LA-UR-98-3525

Approved for public release; distribution is unlimited.

Title: Information Barrier Functional Requirements

CONF-980887--

Author(s): Duncan W. MacArthur
Rena Whiteson

Submitted to: U.S./Russian/IAEA
Trilateral Technical Workshop
Savannah River Site, Aiken, SC
August 25-28, 1998

Los Alamos
NATIONAL LABORATORY

DISCLAIMER

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

Information Barrier Functional Requirements

Duncan MacArthur and Rena Whiteson
Los Alamos National Laboratory

INTRODUCTION: For the purpose of this paper, we have used the term "functional requirement" to indicate a required task rather than the recommended method for accomplishing this task. The creation of effective information barrier technology will proceed as a series of steps:

1) IB Conceptual Description[1]
2) IB Functional Requirements (this document - ongoing)
3) IB hardware and software specification
4) IB hardware and software construction
5) IB implementation

This functional requirements document is not intended to supplant or supercede the conceptual description; rather, these functional requirements are intended to be used along with the earlier description to help generate hardware and software requirements.

ASSUMPTIONS: These assumptions are based on a "straw man" scenario for pit inspection. This set of assumptions are based on conversation with James Tape.[2]

1) Time Frame
   a) Pits are received at the storage facility continuously
   b) Inspectors are not present at the storage site continuously
   c) Pits will be accepted into the program when inspectors are not physically present
2) Measurements
   a) Some unclassified identifiers (such as container ID) will be measured
   b) Some classified identifiers (such as radiation signatures) will be measured
   c) No classified information will be revealed to inspecting party
   d) Verification system operation may be checked (e.g. by inserting blind standards into the measurement area) by either party at any time
   e) Any previously monitored pit can be remonitored with an inspector present
3) Accounting
   a) All declared items must be accounted for
4) Data
   a) Classified data will not be transmitted
   b) Some classified data may be archived
   c) Red light/green light output will be archived along with container identification
   d) Any archived classified data must be in a form which is unalterable by the inspected party
   e) Any archived classified data must be in a form which is unreadable by the inspecting party
   f) Archived red light/green light data must be in a form which is unalterable by either party but readable by both parties

5) Equipment
   a) All inspection equipment will be under dual control
   b) System can be sanitized
   c) Commercial hardware is employed to the maximum extent possible
   d) Core software is unclassified

FUNCTIONAL REQUIREMENTS: Each requirement is numbered to identify the assumptions from which the requirement is derived. Assumption 2 mandates that an IB be in place, but this assumption does not make any specific requirements of the IB. Assumption 3 does not impact the IB directly. Thus, assumptions 1, 4, and 5 directly impact the functional requirements of the IB.
I have divided the IB functional requirements into the following areas:

- Physical protection
- Hardware hardening
- Assurance of capabilities and limitations
- Administrative controls
- Validation and verification of the systems and data
- Measurement error detection and resolution
- System error detection and resolution
- Equipment sourcing and maintenance
- Data paths (intended and unintended)

Physical Protection: (assumptions 1, 2, and 4)

- Access control
- Hardware
- Software
- Classified data archives
- Unclassified data archives

Hardware Emissions Control: (assumptions 1 and 4)

- Emission through the air (e.g. rf radiation)
- Transmission through conductors (e.g. power supply wiring)

Capability Assurance: (assumptions 1, 4, and 5)

- Commercial software
- Task-specific software
- Functional specifications of software elements
- Entire analysis system

Administrative Controls: (assumptions 1, 2, and 5)

- Procedural rules for participant behavior
- Procedural rules for unmonitored inspection
- Procedural rules for maintenance
- Continuity of knowledge
- Agreed on levels of participation in all activities
- Keys, passwords, etc
- Operational Security

Validation and Verification: (assumptions 4 and 5)

- Hardware and software inspection and verification
- Analysis system tests
- Authentication of archived data

Error Detection & Resolution: (assumptions 1 and 4)

- System errors
  - Misidentification of device under test
  - Detection
  - Rectification without revealing classified information
- Measurement errors
  - Identification of error
  - Remeasurement protocol
- Effect of error
  - False negatives
  - False positives

Equipment sourcing and maintenance: (assumption 5)

- Use commercial hardware if possible
- Allow for manufacturer maintenance of commercial hardware
- Use commercial software if possible
- Keep specialized software as simple as possible
- Allow for sanitation of most (all?) of the system

Data Paths: (assumptions 1 and 4)

- IB is combination of hardware and software barriers
- Defense in depth
- Hidden data paths
- Maintenance mode
- Interaction between elements
- Consider all barrier crossings

References:

[1] R. Whiteson and D.W. MacArthur, "Information Barriers In the Trilateral Initiative," Los Alamos National Laboratory Publication LA-UR-98-2137, May 1998.

[2]J. Tape, Private communication.