Review of Two US Information Barrier Implementations

(TRADS & RANGER)

B.D. Geelhood (PNNL), Richard Comerford (DOE/SO-222), David Lee (DTRA/OSPCT), James Mullens (ORNL), and James Wolford (LLNL)

Pacific Northwest National Laboratory
PO Box 999, MS P8-08, Richland, WA 99352, USA (509) 376-0276 bruce.geelhood@pnl.gov
June 26, 2001

ABSTRACT

An information barrier allows an automated measurement system to make non-intrusive measurements on sensitive materials by using negotiated threshold values to convert classified numeric results into unclassified pass/fail results. Allowing the Host to supply the measurement system provides confidence that classified information is provided paramount protection. Allowing the Monitor to authenticate the system provides confidence that the results are credible. Fundamental to information barrier design is a fully open or transparent measurement system. Complete documentation provides the basis for authentication and aids the Host's certification process. One authentication goal is to ensure the system does not contain any generic "hidden switch" feature, which the Host could selectively trigger to alter the inspection results to pass objects erroneously.

This paper is based on a review of two US information barrier implementations (TRADS and RANGER) and explores design options, which promote openness, enhance inspectability, and facilitate cost-effective authentication. These properties should be design goals. An open-design multichannel analyzer, which avoids proprietary internal software and data transfer formats, aids the authentication of gamma-ray spectroscopy. Both sides can have confidence in the results from data collection and analysis software, which is fully documented with complete source code. Confidence increases if the Monitor establishes that all installed software exactly matches a baseline copy prior to each measurement campaign. Without complete understanding of the controlling software, the Monitor is forced to trust that no subtle "hidden switch" is included. There is little point in merely exchanging trust in the Host's declaration regarding canister contents for trust in the measurement system or the controlling software. The design of the information barrier can aid authentication by reducing the amount of complex software and by using a simple operating system or eliminating the operating system. Problem-resolution protocols can be simplified if a robust design and analysis package is used to avoid unnecessary error conditions. Joint-inspection protocols can be simplified if the system uses good design rules, which avoid inspectability problems. Authentication can be more cost effective if the complexity of multiple computers of different types is avoided. Any reduction in the volume of hardware and software to be understood and inspected reduces authentication costs.

INTRODUCTION

An automated measurement system with an information barrier (IB) can be used to make a non-intrusive measurement during a verification inspection to confirm compliance. When the measurement potentially divulges information considered classified by the Host, an IB can be used to protect that information. The US organized a Joint DoD/DOE Information Barrier Working Group (IBWG) with representatives from several agencies and laboratories to develop functional requirements for information barriers [1]. These requirements are a basis for reviewing two example US information barrier systems. The basic, top-level functional requirements for the IB portion of an integrated radiation-signature, IB-protected inspection system are twofold:

1. The Host must be assured that his classified warhead design information is protected from disclosure to the Monitoring Party, and
2. The Monitoring Party must be confident that the integrated inspection system measures, processes, and presents the radiation-signature-based measurement conclusion in an accurate and reproducible manner.

Both these requirements can be achieved under a Host-supply scheme, where the Host has last private access to the system prior to use, as a means of providing the classified information paramount protection. When the Host designs and supplies a transparent measurement system, the Host gains confidence that some covert feature to divulge classified information is not included. In exchange, the Host's design must aid the Monitor's authentication team, which is tasked with gaining confidence that the inspection results are always credible. The IB, which protects classified information by blocking access to raw data and intermediate values, is best implemented through use of a transparent system, where all the details of the data processing within the system are available to all parties. The IB protects classified information by blocking access to all potentially classified information by presenting only pass/fail results regarding pre-agreed criteria. The pre-agreed pass/fail criteria can be based on measured attributes or template matching.

Although it is challenging to design a functioning system that can protect classified information, this task is made more difficult by the additional requirement that the design convinces the Monitoring Party that the results are always credible. The Monitor does not desire to merely transfer trust from the Host's declaration regarding the canister contents to trust regarding the measurement system design. Fundamental to a quality IB design is a fully transparent measurement system where hardware and software details are fully shared. This review of IB systems evaluates designs for both information protection and authentication concerns. *Authentication* is the process by which the Monitoring Party gains appropriate confidence that the information reported by a monitoring system accurately reflects the true state of the monitored item. Thus, the authentication process involves searching for both 1) inadvertent design or implementation flaws leading to incorrect results or a non-robust system and 2) deliberate covert features designed into the system for some Host advantage. The covert feature of primary concern is a selectively triggered hidden switch, which the Host can use at will to covertly switch failing results into passing results. Functional testing addresses some of these authentication concerns, but testing alone is incapable of discovering a selectively triggered hidden switch unless the Host is compelled to supply the trigger signals during such testing. Thus, confidence in pass/fail results comes from continuity of knowledge regarding each data processing step throughout the entire IB system, which is related to the quality of the IB design. Although some of the data used in the actual

measurement process is classified and will be unavailable to the Monitor, the method of data processing itself is unclassified and can be shared.

US INFORMATION BARRIER SYSTEMS REVIEWED

The IBWG commissioned a review of two IB-protected radiation measurement systems, TRADS [2] and RANGER [3], under development for warhead and warhead dismantlement measurement tasks. Since these systems were in development, a major task was to collect sufficient documentation to conduct the review.

TRADS – The Trusted Radiation Attribute Demonstration System (TRADS) [4] was developed by Sandia National Laboratories, Albuquerque (SNLA) for potential use in warhead dismantlement applications. TRADS is a cart-mobile and battery-powered sensor, which includes both a high-resolution 35% HPGe gamma-ray sensor in a lead shield to reduce background sensitivity and a pair of 4-atmosphere ^{3}He-filled tubes as a modest neutron sensor. The IB system known as TRADS has evolved from a template-based NaI(Tl) Radiation Inspection System (RIS) and an attribute-based HPGe system (RIS-plus). TRADS uses an Ortec DART multi-channel analyzer (MCA) for the HPGe sensor electronics, which acquires an 8k-channel spectrum between 30 keV and 3000 keV. The Minimum Mass Estimate (MME) software [5] is used to estimate both the plutonium mass and plutonium isotopics. The development effort focused on the trusted processor and the associated information barrier. A standard TRADS measurement is of 10-minute duration with a 1-meter source-to-sensor standoff between the axis of the inspected item and the detector face. Since the TRADS sensor is mounted 61 cm above the floor on a sturdy cart and the Host positions the sensor relative to the weapon, the slant source-to-sensor distance could be over a meter and include a significant uncertainty. However, the associated minimum mass uncertainty can be tolerable when using a negotiated mass threshold.

TRADS is a versatile portable high-resolution measurement system with the potential to satisfy the following missions during the weapons dismantlement process:

- Make IB-protected attribute measurements in the field to confirm items meet criteria as nuclear weapons as deployed and during a dismantlement process.
- Make IB-protected template-matching measurements in a template mode or version.
- Collect classified weapons signature data on US weapons for US use in a modified non-IB mode.

RANGER – RANGER was originally developed by Los Alamos National Laboratory (LANL) and subsequently commercialized with Quantrad Corporation [6]. RANGER is battery-operated, lightweight and waterproof. RANGER contains a 1.125-inch diameter, 2-inch long ruggedized NaI(Tl) scintillator with a 10% resolution at the 662-keV ^{137}Cs peak, which acts as the sensor for a low-resolution gamma-ray spectrometer. The gamma-ray spectrum covers energies between 60 keV and 3000 keV. RANGER contains a pair of 20-atmosphere ^{3}He-filled tubes as a modest neutron sensor. Plutonium detection requires at least a 6-σ (net-count) 414-keV ^{239}Pu peak and detection of neutrons. The presence of neutrons requirement (>2 cps over a typical 0.1 cps background) prevents spoofing with another gamma-ray source (e.g., ^{133}Ba). Highly enriched uranium (HEU) detection requires either a 185-keV ^{235}U peak or a 2614-keV ^{208}Tl peak typical of ^{232}U contamination. The system uses a low-power 8-bit microcomputer dubbed the "FORTH engine" because is uses the built-in FORTH programming language to analyze the data and display

the results. A standard RANGER hand-held measurement is of 60-second duration with a nominal 20-100 cm source-to-sensor standoff.

RANGER is a hand-held portable low-resolution radiation measurement system for use during weapons dismantlement from field decommissioning through warhead disassembly. Potential tasks include:

- Surveying containers to confirm absence of radioactive materials
- Surveying dismantlement cells to insure absence of radioactive weapon materials before and after a dismantlement operation
- Confirming the presence of radioactive weapon materials in a warhead installed on a missile prior to decommissioning
- Confirming the presence of radioactive materials from weapons during dismantlement and shipments
- Any survey where time or logistics make a more definitive TRADS survey difficult.

DESIGN BASIS CRITERIA REVIEW

The IBWG design guidance looked at ten aspects of IB design. The subsequent sections will briefly summarize these aspects and use examples from the two reviewed IB systems to illustrate issues. These IB systems contain examples of both desirable and undesirable design features because development began prior to the IBWG design guidance. The guidance was not specific and allows implementations to fit various applications. Both IB systems should be slightly modified from the hardware reviewed before being used for IB-protected measurements in a dismantlement scenario. For example, both demonstration units had the ability to internally store the raw data from the weapon measurements to allow the US to collect a set of data typical of dismantlement scenarios for evaluation and algorithm development. The algorithms used to process the data behind an IB must be robust against unexpected circumstances and produce valid results without expert analysis or intervention. Thus, practice data is important for IB algorithm development.

1 - SYSTEM SUPPLY

The IBWG guidance strongly recommends that the Host supply the IB-protected measurement system. The "Host-supply" approach best protects the Host's classified information and meets safety concerns. It is also the least problematic to carry to the negotiating table and to win the approval of security organizations responsible for protecting weapon design information.

TRADS and RANGER were designed, built, and operated by US personnel only. The "Host-supply" approach greatly aids in obtaining the approval of US security organizations for performing measurements at sensitive sites. The security review still requires consideration of an insider threat under Host supply. A transparent and easily inspectable system helps both the Host alleviate information protection concerns and the Monitor mitigate credibility concerns. Once used for classified measurements, automated measurement and analysis equipment generally is not released without sanitation.

The "Host-supply" scheme is consistent with a random-selection-based protocol where the Host provides multiple identical copies of the system after having the last unconditional access to satisfy security and safety concerns. The Monitoring Party then selects one for use and another to

remove for private examination. RANGER is an example of a potentially commercial unit where the Monitor could readily procure extra units for familiarity or additional testing. The relatively small size and low replacement cost of RANGER and the trusted processor module of TRADS facilitates the random selection process.

The "Host-supply" scheme makes the Monitor's authentication task much more difficult than it would be under a "Monitor-supply" scheme. The Monitoring party can have confidence only in results coming from fully transparent systems. As a show of good faith, the developers of TRADS and RANGER fully disclosed all aspects of these systems for which documentation and source code was available. However, a complete hardware and software documentation package sufficient for authentication had not yet been assembled. It remains problematic whether all aspects of the DART hardware and firmware details can be fully disclosed. It may be necessary to develop a MCA unit specifically for arms-control applications requiring transparency.

2 - CENTRAL PROCESSING UNIT (CPU)

The IBWG guidance strongly recommends single-board computers over laptop and desktop computers. The guidance recommends the use of readily inspectable trusted-processor architecture dedicated to specific processing tasks without extraneous functionality. The guidance does not specify a preference for a specific microprocessor.

The trusted processor is the focus of the TRADS design philosophy. TRADS uses a pair of CPUs, which are separated into CLASSIFIED/UNCLASSIFIED or RED/BLACK computers. This dual computer design is based on experience with cryptographic processing and used single-board computers (SBC) with the PC-104 architecture. The RED CPU is a Pentium (Win Systems PC/104 586DX SBC model PCM-586) and the BLACK CPU is an 80386 (Win Systems PC/104 386SX SBC model PCM-SX). These two computers are carefully separated with a custom printed circuit board containing an optically isolated serial communication line as the only connection between the two CPUs. The BLACK computer receives only single-byte messages from the RED computer and is the *de facto* information barrier. The software in the BLACK computer is relatively simple and examination of that software provides confidence that information is adequately protected. The Pentium microprocessor is more complex than 80386 and 80486 microprocessors used elsewhere in other IB systems. However, sufficient details regarding older Pentium microprocessor internals are available for an authentication effort. The use of two different classes of CPU doubles the authentication efforts regarding the computer hardware and system software. TRADS also uses an Ortec DART with an embedded CPU of yet another type. The design using two independent stacks of printed circuit boards is professional and inspectable. Potential thermal problems were mitigated with a robust heat sink between the two CPU cards. Reliability problems traced to static electrical damage were mitigated during subsequent construction. Since the tamper-indicating housing precludes inspections as well as modifications, some protocol for joint inspection and witnessed sealing is required. The review noted avoidable extraneous serial ports in TRADS.

RANGER uses a low-power 8-bit microcomputer, New Micros MC68HC11FN-V3.5 based on the Motorola MC68HC11E9 with the FORTH operating system installed in the 12-K on-chip mask-able read-only-memory (ROM). About 30-kbytes of RANGER-specific firmware resides in an external 32-kbyte UV-erasable EPROM (32x8 PROM of type 27C256). RANGER also

relies on examination of the relatively simple software to provide confidence that information is adequately protected. The RANGER software is the *de facto* information barrier. The simple microprocessor is not widely used, but has many real advantages: 1) it requires no operating system, 2) it requires no separate BIOS software, 3) the application software is limited in size, and 4) it can handle building the spectrum without another CPU embedded in support electronics. Both IB systems require additional system documentation to identify all unused non-volatile memory that might exist in various CPU components and all the I/O details.

3 - NON-CPU EQUIPMENT

The IBWG guidance strongly recommends that the non-CPU equipment be inspectable. Commercial equipment is recommended, and inspectability should be considered on a case-by-case basis. Analog sensor electronics are generally considered less complex than CPUs. However, some sensor electronics contain imbedded microprocessors and should be considered as additional CPUs.

TRADS uses a DART, which is controlled by an embedded CPU, which contains proprietary software that was not available for the review. A non-disclosure agreement to acquire the source codes for the authentication team is preferable to merely showing the code matches that in another unit obtained by anonymous purchase. The DART was specially modified to turn on as soon as power is applied and to discard memory values as soon as power is removed by removing the internal battery. The DART's internal storage of ten 8k-channel spectra should be mitigated by actively clearing all buffers before and after each measurement. It may be difficult to modify any commercial MCA to remove undesired functionality without complete documentation, which exceeds that typically provided. TRADS uses an 8k-channel full-energy spectrum (30 - 3000 keV) without compromising information. Energy calibration requires measurement of thorium welding rods and is based on fitting three peaks (238 keV, 583 keV, and 2614 keV). Since automatic energy calibration using peaks in each spectrum is not used, it is potentially not robust against gain drift.

RANGER uses an 8-bit flash ADC in a non-traditional manner. Energy calibration requirements are not as stringent with a low-resolution NaI(Tl) spectrum as with a HPGe spectrum and automatic energy calibration on several known peaks in each spectrum is not feasible.

4 - PROCEDURAL ISSUES

The IBWG guidance strongly recommends that procedures be used to prevent the Monitoring party from gaining collateral information about the test items based on the measurement geometry and the transparent sensor characteristics. Automatic dead-time controls and a fixed counting time can prevent disclosure of the source strength. Procedures should also address operational security to prevent collection of collateral information from postings, observing security measures, and careless talk.

The dynamic range of TRADS is large enough to control the deadtime and avoid the use of apertures. The 1-meter standoff and relatively wide acceptance angle of the shielded HPGe sensor makes measurements insensitive to weapon geometry details.

As the IBWG design guidance noted, an IB must not only prevent the disclosure of sensitive information from measurement data, it must prevent the deduction of sensitive information from the overall inspection process. Protocols for the use of RANGER need to be written to prevent its use in sweep mode near weapons. A radial sweep approaching a weapon could indicate source strength from the range at which detection first occurs. An axial sweep along a weapon could indicate geometry information. The hand held RANGER is more subject to neutron moderation and/or interference from nearby humans.

5 - ELECTRONIC EMANATIONS

The IBWG guidance is concerned with two possibilities regarding electronic emanations. The Host is concerned that the classified information is not revealed by electronic, audio, or optical emanations. The Monitoring party is concerned that the Host could covertly control the results remotely by radio frequency (RF) or other means.

As reviewed, TRADS did not attempt to RF shield anything except the trusted processor within a tamper-indicating enclosure made of austenitic stainless steels. The exposed neutron tubes are a source of concern for extra signals induced by external RF signals. RF shielding improvements should be made to TRADS components outside the tamper-indicating enclosure. The plastic case of some RANGER models provides no RF shielding and the metal case of other models had gaps in the RF shielding for the keypad and display. Both systems could improve their RF shielding.

6 - LOCATION OF BARRIERS

The IBWG guidance recognizes that filtering unnecessary data early in the acquisition and analysis process is a valid IB design principle. The guidance also provided that intermediate barriers could afford some additional security, but the final output was all that really mattered. However, it cautioned against using intermediate barriers if those barriers hinder checking system functionality or compromise functionality assurances.

Neither system used a design based on several layers of protection. This is acceptable under the IBWG guidance because the absolute protection of classified information is a paramount requirement and a partial leak is unacceptable. TRADS relies on the pair of RED/BLACK CPUs as the only layer of protection with the software in the BLACK CPU the *de facto* IB. RANGER relies on the software in the single CPU as the *de facto* IB. The IBWG does not require a hardware-only data barrier. The concept of a separate computational block computer where classified numeric results are converted to an unclassified pass/fail display was not implemented on either system. The lack of a computational block is desirable since it reduces the CPU count. If a separate and simple program is desired to accomplish that function, it can easily be implemented as a separate batch-mode program on the analysis computer.

The full-energy gamma-ray spectrum (30 – 3000 keV) is used in both systems. This allows use of peaks indicative of HEU at 185 keV and 2614 keV as well as all the plutonium peaks used by the MME algorithms (300 – 800 keV), which estimate mass based on relative peak attenuation and steps in the baseline due to attenuation. No attempt is made to segregate neutron and gamma-ray information or plutonium and HEU peaks within either system. The IBWG guidance allows the analysis full use of the measurement data.

7 - SOFTWARE, FIRMWARE, and OPERATING SYSTEMS

The IBWG guidance is concerned with two possibilities regarding software. The Host is concerned that the classified information is not revealed by planted or inadvertent computer code quirks of system operation. The Monitoring party is concerned that the Host could covertly control the results if the computer code cannot be adequately examined because it is either proprietary or too complex. The IBWG guidance strongly recommends avoiding extraneous code and complex operating systems. The IBWG guidance requires that all computer code in the form of firmware, applications software, and operating system must be inspectable and shared.

TRADS specific software was provided as source code to the review team on a floppy disk. Full transparency of the embedded software and firmware in the DART is viewed as problematic at this time. This may require development of a transparent MCA or non-disclosure agreements for authentication purposes. TRADS uses ROM-DOS version 6.22 from Datalight. Full source code is available for a fee and a non-disclosure agreement must be signed. The software to handle the serial and parallel I/O (COM and LPT ports) was custom written in a concise manner. This facilitates authentication by avoiding large commercial I/O libraries that generally involve extraneous functionality and massive amounts of code. Dean Mitchell wrote concise custom software for data collection based on Ortec's DIALOG library and his own MME analysis software in FORTRAN. Since a batch file controls sequential analysis programs, some method of storing intermediate data files is necessary (e.g., RAMDISK).

All LANL-developed RANGER software was provided to the review team to demonstrate transparency. RANGER contains minimal amounts of software. No operating system is used, but the system boots to a single dedicated program written in FORTH. All the applications software for the fully functional commercial version resided in PROM, but the calls for the unused code were deleted from the software used for the IB-protected version of the code. All unused or "dead code" should be removed. The software builds the spectral histogram internal to the CPU as a 256-channel spectrum using an interrupt-service routine to read the ADC value and increment the desired channel. The IB version uses 32 bits per channel and collects data for a full 60 seconds prior to analysis avoiding rollover and early termination problems. The software has extra tests to protect against erroneous plutonium results due to ^{133}Ba and ^{137}Cs sources.

8 - DATA STORAGE

The IBWG guidance strongly recommends elimination of nonvolatile data storage.

A template-processing version of TRADS contains a provision for external data storage of template information. A template initialized by a warhead measurement would be considered classified by the Host. One might also consider a scenario were the Monitor supplied a classified template. In any template application, an external Dallas button with serial communication to the CPU is a reasonable mechanism for separable and limited nonvolatile template storage, which could eliminate single-party control over or use of the template data. The access via a COM port allows the Host-supplied software system to read in the data, but prevents execution of any software potentially located in the external memory. The Dallas button is not desirable or intended for use with an IB system based on attributes.

TRADS used an 8-Mbyte DiskOnChip Solid State Disk to hold the system software (1 Mbyte) and to log spectra during a demonstration. RANGER had two battery backed up 32-kbyte SRAM memories used to log spectra, which could also hold expansion software. In both, the logged data was internal to the device and could be protected by protocol. The demonstration also involved collecting data so the logging feature was not covert. The logging feature could be very useful during development and private authentication. This spectra-logging version should be replaced with IB-specific software on a non-rewritable PROM for two-party inspection applications. The review discovered a means of updating the TRADS software held on the DiskOnChip via an accessible serial port. A means of adding programming to RANGER via an accessible serial port was also found. The software update feature should be removed at completion of development, but modification would not be possible to software held in PROM.

TRADS is unique among the IB demonstration systems in giving serious consideration to the problem of verifying that the contents of the PROM containing the system software remains unchanged from a previously inspected and "trusted" baseline version. The Secure Hash Algorithm maps user-input seed values with the protected data into output digest values. This approach provides protection against any deliberate attempt to modify the software content or the comparison software. The approach requires both input of Monitor-selected seed values and output of digest values in an open mode without classified data present. Although the CPU may have been previously used for classified processing, sensitive or classified information is not at risk during the authentication process when this hash-function approach is combined with first purging all data from the system. The hash function protection should be implemented to examine all computers and all memory within the system. Software verification should occur prior to each measurement campaign. There should be some direct method of absolutely purging all classified data from the system both at the completion of each measurement and prior to software verification to preclude any possibility of covert disclosure. The unused bytes in PROM or flash memory should be cleared to either hexadecimal $00 or $FF, whichever is the opposite of the memory value set by a "block-erase" command prior to initial programming. RANGER only uses a checksum test, which is effective only against modifications due to memory failures and provides no protection against intentional modifications.

9 - INPUTS AND OUTPUTS

The IBWG guidance strongly recommends against extraneous input or output ports, but in favor of the use of dedicated I/O ports and the use of YES/NO type results.

TRADS uses a hand-held device user interface with a liquid crystal display (LCD) [4 lines of 20 characters] and a 24-button keyboard. RANGER also uses a LCD [240x128-pixel resolution with an on-board character generator for 16 lines each with 30 characters] with a small keypad with some keys unrecognized. Some prefer a small array of light-emitting diodes (LED), which are physically limited to passing only 1-bit of information per attribute in secure mode. Experience shows that certification officials strongly favor simple displays without any physical ability to pass classified information, although software can limit the output just as effectively. The IBWG design guidance recommends a two-line LCD as acceptable, but further IB experience indicates problems with LCD acceptability in secure mode. The ability to output hash function digest values requires the use of the LCD. Systems with only simple LED displays require an additional more capable display in open mode, which is often a video display.

The only difference between the current IB-protected version of RANGER and the commercial version without an IB is the software running in the device. Since swapping PROMs is all that is necessary to convert between the two versions, the reduced keypad for the IB version is really the same keypad as on a commercial Ranger with several software calls removed. The IB version of RANGER has the serial port connection mounted internally rather than externally. Currently, the serial port can be used to reconfigure the RANGER unit by downloading additional software or to change existing software settings. This is highly undesirable in terms of both protecting information and authenticating the system against a "hidden switch".

10 - AUTHENTICATION AND REPAIR

The IBWG guidance addresses authentication of "Host-supplied" equipment and recommends Monitor selection by random means between multiple copies as a possible solution. It assumes that the Host and Monitoring Party will completely share designs.

TRADS and RANGER are not yet authenticatable systems. Complete documentation was not available for the reviews because development was incomplete, but the developers were open and supplied available information. Disclosure of software source codes indicated a desire for transparency. The size and cost of RANGER and the TRADS trusted processor enable random selection protocols. The use of a secure hash function to verify software integrity on the PROMs also facilitates authentication, but requires further development. The tamper-indicating enclosure is a useful and unique feature to TRADS, as the other demonstration IB systems have no such tamper-indicating barrier. The tamper-indicating enclosure provides protection for the software/firmware and hardware components within, which relaxes the need for visual and software authentication at the start of each measurement shift.

These systems lend themselves to repair by module replacement subject to a random selection scheme.

SUMMARY

The IBWG team examined two US information barrier systems and noted several issues regarding the IBWG design guidance that should be useful for future design revisions. These systems can protect classified information using a combination of technology and protocol. Design improvements can facilitate authentication. Complete documentation was not available for the review, but sufficient information was gained from the design teams and public sources to demonstrate authentication was in principle possible.

ACKNOWLEDGEMENTS

This work was supported by the U.S. Defense Threat Reduction Agency and by the U.S. Department of Energy. Battelle operates Pacific Northwest National Laboratory for the U.S. Department of Energy under contract DE-AC06-76RLO 1830. The developers of these two systems, Dean Mitchell (TRADS) and Bill Murray (RANGER) were extremely helpful and cooperative during these reviews.

REFERENCES

[1] Joint DoD/DOE Information Barrier Working Group, *Functional Requirements for Information Barriers*, PNNL-13285, Pacific Northwest National Laboratory, Richland, WA, May 1999.

[2] Bruce Geelhood, PNNL, Richard Comerford, SO-222, David Lee, DTRA/OSPCT, James Mullens, ORNL, James Wolford, LLNL, "Information Barrier Working Group Evaluation of Ranger", PNNL-13260, August 2000.

[3] Bruce Geelhood, PNNL, Richard Comerford, SO-222, David Lee, DTRA/OSPCT, James Mullens, ORNL, James Wolford, LLNL, "Information Barrier Working Group Evaluation of TRADS with Particular Attention to Its Authentication Merits", PNNL-13259, August 2000.

[4] Dean Mitchell, Trusted Radiation Attribute Demonstration System – TRADS, Info sheet.

[5] Dean Mitchell and Keith Marlow, Minimum Mass Estimates for Plutonium Based on the Peak Intensities and Scattered Radiation in HPGe Spectra, Sandia National Laboratories, Oct 13, 1999.

[6] William Murray, ----