be thoroughly and regularly inspected to assure the host country of the protection of its data. Having a modular system in which components can easily be swapped and having full understanding of the system as a whole and how the components work together is vitally important to minimizing the vulnerability of a system.