SAND2019-6474C

Physical Encryption of Sensitive Gamma-Ray Templates

Michael Hamel

Sandia National Laboratories[1], Albuquerque, NM, USA

Prepared for the Institute of Nuclear Materials Management 60th Annual Meeting
Palm Desert, CA, USA
July 14-18, 2019

Abstract

A warhead template that is derived from a gamma-ray spectrum would be considered sensitive information if used in an arms-control application. Any system that captures spectral information, even if an information barrier is used, will have an associated risk of information loss. This work assesses the possibility of "physically encrypting" a template such that the gamma-ray spectrum measured by a system is no longer considered sensitive but can still be used to confirm the presence of a treaty accountable item (TAI). To ensure that the template does not contain sensitive information, a mixture of radioisotopes and intervening material could be measured with a TAI, which would obscure the true gamma-ray spectrum of the TAI. The radioisotopes in the encrypting source and intervening material would be chosen by the host such that a combined measurement with the TAI would not be considered sensitive information. This paper explores this concept and outlines potential procedures that could be used for its implementation.

Introduction: Warhead Verification Concepts

Future hypothetical arms-control agreements may seek to include technologies capable of confirming warhead or other TAI presence. Such a technology may be used to perform a measurement that provides a monitor confidence that the measured item is a TAI while also providing assurance to the host that no sensitive information about the TAI is transferred to the monitor. There are two main categories of technologies designed for TAI verification: Attribute measurements and template matching.

Attribute matching involves measurements of a TAI to confirm specific properties. An example of an attribute measurement could be a minimum mass estimate of nuclear material [1]. In this scenario, the verification technology would perform a measurement and then either confirm or not confirm that the agreed upon attribute is met. For a template matching technology, attribute definitions are not required. In this case, a template of a trusted TAI is measured and stored. That template is then used when subsequent TAIs are measured to either confirm or not confirm their authenticity.

A technical challenge for both attribute measurement and template matching technologies is that sensitive information about the TAI may be collected to confirm attributes or a template. To

[1] Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

protect this information and to only show the monitor the conclusion of a measurement, information barriers are used. With an information barrier, the system processes the sensitive information but does not reveal it. In addition to the information barrier, host confidence that sensitive information has not been passed to the monitor can be improved if the measurement device does not require the collection of sensitive information to perform its function. Techniques using this principle are often referred to as *zero-knowledge protocol* or *physical encryption* [2-4].

This paper presents an idea for physical encryption using the Trusted Radiation Identification System (TRIS), which is a template matching device that uses a gamma-ray spectrum as a template [5]. TRIS creates a template of a TAI by performing a gamma-ray measurement with NaI(Tl) and then subsequently uses that template to confirm TAIs that are declared to be the same as the original. Because attributes are not being measured, it may be possible to physically encrypt the signal measured by TRIS so that it no longer contains sensitive information, but in a manner that still allows it to be used for confirmation measurements.

To accomplish this physical encryption of the sensitive signal, a procedure is imagined in which the host is allowed to use other gamma-ray sources and intervening material (between the TAI and detector) that will change the spectrum in such a way in that it is no longer considered sensitive. This paper will introduce potential methods that could be used to accomplish the physical encryption as well as outline what procedures would look like in practice using TRIS as a template matching platform.

Trusted Radiation Identification System (TRIS)

The current iteration of TRIS is known as Next Generation TRIS (NG-TRIS) [6]. It consists of a NaI(Tl) detector attached to a *trusted processor*. The trusted processor is separated into a *red* side, which handles sensitive information, and a *black* side which acts as an information barrier and passes only approved messages to the user display. If NG-TRIS was used in an imagined TAI verification scenario, it would first collect and store a template of the TAI, before using that template to confirm other objects. The template is stored on a low memory storage device and has a digital signature applied to ensure that it is an authentic template when used for confirmation measurements. Other features of TRIS that are designed to give the host and monitor confidence include firmware authentication using a secure hash algorithm and a design that allows for indication of physical tampering. The concept proposed in this paper could be used with a device such as NG-TRIS and may provide improved host confidence because sensitive information would never be recorded by the template matching system in the first place.

Signal Encryption Methods

Two methods are proposed for physically encrypting the signal from a TAI such that TRIS does not record sensitive information. First, a mixture of radioisotopes could be measured along with a warhead or other TAI to change the measured spectrum. This method has the potential to obscure photopeaks present in the spectrum by using an encrypting source that has photopeaks of

a similar energy. This method could also be used to obscure ratios of radioisotopes. In this case, radioisotopes used in the encrypting source would also be present in the TAI.

As a second method, intervening material could be placed between TRIS and the TAI. The gamma rays emitted from the TAI would interact in the intervening material and change the collected spectrum. For example, gamma rays with less energy are attenuated at a greater rate than higher energy gamma rays. Other radiation interactions may occur in the material that produce gamma rays that would contribute to the spectrum collected by TRIS.

For both of these methods, constraints would likely be required on the encrypting source and intervening material to ensure that the TAI signal being measured isn't dominated by these additions. Another important consideration is the effect of the template matching routine performed by TRIS. The encrypting source and materials must not inhibit the confirmation of genuine TAIs.

Constraints and Monitor Verification

An encrypting source that is too strong could dominate the entire signal and would not provide confidence to the monitor. In practice, a maximum allowable encrypting source strength could be included as part of the verification regime. A non-spectroscopic radiation measurement, possibly performed with a Geiger counter, could provide the monitor confidence that the encrypting source activity is within allowable limits. This task would likely require the Geiger counter to undergo inspection procedures such that both the host and monitor have confidence in its operation. Chain-of-Custody (CoC) methods could be employed for the encrypting source once it has been determined to be allowable because it will need to be used again for confirmation measurements. Considerations for the decay of the encrypting source would also need to be taken into account with the timeline of verification activities and CoC procedures. If the radioisotopes in the encrypting source decay a significant amount between template creation and TAI confirmation measurements, TRIS may not confirm what would be genuine TAIs.

For intervening material to encrypt the signal, a container of a specific size could be placed in between the TAI and the TRIS detector. The size of the container would bound the amount of material that could be included in the container. It would be the choice of the host to decide on the material composition, density, and amount. The size of the container, and a finite number of chemical elements bounds the minimum and maximum attenuation that the intervening material will provide. After use in template generation, this container could be placed under CoC for use in confirmation measurements.

Imagined Procedures

The procedures required for implementation of this concept must take into account several considerations. When considered individually, it is likely that a spectrum of the encrypting source would be considered sensitive information just like the TAI because a known spectrum could be subtracted from the overall measurement. However, when the TAI, encrypting source, and intervening material are all present, it is possible that a radiation measurement taken in the

proper location would not be considered sensitive. A such, TRIS should not be brought into the area that measurements will occur until the TAI, encrypting source, and intervening material are all in the proper locations. The intervening material should not be considered visually sensitive because it is placed inside a container that the monitor will not see inside. The monitor however, would likely be precluded from handling the container as that might provide information as to the amount of material in the container. Potential procedures for implementation follow. The procedures were developed assuming that the monitor would not be allowed to physically touch anything. As such the host will perform all physical actions while the monitor observes. When CoC is referenced, a tamper indicating enclosure (TIE) could be used with a seal.

Template Collection

1. Place encrypting source and intervening material in correct location
2. Place trusted TAI in correct location
3. Verify that encrypting source and intervening material are in the correct locations
4. Place TRIS in correct location
5. Operate TRIS to collect and store template
6. Place template key under CoC
7. Remove TRIS and place under CoC
8. Remove TAI from location
9. Verify that encrypting source is allowable
10. Verify that container for intervening material is allowable size
11. Place encrypting source under CoC
12. Place intervening material under CoC

Confirmation Measurements for two TAIs

1. Verify CoC on encrypting source
2. Remove encrypting source from TIE
3. Re-verify that encrypting source is allowable
4. Place encrypting source in correct location
5. Verify CoC on intervening material
6. Remove intervening material from CoC
7. Re-verify that container for intervening material is allowable size
8. Place intervening material in correct location
9. Place TAI in correct location
10. Verify CoC on TRIS template key
11. Remove template key from TIE
12. Place TRIS in correct location
13. Operate TRIS to confirm TAI
14. Remove TRIS
15. Remove first TAI
16. Place second TAI in correct location
17. Return TRIS to correct location

18. Operate TRIS to confirm TAI
19. Remove TRIS and place under CoC
20. Remove second TAI
21. Place encrypting source under CoC
22. Place intervening material under CoC

Summary and Future Investigation

This paper presents a concept that could offer improved confidence in a template matching regime that could be used as part of a future hypothetical arms-control agreement that includes warhead verification. The concept involves the use of radioisotopes and intervening material that would physically encrypt the gamma-ray signal emitted from a TAI such that a template matching device like TRIS never collects sensitive information. Imagined procedures that could be used to implement this concept were created to ensure that items that would be considered sensitive if measured individually such as the TAI and the encrypting source are never alone in the presence of TRIS. The procedures also include steps for CoC that could be implemented.

Future work on this topic will seek to determine its feasibility. Specifications such as allowable encrypting source properties and allowable amounts of intervening material will be studied as well as performance of the template matching routine when used with encrypting sources and intervening material.

References

[1] D. J. Mitchell and K. W. Marlow, "Minimum Mass Estimates for Plutonium Based on the Peak Intensities and Scattered Radiation in HPGe Spectra," Sandia Report, SAND2002-3426P, October 13, 1999.

[2] S. Kemp et al., "Physical cryptographic verification of nuclear warheads," Proceedings of the National Academy of Sciences of the United States of America 113, no. 31, pp. 8618-23, 2016, doi:10.1073/pnas.1603916113.

[3] A. Glaser et al., "A zero-knowledge protocol for nuclear warhead verification," Nature 510, pp. 497-502, June 2014, doi:10.1038/nature13457.

[4] P. Marleau and R. Krentz-Wee, "Investigation into Practical Implementations of a Zero Knowledge Protocol," Sandia Report, SAND2017-1649, February 2017.

[5] K. D. Seager et al., "Trusted Radiation Identification System," Proceedings of the INMM 42nd Annual Meeting, 15-19 July, Indian Wells, CA, USA, 2001.

[6] P. B. Merkle et al., "Next Generation Trusted Radiation Identification System," Proceedings of the INMM 51st Annual Meeting, 11-16 July, Baltimore, MD, USA, 2010.