Trusted Radiation Identification System

Kevin D. Seager, Dean J. Mitchell, Thomas W. Laub, Keith M. Tolk,
Richard L. Lucero, and Kenneth W. Insch

Sandia National Laboratories[a]
Albuquerque, New Mexico 87185-1207

ABSTRACT

The Trusted Radiation Identification System (TRIS) was developed at Sandia National Laboratories to provide a means for confirming the identities of Treaty Accountable Items (TAIs) by comparing gamma-ray spectral measurements, which is a technique that is often referred to as template matching. TRIS incorporates design features that accommodate the conflicting requirements of ensuring that host-country classified information is protected while assuring the inspector that the measurement results are valid.

TRIS uses a divided hardware and firmware architecture that isolates classified information from the unclassified output to facilitate certification for use with classified components. Data are collected and analyzed by a trusted processor that contains two separate processing units mounted within a tamper-indicating enclosure. The red side of the trusted processor acquires classified data from a sodium iodide gamma-ray spectrometer connected to a commercial multichannel analyzer. The black side of the trusted processor interfaces with the operator via a serial port connected to a simple hand-held input/output device that has a small keypad and a four-line liquid-crystal display. Communication lines between the two processors are optically isolated and a central steel plate provides radio-frequency isolation between the two processing units. The steel plate also provides a conductive heat path from the processing units to the steel enclosure. A 12-volt battery supplies power to both the trusted processor and the spectrometer.

The trusted processor employs hardware and software features to facilitate inspection of the equipment. An eddy-current scanner is used to inspect the trusted processor: the material properties associated with the random crystallization patterns in the welds uniquely identify the stainless-steel enclosure; the eddy-current scans would also reveal penetrations into the enclosure that may not be visually observable. The trusted processor also uses an algorithm that employs cryptographic functions to authenticate both the firmware and the radiation templates.

INTRODUCTION

Sandia National Laboratories (SNL) has considerable experience in using low-resolution spectral data from sodium iodide (NaI) detectors for radiation template measurements. SNL designed the man-portable Radiation Measurement System (RMS), which has been used at Pantex since 1994 to confirm the identities of containerized pits by comparing low-resolution gamma-ray spectra with certified spectral templates for the components.[1] Template comparison methods have also been applied in arms control demonstrations, which differ from domestic applications because classified information must be protected. SNL's first-generation approach was the Radiation

[a] Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

Inspection System (RIS), which was used at Los Alamos National Laboratory (LANL) and Pantex in 1997 to demonstrate that template matching can be performed in a way that is robust and does not reveal classified information. However, RIS did not contain any tamper-indicating features or information barrier technology other than having an unclassified display, and it used a laptop computer, which cannot be easily inspected.

The Trusted Radiation Identification System (TRIS) has recently been developed at SNL to generate and confirm radiation templates of Treaty Accountable Items (TAIs). TRIS builds on the technology that was previously demonstrated as RIS and incorporates many of the information barrier features utilized by the SNL-developed Trusted Radiation Attribute Demonstration System (TRADS).[2,3] There are two fundamental requirements for an information barrier in a radiation signature inspection system: warhead design information must be protected, and inspectors must be confident that the results accurately reflect the characteristics of the item being measured.[4] The protection of classified information is the more important requirement, which dictates that the inspection equipment must be provided by the host country. Consequently, ensuring inspector confidence is more challenging than previous arms control applications (INF and START), where inspector-supplied equipment was used to perform radiation measurements.

HARDWARE

The components used in the current TRIS are shown in Fig. 1. These components include a NaI gamma-ray detector, an Ortec DART multichannel analyzer (MCA), a trusted processor, a hand-held input/output (I/O) device, a 12-volt battery, and data storage devices referred to as iButtons.

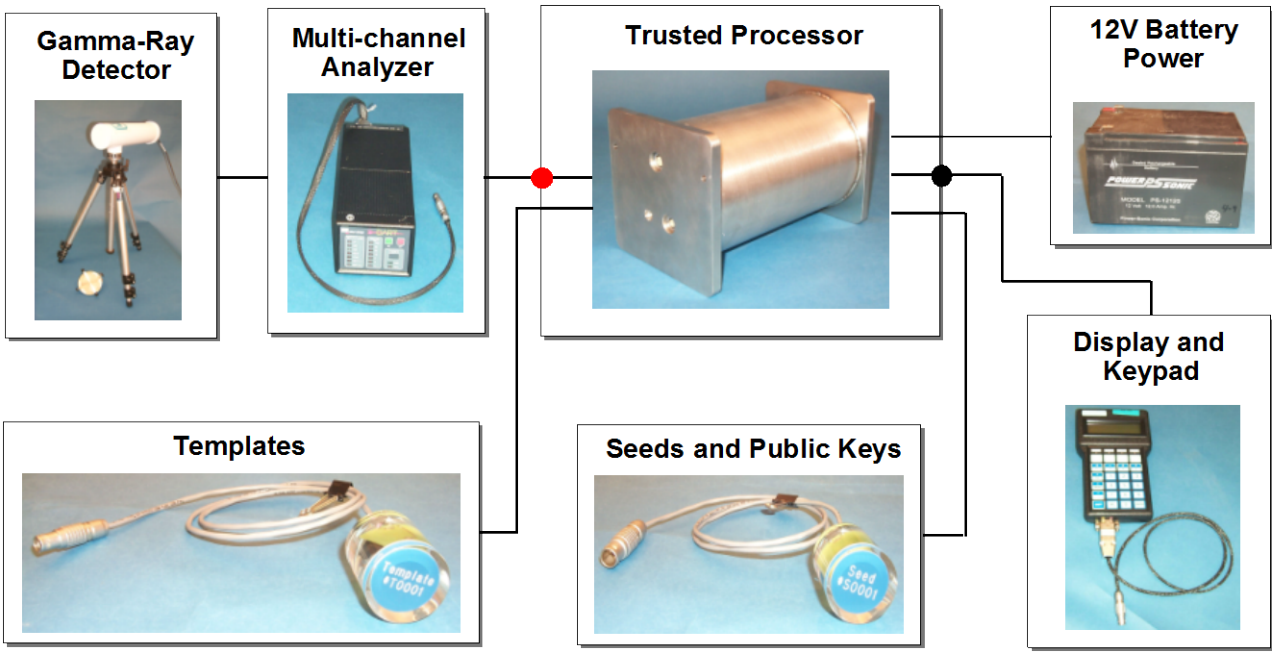

Figure 1. TRIS Components

NaI Detector Assembly

TRIS utilizes a two-inch diameter by two-inch long NaI scintillation crystal to detect gamma rays emitted by radioactive material in a nuclear weapon. An Ortec Model 269 preamplifier/tube base is attached to the photomultiplier tube. The detector is housed in an aluminum tube with a diameter of 4″ and a length of 16.5″. The sides of the detector are shielded by 0.5″ of lead and the back of the detector is shielded with 0.25″ of lead. A 0.030″-thick tin sheet surrounding the detector is used to attenuate low-energy gamma rays emitted by the inspected items and to block x-rays emitted by the lead. The detector tube can be mounted on a tripod and thus positioned at a variety of heights above floor level. A 0.5″-thick tungsten shield is placed in front of the detector when background measurements are performed.

Multichannel Analyzer

Spectra recorded by the Ortec DART MCA are passed to the trusted processor through the parallel port. The DART was modified to turn on when power is applied, and replacement of the lithium backup battery with a high-impedance resistor prevents data storage after power is removed. Long-term plans call for replacement of the external, commercial multichannel analyzer with a trusted analog-to-digital (ADC) converter board that will be added to the board stack on the red side of the trusted processor. The use of digital electronics will be minimized and the Trusted ADC will have a simple, open architecture to facilitate inspection.

Trusted Processor

The TRIS trusted processor has separate red (classified) and black (unclassified) sub-systems, which are physically identical. Each subsystem contains three commercial PC-104 cards (586 CPU, COM4A serial communications board, and DC-DC power supply) and three SNL-designed PC-104 cards (optical communications board, communications interface board, and spiral tamper board). Figure 2 shows an assembled trusted processor in a Lucite enclosure, which is used for illustrative purposes only.

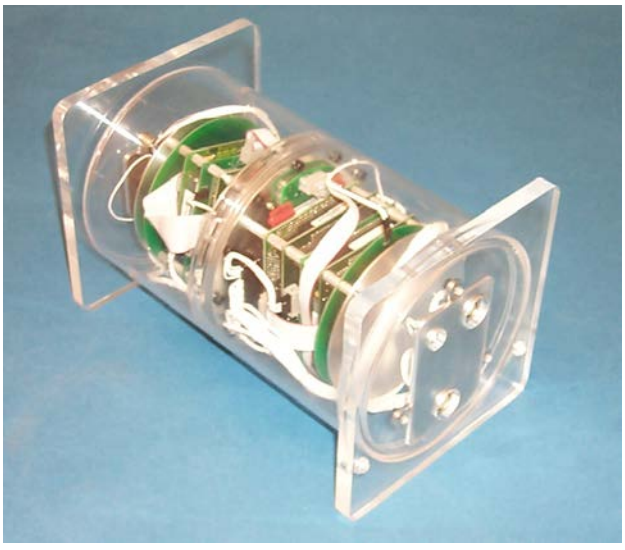

Figure 2. Transparent Version of TRIS Trusted Processor

The “red” side of the trusted processor collects and processes gamma-ray spectra, which may be classified. The only function of the “black” side is to provide a security buffer for communications between the red processor and the hand-held I/O device, so that no single-point failure can result in the release of classified information. A 0.375″-thick steel plate provides radio-frequency (RF) isolation between the two sub-systems; it also serves as a heat sink for the processor chips, which are abutted against the plate. The serial communication lines between the two processors are isolated to avoid ground loops and to prevent inadvertent RF transmission between the two processors. This is accomplished by using an optical communication board on each of the processors to interface with three emitter-detector pairs, which face each other through pinholes in the steel plate.

The fully welded stainless steel container minimizes RF emissions to ensure protection of classified information. The stainless steel canister also serves as a tamper-indicating enclosure (TIE). The eddy-current scanner, shown in Fig. 3, requires about 10 minutes to inspect for evidence of penetrations and to identify the trusted processor based on the unique signatures produced by the random crystallization patterns of the welds.[5] The spiral tamper boards provide additional tamper indicators. Both sides of the tamper boards have continuous 0.010″ electrical traces with 0.010″ spacing, and the traces on the two sides are offset. A continuity check, which is performed during the boot-up process, would detect penetrations through connectors mounted on the ends of the enclosure.

Figure 3. Prototype Eddy-Current Scanner scanning Trusted Processor

Connectors mating to the trusted processor are uniquely sized and cannot accidentally mate with an incorrect connector. 12-volt DC power is supplied to the black side of the trusted processor via the 2-pin Lemo plug. A power filter in the steel ground plate eliminates high frequency noise before it enters the red side of the trusted processor.

Hand-Held Input/Output Device

The black side of the trusted processor interfaces with the operator via the hand-held QTERM-II Model T1005 input/output device. This I/O device has a small keypad and a four-line liquid crystal display (LCD). It uses a serial port for data communications.

iButton® Memory Storage

The storage devices utilized by TRIS are memory computer chips with a networking serial interface housed in a 0.63″ diameter stainless steel can. The devices are manufactured by Dallas Semiconductors and are commonly referred to as Dallas Buttons or iButtons®. These iButtons are enclosed in acrylic cylinders with attached cables. Random number seeds, public keys, and templates are stored on iButtons. Two types of iButtons are used: a DS1996 Read/Write 64 Kbit nonvolatile memory device and a DS1986 64 Kbit erasable programmable read only memory (EPROM) device. Both devices transfer data serially via a 1-wire protocol using a single data lead and ground return. An EPROM iButton can have data written to it only once. During TRIS development, the Read/Write iButtons were preferred because of the extensive amount of testing with the writing and reading of seeds, public keys, and templates. In actual operation during an arms control regime, TRIS will only support the use of the EPROM iButtons for storing public keys and templates because they have a longer memory retention time than the Read/Write iButtons. TRIS can verify whether an EPROM iButton has been used previously, and it will prompt the user for a new EPROM device if it has been used before.

FIRMWARE

During the development of the TRIS trusted processor, preliminary versions of application programs were stored on nonvolatile 8-Mbyte disk-on-chips. This allowed developers to make software upgrades easily. In the current system, application programs are stored on 1-Mbyte EPROM chips that cannot be reprogrammed while they are inside the trusted processor.

Firmware Integrity Verification

TRIS utilizes a verification algorithm to confirm the authenticity of the firmware without revealing classified information. As illustrated in Figure 4, the inspector performs authentication of the TRIS firmware using the secure hash algorithm (SHA-1) in a keyed-hash protocol.[6] Numerical hash keys are entered via the hand-held user I/O device. The TRIS firmware that is hashed includes the basic input/output system (BIOS), the interrupt vectors, the operating system, and all the application programs. The red and black sides of the trusted processor are independently hashed using the same hash key. The hash values generated during an inspection must exactly match the hash values generated earlier using the same hash key on an identical trusted processor with firmware known to be correct.

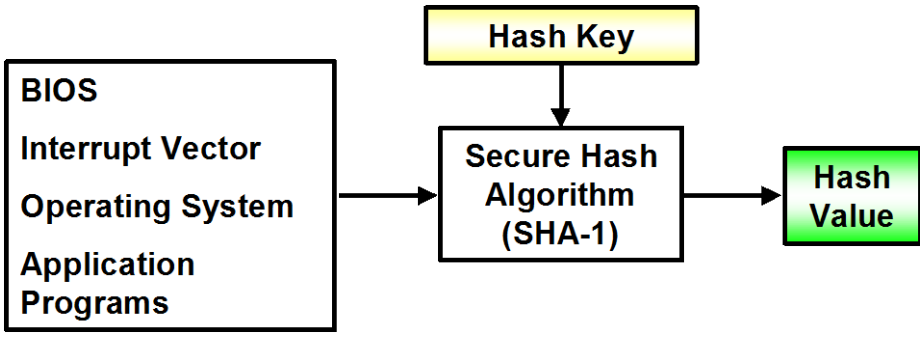

Figure 4. Firmware Integrity Verification Process

Seeds

The host and inspector independently generate random number seeds, which are stored on iButtons, to be used in the key generation process illustrated in Fig. 5. These seeds are connected to the black side of the trusted processor, and they are used as input to a pseudorandom number generator that calculates the private/public key pair that will be used to sign and verify the template file. The party that generates the seed will determine the manner that is used to generate the seed. Knowledge of only one of the random number seeds is not sufficient to allow either party to determine the private key.

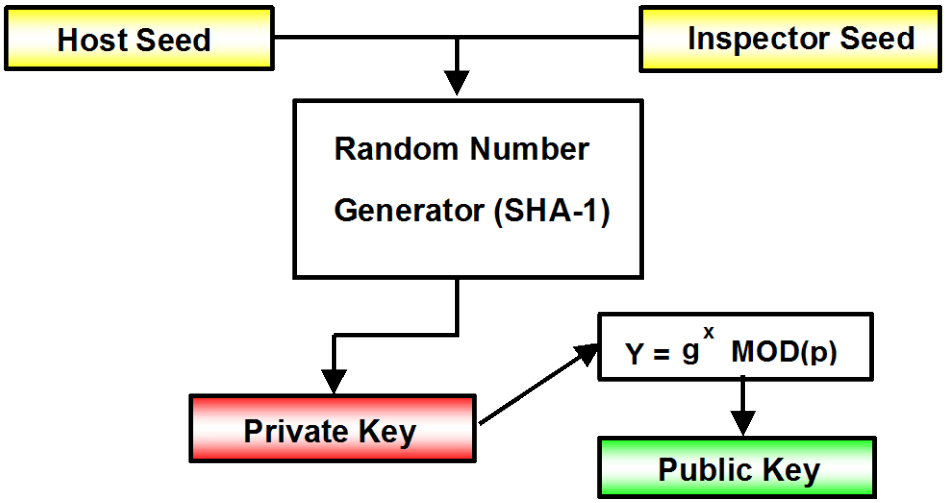

Figure 5. Process for Generating Private/Public Key Pair

Private Key

The private key is generated on the red side of the trusted processor using the SHA-1 algorithm as a pseudorandom number generator with the host- and inspector-provided random number seeds as input values. This private key is used to sign the template data file using the Digital Signature Algorithm (DSA) as illustrated in Fig. 6. The private key is stored in volatile random access memory (RAM) and disappears when power to the trusted processor is turned off.

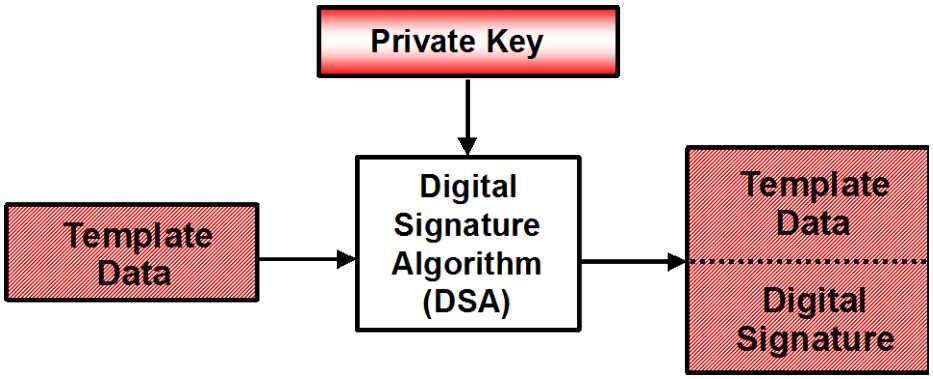

Figure 6. Signing the Template Data with the Private Key

Public Key

As illustrated in Fig. 7, the public key is used to verify the template signature. The public key is written to an iButton that is connected on the black side of the trusted processor during the template generation process. The public key is used to verify the template signature during the template confirmation process. The host and inspector can both know the public key since knowledge of the public key does not allow one to determine the private key.

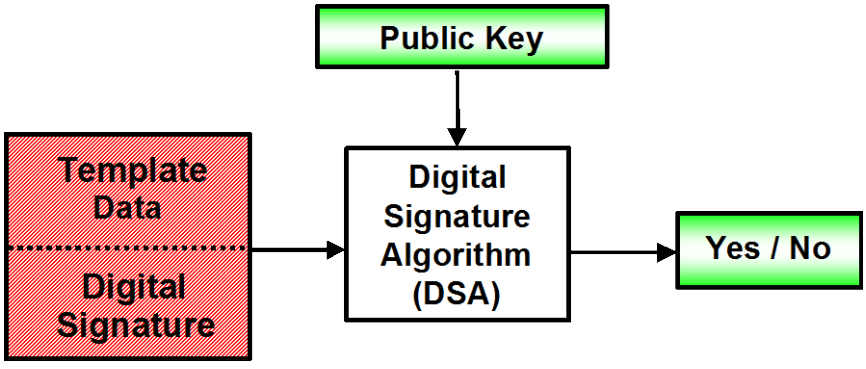

Figure 7. Verifying the Template Signature with the Public Key

Red-Black Communications

An important part of the TRIS information barrier is that communication between the red side and black side of the trusted processors, via the optical communications boards, is restricted to the passing of integer message codes. The user provides input to the black side via the hand-held I/O device, and an integer message code is sent to the red side to tell which function to execute. The black-side CPU only responds to message codes from the red-side CPU, and hard-coded messages associated with the received message code are displayed on the hand-held I/O device. This restriction has three exceptions, which all occur before items are measured or classified information is read by the red CPU:

1. The hash key is passed to the red-side CPU to perform the firmware integrity verification of the red side, and the red-side hash value is passed back to the black CPU for display on the hand-held I/O device.
2. The public key is passed from the red to the black CPU for storage on the black-side iButton in preparation for template generation.
3. The public key is read from the black-side iButton and passed to the red side in preparation for verification of the template signature during template confirmation.

Data Acquisition

The red-side CPU communicates with the MCA through the parallel port to record gamma-ray spectra. After setting the number of channels and the amplifier gain, a program running on the red-side CPU erases the MCA memory and starts the collection. The program examines the system clock of the red-side CPU and stops the collection after a fixed measurement time. The spectrum is written to a file on the red-side RAM disk.

Energy Calibration

Following measurement of a background spectrum, an energy calibration is performed. A program reads the gamma-ray spectrum and searches for peaks. If the detector and MCA are operating properly, the 239-keV and 2614-kev peaks associated with ^{232}Th present in the internal calibration source (i.e., thoriated welding rods) should always be identifiable. The gain and offset parameters are calculated using these values plus a correction for the intrinsic non-linearity of NaI detectors. If the calibration is successful, the background spectrum is rebinned to a fixed, 17-channel group structure. The calibration parameters and the 17-channel background spectrum are written to files on the RAM disk.

Template Generation

Following measurement of the foreground spectrum, a template file is created. The spectrum is rebinned to a fixed 17-channel, group structure. The net spectrum is then computed by stripping the data recorded in the background spectrum from the foreground spectrum. Statistical uncertainties are computed for the 17 energy groups by combining uncertainties for the foreground and background spectra. The net spectrum and the uncertainty array are written to a file on the RAM disk. This template file is digitally signed using the private key, and the signed template is stored on an iButton that connects to the red-side of the trusted processor.

Template Confirmation

During the template confirmation process, the signed template file created during the template generation process is read from an iButton connected to the red side of the trusted processor. Following successful verification of the template signature, the red-side CPU determines whether confirmation measurements are consistent with the template for an item of the declared type by performing the following actions. The energy calibration parameters and the foreground, background and template spectra are read from files on the RAM disk. The energy calibration parameters are used to rebin the foreground spectrum to the 17-channel group structure (the background and template spectra are already in this group structure). The variance array is equated to the sum of variances resulting from the statistical uncertainties of the foreground, background and template spectra. Additional uncertainties are added to the variance array to compensate for item-to-item differences associated with typical isotopic variations. The reduced chi-square, χ_r^2 is then computed to reflect differences between spectral shapes and intensities. If χ_r^2 is less than 4, the template is confirmed. The template is not confirmed for greater values of χ_r^2.

SUMMARY

TRIS has been developed at SNL to provide a means to generate and confirm radiation templates for classified components. TRIS incorporates "defense-in-depth" in the design of its information barrier to ensure protection of host-country classified information and inspector-country confidence in the host-supplied equipment via authentication. A divided hardware and firmware architecture isolates classified information from the unclassified output to facilitate certification of the measurement equipment for use with classified components. TRIS also employs cryptographic functions for authentication of both the firmware and the measured radiation templates.

REFERENCES

1. D. J. Mitchell, H. L. Scott, K. W. Marlow, and P. E. Havey, *Radiation Measurement System for Weapon Component Certification*, Systems Research Report, Sandia National Laboratories, Albuquerque, New Mexico, July 1994.
2. D. J. Mitchell and K. M. Tolk, *Trusted Radiation Attribute Demonstration System*, Proceedings of the 41st Annual INMM Meeting, New Orleans, LA, 2000.
3. B. Geelhood, PNNL; B. Bartos, NSA; R. Comerford, SO-222; D. Lee, DTRA/OSPCT; J. Mullens, ORNL; J. Wolford, LLNL; *Information Barrier Working Group Evaluation of TRADS with Particular Attention to Its Authentication Merits*, PNNL-13259, August 2000.
4. Joint DoD/DOE Information Barrier Working Group, *Functional Requirements for Information Barriers*, PNNL-13285, Pacific Northwest National Laboratory, Richland, WA, May 1999.
5. K. M. Tolk and G. C. Stoker, *Eddy-Current Testing of Welded Stainless Steel Structures to Verify Integrity and Identity*, Proceedings of the 40th Annual INMM Meeting, Phoenix, AZ, 1999.
6. K. M. Tolk and R. K. Rembold, *Verification of Operating Software for Cooperative Monitoring Applications*, Proceedings of the 38th Annual INMM Meeting, Phoenix, AZ, 1997.