LA-UR-12-22774
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, 2012-07-15/2012-07-19 (Orlando, Florida, United States)

Simultaneous Authentication and Certification of Arms-Control Measurement Systems

Duncan W. MacArthur, Danielle Hauck, Jonathan Thron

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 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 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.

Simultaneous Authentication and Certification of Arms-Control Measurement Systems

Duncan MacArthur, Danielle Hauck,
and Jonathan Thron

LA-UR-12-xxxxx

Treaty Verification

- Host party makes a declaration regarding its nuclear material or items and
- Monitoring party verifies that declaration.

- Measurement system

Trusted Measurement System

- Host concern: Any potentially sensitive information that is collected must be protected. (Certification)
  - Direct information (Treaty Limited Item)
  - Corollary information (Facilities and procedures)
- Monitoring party concern: It must be possible to confirm the veracity of the measurement. (Authentication)
  - The measurement system
  - The data produced by this measurement system

Certification

"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."

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

Authentication

"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."

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

Certification & Authentication are Complementary

- Negotiated treaty or agreement
- Assume that both parties are officially and unofficially committed to the agreement

- Certification performed by Host party
- Authentication performed by Monitoring party
- Both parties are concerned with system reliability

Confidence Levels

- Host requires total confidence in certification
- Monitor requires “appropriate” confidence in authentication
- Seeming asymmetry, but
- Either party can “veto” the system design

- Perception vs. reality

Design for Certification

- Access for certification
  - Simplicity
  - Modularity
  - Shared access points,
  - Not shared certification procedures.
- No monitor supplied “black boxes”
  - Transparency
  - No secret keys
- Version control
  - Documentation
  - Procedures
  - Chain of Custody (CoC)

Design for Authentication

- Access for authentication
  - Simplicity
  - Modularity
  - Shared access points,
  - Not shared authentication procedures.
- No host supplied “black boxes”
  - Transparency
  - No secret keys
- Version control
  - Documentation
  - Procedures
  - CoC

Design Concerns are not Completely Identical

- Host concerns
  - Non-sensitive failure modes
  - Non-sensitive at rest
- Monitoring party concerns in a host facility
  - Tamper indicating features
  - Access control
- Two parties to an agreement
  - Not necessarily a conflict between parties, but
  - A conflict between traditional approaches
  - Both parties want the last possession of the measurement system

Who gets it last?

- Traditional approach
  - Monitor-centric: we build it; we get it last
  - Host-centric: we build it; we get it last
- Treaty verification
  - Can't both have it last
  - And by the way: we don't want you to build it
- An alternative approach
  - Joint development
  - Certification
  - Random selection
  - Off-site hardware authentication
  - On-site functional testing

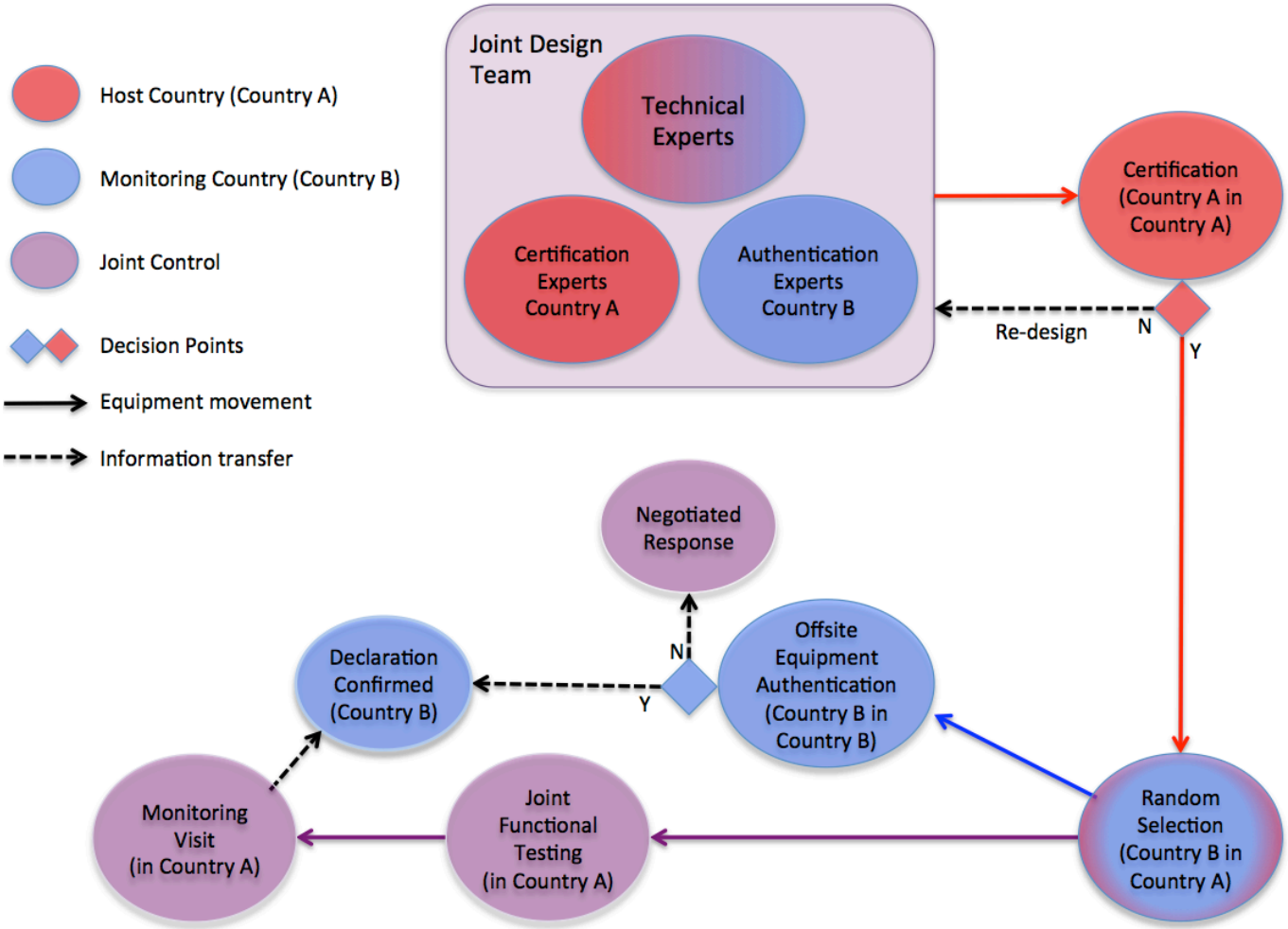
Joint Development

- Both parties jointly develop design
  - Design is specific to use in host country. Both classification guidance and facility requirements may be different in different countries.
  - Design for certification and authentication
- Both parties have identical copies of agreed design
- Both parties are intimately familiar with monitoring system
  - Design
  - Construction
  - Capabilities
  - Limitations

Random Selection

- Motivation – Enable the monitoring party to authenticate a measurement system without destroying the host party's certification of that system.
- Simple in concept
  - Several "identical" certified copies of a component or system are presented to the monitoring party
  - One (or more) is randomly chosen for use in the measurement system
  - One (or more) is randomly chosen for off-site authentication
  - If the two remain identical, authentication of the "authentication copy" is equivalent to authentication of the measurement system
  - But the devil is in the details
- CoC of all copies

Joint Development and Random Selection



The 3G-AMS and Authentication

- Joint development
  - Can be very effective
  - Partially tested
- Random selection process
  - The section itself is the tip of the iceberg
  - Can be cumbersome and expensive
- Off-site hardware authentication
  - Does the system match the design?
  - Whatever the monitoring party wants
- On-site functional testing
  - What is possible?
  - Must be negotiated