LA-UR-12-21844
Approved for public release; distribution is unlimited.

Title: Simultaneous Authentication and Certification of Arms-Control Measurement Systems

Author(s): MacArthur, Duncan W.
Hauck, Danielle K.
Thron, Jonathan L.

Intended for: INMM Annual Meeting, 2012-07-15 (Orlando, Florida, United States)

SIMULTANEOUS AUTHENTICATION AND CERTIFICATION OF ARMS-CONTROL MEASUREMENT SYSTEMS

Duncan MacArthur, Danielle Hauck, and Jonathan Thron
Los Alamos National Laboratory
PO Box 1663, MS E540, Los Alamos, NM 87545, USA

ABSTRACT

Most arms-control, treaty-monitoring scenarios involve a host party that makes a declaration regarding its nuclear material or items and a monitoring party that verifies that declaration. A verification system developed for such a use needs to be trusted by both parties. The first concern, primarily from the host party's point of view, is that any sensitive information that is collected must be protected without interfering in the efficient operation of the facility being monitored. This concern is addressed in what can be termed a "certification" process. The second concern, of particular interest to the monitoring party, is that it must be possible to confirm the veracity of both the measurement system and the data produced by this measurement system. The monitoring party addresses these issues during an "authentication" process. Addressing either one of these concerns independently is relatively straightforward. However, it is more difficult to simultaneously satisfy host party certification concerns and monitoring party authentication concerns. Typically, both parties will want the final access to the measurement system. We will describe an approach that allows both parties to gain confidence simultaneously. This approach starts with (1) joint development of the measurement system followed by (2) host certification of several copies of the system and (3) random selection by the inspecting party of one copy to be used during the monitoring visit and one (or more) copy(s) to be returned to the inspecting party's facilities for (4) further hardware authentication; any remaining copies are stored under joint seal for use as spares. Following this process, the parties will jointly (5) perform functional testing on the selected measurement system and then (6) use this system during the monitoring visit. Steps (1) and (2) assure the host party as to the certification of whichever system is eventually used in the monitoring visit. Steps (1), (3), (4), and (5) increase the monitoring party's confidence in the authentication of the measurement system.

THE VERIFICATION CHALLENGE

Most treaty monitoring scenarios can be reduced to two requirements:

(1) The owner (the host party) of nuclear material or a device makes a declaration concerning that item to another entity (the monitoring party).

(2) The monitoring party must verify this declaration without observing any sensitive information.

The crux of the treaty-monitoring problem lies with the final phrase "without observing any sensitive information." Traditional nondestructive assay (NDA) techniques (based on gamma-ray detection, neutron detection, or calorimetry) are widely and successfully used in numerous scenarios (e.g., waste assay and spent fuel monitoring) that do not involve sensitive information. [1] The host party and the monitoring party can use NDA instrumentation, either jointly or separately, to observe all relevant information concerning the nuclear material (or waste) in a sealed container.

This relatively simple measurement scenario breaks down if a sensitive nuclear item is present in the measurement system. In this case, even though the NDA instrumentation may be similar or identical, the output cannot be shared directly with the monitoring party. One way of protecting the sensitive information is to introduce an information barrier (IB) that surrounds the sensitive material and any measuring electronics that might contain sensitive information [2]. A practical IB includes layers of hardware, software, and procedural protection to provide a barrier system that, as a whole, is fault resistant and the components of which are fault tolerant. This approach results in a sensitive information measurement system that is not prone to single-point failures [3].

Unfortunately, the same IB system that excels at protecting the host party's sensitive information also excels at "protecting" the monitoring party from any information that could be used to confirm the host party's declaration. Some non-sensitive information release is required to give the monitoring party any confidence at all. One way to allow a carefully controlled information release from inside the IB is to use the attribute measurement technique in an attribute measurement system (AMS). [4] Attributes, as measured in an AMS, are non-sensitive indicators of potentially sensitive measurement results. Potentially sensitive information can be made into an attribute by comparing the information with a threshold (i.e., the attribute is "quantity above threshold"). In any fielded implementation of an AMS, the host and monitoring parties would agree on the attributes to be measured (as well as on the details of the AMS itself).

CERTIFICATION AND AUTHENTICATION

Certification can be generally defined as *"A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system."* [5] This definition is more general than is needed in a treaty-verification environment, but the principles are still valid in this case. The host party is most concerned that sensitive information, about either the treaty limited item (TLI) or the facility, not be released during an inspection visit.

Authentication has been defined in this context as *"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."* [6] This definition is much more focused on treaty verification. The monitoring party is concerned with the veracity of the (small amount of) information presented to them by the measurement system.

If we assume the existence of a negotiated treaty or agreement between the two parties, it follows that both parties are officially and unofficially committed to that agreement. The case where one or both parties are not committed to the agreement is beyond the scope of this paper and will not be considered here. This commitment implies that designers from the host, although primarily concerned with certification, will also be willing to listen to authentication concerns. Similarly, designers from the monitoring party, although primarily concerned with authentication, will also be receptive to certification concerns. We are not suggesting that either party should act against their best interests,

but only that both parties will be motivated to see the agreement succeed and that such success can only occur if both parties are satisfied.

In such a bilateral agreement, we assume that the host party performs certification and all certification-related activities and that the monitoring party performs authentication and all authentication-related activities. Both parties are equally concerned with system reliability as both have an equal stake in the success of the agreement. In a trilateral agreement, some or all, of the responsibilities of the monitoring party may be assumed by a third party such as the IAEA.

At first glance, there is a seeming asymmetry between the required confidence levels. The host party requires total confidence in certification of the measurement system while the monitoring party requires only "appropriate" confidence in authentication. Two factors work against this apparent asymmetry:

1) Most treaties and agreements are reciprocal in nature. The host party during one monitoring visit will be discouraged from taking unnecessary advantage of their role by the knowledge that they will be the monitoring party in an upcoming reciprocal visit.
2) Either party can veto the design of the measurement system. If the system does not simultaneously meet the needs of both parties, the system will not be used for treaty verification. In this sense, the needs of the monitoring party are equally valued to those of the host.

DESIGN FOR AUTHENTICATION AND CERTIFICATION

Although it would appear on the surface that certification and authentication are antagonistic, in terms of design, authentication design principles and certification design principles are remarkably similar. Below are a number of techniques potentially useful in design for authentication and design for certification. The majority of these appear on both lists and none of these will be actively opposed by the other party; however, the two parties will place different emphases on the various items on the list.

Design for Authentication— At a high level, design for authentication can be expressed as two general requirements:

1) Make sure that the necessary authentication access is included the system design. Authentication access can include physical features like windows in cabinets and simple circuit layout; chain of custody (CoC)-related technologies like tamper-indicating enclosures (TIEs), and design aspects for mitigating human-factors issues such as extra such as extra large indicator lights and ease of data retrieval. In a joint design, the host will be placing similar certification enablers in the design. As noted below the certification and authentication enablers will be the same in many cases.
2) Do not allow the host to put "black boxes" into the system design. In this case a black box is any element of the design (mechanical, electrical, procedural, etc.), either overt or covert, that is not fully transparent and understood by the inspecting party. The host will probably have a similar requirement disallowing any "monitor-supplied" black boxes.

Starting from a list of general AMS design principles; we have crossed out the two that pertain only to certification to generate Table 1. Note that neither of these principles is necessarily inimical to authentication – the monitoring party just doesn't have these requirements.

Table 1. Design principles for design for authentication.

- Modularity
- Simplicity in design
- Transparency and Open design
- Minimal Functionality
- Fully inspectable components
- Simple communication between modules
- Details of the Information Barrier
- Protection from unauthorized access
- ~~Failure modes which do not release sensitive or classified information~~
- Tamper-indicating features
- ~~The system shall be unclassified at rest (i.e. when powered down). No components of the system shall store any classified or sensitive information that remains when the system is powered down.~~
- Complete documentation (sufficient detail that an independent party could replicate the system).
- Equipment should be designed to inhibit extraneous signal transmission, including: Radio Frequency, Ultra Violet/Infrared, acoustic signal, or other energy.
- A complete set of procedures for all aspects of the system.

Design for Certification— At a similarly high level, design for certification can be expressed as the same two general requirements (although the examples are different):

1) Make sure that the necessary certification access is included in the system design. Certification access can include choices for components, circuits, and software as well as overall system layout. In a joint design, the monitoring party will be placing similar authentication enablers in the design. As noted above the certification and authentication enablers will be the same in many cases.
2) Do not allow the monitoring party to put "black boxes" into the system design. In this case a black box is any element of the design (mechanical, electrical, procedural, etc.), either overt or covert, that is not fully transparent and understood by the host party. The monitoring party will have a similar requirement disallowing any "host supplied" black boxes.

Starting with the same list of general AMS design principles; we have crossed out the two that pertain only to authentication to generate Table 2. Note that neither of these principles is necessarily inimical to certification – the host party has similar requirements that are largely satisfied by the location of the monitoring system within the host facility.

Table 2. Design principles for design for certification.

- Modularity
- Simplicity in design
- Transparency and Open design
- Minimal Functionality
- Fully inspectable components
- Simple communication between modules
- Details of the Information Barrier
- ~~Protection from unauthorized access~~ (see discussion below)
- Failure modes which do not release sensitive or classified information
- ~~Tamper-indicating features~~ (see discussion below)
- The system shall be unclassified at rest (i.e. when powered down). No components of the system shall store any classified or sensitive information that remains when the system is powered down.
- Complete documentation (sufficient detail that an independent party could replicate the system).
- Equipment should be designed to extraneous signal transmission, including: Radio Frequency, Ultra Violet/Infrared, acoustic signal, or other energy.
- A complete set of procedures for all aspects of the system.

This isn't intended to say that host and monitor concerns are identical. The host party is very concerned with anything relating to sensitive information; i.e. non-sensitive failure modes of measurement systems and designing systems that do not contain sensitive information in the rest state. The monitoring party may be peripherally concerned; either from a Nuclear Nonproliferation Treaty (NPT) point of view or from a reciprocity point of view, but sensitive information is not a primary monitoring party concern.

However the monitoring party is very concerned with controlling access to the measurement system. The host also has access control concerns, but these concerns are greatly reduced by the location of the measurement system in a host-controlled facility within the host country. On the other hand, it is extremely difficult for the monitoring party to maintain CoC within the host facility, so features such as tamper indicating devices (TIDs) and TIEs are of special interest to the monitoring party.

APPROACHES TO MEASUREMENT SYSTEM DEVELOPMENT

In a traditional development scenario, one party designs and builds a measurement system and convinces themselves that it is functioning correctly. The other party must then convince themselves of correct functioning without causing the first party to loose confidence. This type of development is used when one of the parties is driving the agreement. Most IAEA safeguards inspections are examples of an "inspector-driven" regime. In this case, the inspecting party designs, builds, and authenticates the measurement system and then the host is given an opportunity to certify the system. Second-generation attribute measurement systems, such as the FMTTD, [7] are examples of "host-driven" system design. In this case, the host party designs, builds and certifies

the measurement system and then the monitor is given an opportunity (often very constrained) to authenticate the system.

Addressing either party's concerns independently is relatively straightforward. However, it is more difficult to simultaneously satisfy host party certification concerns and monitoring party authentication concerns. Typically, both parties will want the final access to the measurement system. We describe an alternative approach that allows both parties to gain confidence simultaneously. This approach starts with (1) joint development of the measurement system followed by (2) host certification of several copies of the system and (3) random selection by the inspecting party of one copy to be use during the monitoring visit and one (or more) copy(s) to be returned to the inspecting party's facilities for (4) further hardware authentication; any remaining copies are stored under joint seal for use as spares. Following the selection process, the parties will jointly (5) perform functional testing on the selected measurement system and then (6) use this system during the monitoring visit. Steps (1) and (2) assure the host party as to the certification of whichever system is eventually used in the monitoring visit. Steps (1), (3), (4), and (5) increase the monitoring party's confidence in the authentication of the measurement system.

Joint Development (1)— In a treaty verification scenario, both the host and the monitoring parties are driving system requirements simultaneously. It is difficult to achieve certification and authentication simultaneously in a traditionally developed system. In a jointly developed measurement system, [8] both parties develop the design together, the two parties collaborate as much as possible on fabrication and testing of the system, and both parties obtain identical "gold copies" of the system based on agreed design. In this scenario, both parties are intimately familiar with design and capabilities of measurement system. This development technique allows simultaneous design for both authentication and certification.

Random Selection (3)— In a scenario involving measurements on a nuclear treaty limited item (TLI), both the host party and the monitoring party will insist on having the last private inspection (for certification and authentication respectively) of the measurement system. If the measurement system itself cannot be inspected then a random selection technique [9] can be used to generate monitoring party confidence while allowing the host to maintain certification of the measurement system. The random selection process as applied to authentication consists of several selections:
a) The monitoring party chooses one of the "pre-certified" systems or components to be used in treaty verification.
b) The monitoring party also chooses one (or more) of these systems or components for off-site inspection in a monitoring party's facility.
c) The treaty inspection is performed using the randomly selected (by the monitor) but still certified (by the host) measurement system.
The success of this technique depends on the host maintaining CoC of the actual measurement system from the time it was certified until the time of the inspection. The monitoring party must maintain CoC on the measurement system from the time of random selection until the time of the inspection as well as maintaining CoC on the verification system from the time of selection until the system arrive at the monitor facility.

Functional Testing (5) — In this context, we can define functional testing as the testing that occurs on the agreed measurement system within the host facility. This testing will probably occur shortly before a treaty verification measurement. The traditional method for testing a measurement system

is to use the system to measure the characteristics on an unknown (to the system and its designer) radioactive source. In our case, this method is greatly complicated by the facts that the "sources" measured by an AMS are multi-kg quantities of Special Nuclear Material and that all measurements must take place in the host-controlled facility. It is possible, although not simple, to generate host-owned and monitor-trusted calibration standards. It is difficult to conceive of a method for placing one of these standards within the AMS without the host knowing which standard was being used. Another possibility is the creation of a pulse generator that would generate switchable neutron and/or gamma signals. Such a pulse generator could be used to authenticate the AMS equipment with the exception of the detectors themselves. The ramifications, authentication, and constraints on the use, of either isotopic sources or pulse generators have not been examined in detail.

PUTTING IT ALL TOGETHER

All of the authentication and certification techniques proposed above can be illustrated schematically as shown in Fig. 1. This type of development and use scenario would all the host and monitoring parties to simultaneously gain confidence in a monitoring system.

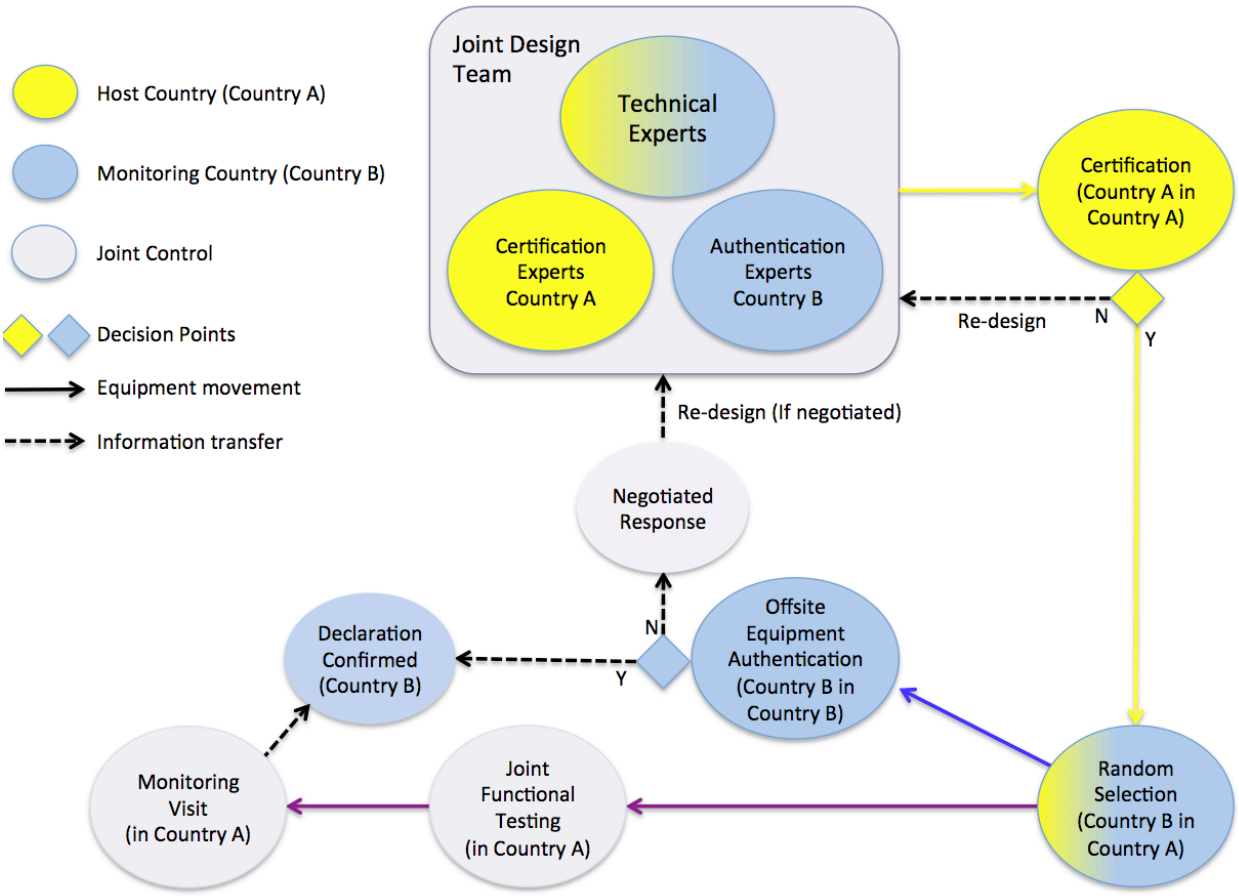

Figure 1. Proposed implementation of random selection to achieve simultaneous certification and authentication of a measuring system.

FUTURE DIRECTIONS

We have proposed a procedure to allow simultaneous authentication and certification of a treaty verification measuring system. Implementation of this, or a similar, approach will require further development in a number of authentication-related areas:

1) Joint development has been partially demonstrated in the AVNG project described elsewhere. [10] This development technique can be very effective in convincing the monitoring party as to the capabilities of the measurement system and limited display. However, as was mentioned in Ref. [8], the AVMP project explored some of the issues involved with joint development rather than being a true joint development.
2) Random selection can be a powerful method for reassuring the monitoring party of the veracity of a measurement system that they (the monitoring party) are not allowed to directly authenticate. However, random selection, and the requisite CoC, carried to extremes, can be cumbersome and expensive. The trade-off between additional confidence and cost needs to be more fully explored. Although the term "random selection" is often invoked, the operational practicalities are not well understood.
3) Off-site hardware authentication gives the monitoring party the opportunity to subject an identical measurement system to any desired test. The simplest, and potentially very useful, is simply to determine whether the system exactly matches the documented design.
4) On-site functional testing is a staple of more traditional authentication approaches. However, in a warhead-monitoring scenario, the amount of allowed testing may be severely limited. To the best of the authors' knowledge, there has been no comprehensive study of allowable on-site testing methods.

ACKNOWLEDGMENT

This work is supported by the United States National Nuclear Security Administration's Office of Nuclear Verification.

REFERENCES

These references are intended, not as a review of all work done in the field, but rather as additional information on background material directly related to this paper.

1. Doug Reilly, Norbert Ensslin, Hastings Smith Jr., and Sarah Kreiner "Passive Nondestructive Assay of Nuclear Materials" *US Nuclear Regulatory Commission, NRC FIN A7241, 1991*.
2. Duncan W. MacArthur, Rena Whiteson and James K Wolford, Jr., "Functional Description of an Information Barrier to Protect Classified Information," *Proceedings of the INMM 40th Annual Meeting, Phoenix, AZ, July 25-29, 1999*.
3. Rena Whiteson, Duncan W. MacArthur, and Robert P. Landry, "Functional Specifications for a Prototype Inspection System and Information Barrier", *Los Alamos National Laboratory Publication LA-UR-99-1174, March 1999*.

4. Diana Langner, Robert Landry, Sin-Tao Hsue, Duncan MacArthur, Doug Mayo, Morag Smith, Nancy Jo Nicholas, Rena Whiteson, Thomas B. Gosnell, Zachary Koenig, S. John Luke, James Wolford, "Attribute Measurement Systems Prototypes and Equipment in the United States," *Proceedings of the INMM 42nd Annual Meeting, Indian Wells, CA, July 15-19, 2001*.

5. FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems,* http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

6. The Joint DOE-DoD Authentication Task Force, "Guidelines for Authenticating Monitoring Systems," June 24, 2001.

7. http://www.lanl.gov/orgs/n/n1/FMTTD/index_main.htm

8. Duncan W. MacArthur, " Joint Development: Technical Considerations and Past Experience," *Proceedings of the INMM 52nd annual meeting, Palm Desert, CA, July 17 – 21, 2011*.

9. Duncan MacArthur, Danielle Hauck, Diana Langner, Morag Smith, and Jonathan Thron, "Random Selection as a Confidence Building Tool," *Proceedings of the INMM 51st annual meeting, Baltimore, MD, July 11-15, 2010*.

10. 2010 INMM Special Session—Nonproliferation and Arms Control—The Russian AVNG Attribute Measurement System (A total of nine papers by M. Smith, D. MacArthur, S. Razinkov, J. Thron, S. J. Luke, A. Livke, and S. Kondratov), *Proceedings of the 51st INMM Annual Meeting, Baltimore, MD, July 11-15, 2010.*