SAND2008-2065C

The Impact of Safeguards Authentication Measures on the Facility Operator

Keith Tolk, Peter Merkle
Sandia National Laboratories[1], PO Box 5800, Albuquerque, New Mexico, USA 87185
kmtolk@sandia.gov, pbmerkl@sandia.gov

Massimo Aparo
International Atomic Energy Agency, 5-9 Iidabshi 1 Chome, Chiyoda-Ku Tokyo 102
Japan
m.aparo@iaea.org

Abstract

In order for the IAEA to draw valid safeguards conclusions, they must be assured that the data used to draw those conclusions are authentic. In order to provide that assurance, authentication measures are applied to the safeguards equipment and the data from the equipment. These authentication measures require that IAEA personnel have direct electronic and physical access to the equipment and severely limit access to the equipment by the operator. Providing the necessary access for the IAEA personnel can be intrusive and potentially disruptive to plant operations. If the equipment is to be used jointly by the operator and the IAEA, the authentication measures can cause difficulties for the operator by limiting his ability to repair and maintain the hardware. In many cases, tamper indicating conduit and enclosures are also required. The installation, sealing, and inspection of this tamper indicating hardware also add to the intrusiveness of the safeguards activities and increase the cost of safeguards. This paper discusses these impacts and proposes methods for mitigating them.

Key Words: International Safeguards, Authentication

Introduction

As facilities become larger and more highly automated, more unattended and remote monitoring systems will be necessary for safeguards. These systems reduce the need for inspector visits and thus the impact of routine safeguards activities on both the operator and the IAEA. Without careful implementation, the authentication measures required to provide the IAEA with data assurance may significantly increase installation costs and impede facility operations. These operator burdens can be reduced through consideration of authentication needs early in a facility's safeguard system design process.

Unattended and remote monitoring systems support the mission of the IAEA to verify Member State commitments to use nuclear material and facilities for peaceful purposes

8th International Conference on Facility Operations – Safeguards Interface, March 30 – April 4, 2008, Portland, OR, on CD-ROM, Danielle Peterson, Pacific Northwest National Laboratory, Richland, WA 99352 (2008)

only. An IAEA objective is to establish an integrated and effective verification system which can be more widely and efficiently applied throughout the world. This verification system will use advanced monitoring technologies and secure data communications to augment and replace some manual on-site inspection activities with more efficient, authenticated electronic containment, surveillance, and accounting methods. This will enhance safeguards effectiveness while minimizing resource requirements and the imposition of additional burdens on Member States. It will permit more locations to be monitored for longer periods of time, and an increase in the number of variables monitored. The adoption of standard data formats will facilitate easier data management and promote the use of standard review software. Without robust authentication measures, few benefits of unattended and remote monitoring systems are available.

Equipment Security and Authentication

The term "authentication" can be confusing, since it takes on different meanings in different situations. It can refer to a cryptographic process in which a digital signature used to verify the authenticity of a piece of data is calculated and incorporated into the data set. It can also refer to the inspection process used to verify that a piece of equipment has not been altered and is therefore still "authentic". It also has other meanings in other contexts. In this paper, the term "authentication" will be used to refer to the entire process of verifying that a system is secure and can be trusted to provide data that accurately reflects conditions at the monitored facility without concerns that an adversary could manipulate the equipment or the data to produce false results. The terms "data authentication" or "authenticated data" will refer to the cryptographic processes of adding a digital signature or message authentication code to the data.

Equipment security is essential for authentication processes. The foundation of equipment security is the implementation of a life-cycle approach, beginning with the initial conceptual design phase and continuing through to the decommissioning of security critical modules. It is difficult, if not impossible, to increase the security of equipment that has not been designed to meet defined security performance requirements. For this reason, safeguards equipment security requirements must be formally integrated with the design process from initial concept to prototype development and construction. An earlier paper[2] discusses the process of designing safeguards systems for authentication in some detail.

Successful design and installation of data authentication involves specific approval procedures[3]. Before any equipment can be authorized for safeguards use, the IAEA requires either a Vulnerability Review (VR) by IAEA experts or a Vulnerability Assessment (VA) of the design or actual system by an outside party. In these vulnerability studies, the assumed adversary is the facility operator with the support of the host nation. This type of "insider" adversary is extremely formidable, driving the need for system authentication architectures that are verifiably robust against all forms of tampering and subversion. The formal vulnerability reviews are performed to identify security flaws before safeguards equipment is installed, to avoid costly retrofitting and facility disruption.

8th International Conference on Facility Operations – Safeguards Interface, March 30 – April 4, 2008, Portland, OR, on CD-ROM, Danielle Peterson, Pacific Northwest National Laboratory, Richland, WA 99352 (2008)

A good authentication design will incorporate features to protect both equipment and data from tampering and subversion. The IAEA's fundamental authentication requirements address both hardware and software components; additional authentication measures may be needed in specific cases. An essential authentication measure is tamper indication to ensure that any attempt to alter equipment or to introduce falsified data is detected. All sensors, cables carrying raw data, stored cryptographic keys, equipment cabinets that are processing unauthenticated data, and all other security critical components must be sealed inside a tamper indicating enclosure (TIE) or tamper indicating conduit.

The failure to consider tamper-indicating enclosure requirements can be extremely expensive and disruptive to operations. In one example, a safeguards system was designed with long cable runs between the sensors and the electronics that digitized the data. These cables were not enclosed in tamper indicating conduit during facility construction. When this flaw was discovered, several hundred meters of the proper conduit had to be retrofitted into the facility. Since the conduit lengths had to be limited to allow the cable to be pulled through the conduit, sealed junction boxes were also required. Installation costs in the facility were much higher than they would have been had the conduit been installed during initial construction. If the monitoring system had been designed with the digitizing electronics closer to the sensors, the installation of much of the conduit could have been avoided, and both the operator and the IAEA could have avoided the costly inspection of the conduit and junction box seals.

An inspection plan that includes a systematic and random physical inspection of all tamper indicating surfaces is also needed. Each inspection requires an inspector to enter the facility under escort to gain access to the surfaces, which are often in places that are difficult to inspect, including areas that might require erection of scaffolding. Of course, these inspections are very intrusive and expensive, both for the IAEA and for the operator.

Cryptographic authentication must be applied on all data before transmittal outside a tamper indicating enclosure. This prevents data substitution by the adversary. Data that will not be shared must also be encrypted. One method of minimizing the area of tamper indicating surfaces to be inspected is to apply cryptographic data authentication and encryption as close to the sensor as possible. Data that has been properly authenticated can be transmitted through unprotected cables without concern of an adversary introducing false data records, and in many cases the computers storing the data also do not require seals. In at least one installation, the authenticated data is transmitted over the host country's network and stored on their computers.

Equipment when not in use must always be sealed in a TIE when there is any possibility that unauthorized persons might gain access to it. This requirement includes shipment, storage outside IAEA approved storage locations, and during its installation, decommissioning and routine inspection use. Protecting the equipment in locked cabinets is not adequate unless other equivalent security measures are in place, or unless

8th International Conference on Facility Operations – Safeguards Interface, March 30 – April 4, 2008, Portland, OR, on CD-ROM, Danielle Peterson, Pacific Northwest National Laboratory, Richland, WA 99352 (2008)

the lock and cabinet have been certified for use as a TIE. Without such enclosures, the adversary can subtly alter hardware and software or undetectably extract and analyze safeguards information to compromise the system's integrity.

All safeguards equipment systems must have a security plan, including a recovery plan outlining the procedures required to reestablish the authenticity of the system if its security may have been compromised.

Note that data authentication benefits both the facility operator and the national party under safeguards, as well as the IAEA. With robust authentication in place, the safeguards analysis of IAEA can be based on high-confidence data records. With an unauthenticated system, data errors or deliberate subversions by an unknown adversary may place a legitimate facility operation under needless suspicion of nuclear material diversion, with attendant costs and disruptions.

Unattended and Remote Monitoring Systems

There are many advantages of unattended and remote monitoring systems using authentication. They increase the efficiency of both the operator and the IAEA safeguards activity. As facilities become larger and more highly automated, inspectors' entry into the facility becomes more difficult and more intrusive. Escorting inspectors diverts facility personnel, and normal plant operations can be disrupted. Installation of unattended or remote monitoring equipment lowers costs by reducing of the number of inspector facility visits to verify operations and collect data, also relieving the burden on traveling inspectors.

The major disadvantage of unattended and remote monitoring is the costs associated with the required authentication measures and the subsequent inspection activities to verify that the authentication measures have not been compromised. Incorporating authentication components and supporting infrastructure in the equipment and facility design phase is most economical; retrofitting existing equipment already installed, even if technically feasible, may be prohibitively expensive and interrupt operations.

Joint Use Equipment

There are numerous benefits of Joint Use Equipment (JUE) systems to both the Agency and the external party. Properly developed and deployed joint systems result in ease of data collection, reduction of support burdens, and reduced costs for both the IAEA and the operator. However, the potential disadvantages are significant. The independence, integrity, and authenticity of data from JUE must be achieved with a high degree of assurance in order to protect the interests of the external party and the Agency. The implementation in practice of joint use systems is subject to IAEA policies[4] and the associated technical requirements. These considerations govern the negotiation of the formal Joint Use Arrangement (JUA) implementing the equipment and data sharing arrangements between the IAEA and the external party

8th International Conference on Facility Operations – Safeguards Interface, March 30 – April 4, 2008, Portland, OR, on CD-ROM, Danielle Peterson, Pacific Northwest National Laboratory, Richland, WA 99352 (2008)

After the IAEA performs authentication procedures on the equipment, it is placed under IAEA seal. The operator is not permitted access to the equipment unless accompanied by an IAEA inspector, and all maintenance of security critical components must be performed by IAEA personnel. This may complicate maintenance and repairs of failed equipment, but the facility is not burdened with the costs associated with maintaining these items.

Any upgrades and software changes to the equipment proposed by partner in the JUA will require advance approval by the IAEA, and will likely be carried out by IAEA personnel. Depending on the scope and complexity of the modifications, a new VR or VA could be required.

The complete data record from JUE is typically not immediately available to the operator or any other party outside the IAEA. At least some data may not be shared until after the operator's declaration has been received by the IAEA, since an independent conclusion must be ensured. If this delay in receiving data causes significant problems to the operator, a JUA may not be appropriate.

Inspector and Technician Visits

Visits by IAEA inspectors and technicians inside the facility are expensive for the operator. Site personnel must leave their normal duties to serve as visit escorts, and the presence of the IAEA staff may disrupt facility operations. While the need for inspectors and technicians to access equipment for inspection, maintenance, and upgrades can never be completely eliminated, such visits can be minimized by implementing the following features:

- Design the equipment to minimize the need for inspections.
- Apply cryptographic data authentication as close to the sensor (data generator) as possible to minimize the need for tamper indicating enclosures and periodic seal inspection and replacement by inspectors
- Use active intrusion detection measures instead of passive tamper detection.
    - Multiple layers of active tamper detection increase confidence in the integrity of the system.
    - Physical inspection of passive tamper indicating features may not be necessary except for resolution of anomalies if adequate active measures have been implemented.
- If the operator has agreed to remote IAEA access to the equipment by virtual private network (VPN) technology, the IAEA may be able to remotely maintain the equipment and install of upgrades and patches without an inspector visit.

Conclusions

Unattended and remote monitoring systems provide many benefits to both the facility operator and the IAEA; however, these systems require authentication measures that are

not generally required in systems that are used in attended mode by the inspectors. The adverse impacts of these measures on the IAEA and the operator can be minimized with careful planning at the design stages of the equipment and of the facility. Designing the safeguards system to minimize the need for inspector visits will also help minimize the impact of these measures on the facility operator.

Agreements providing remote access to the equipment through a VPN or other cryptographically secure link may eliminate some inspector and technician entries into the facility.

While Joint Use Arrangements can have significant advantages, all parties should be aware of the potential negative impacts of the authentication and data sharing provisions of these arrangements early in the negotiation process.

---

[1] 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.

[2] Tolk, K., Aparo, M., Liquori, C., and Capel, A., "Design of Safeguards Equipment for Authentication" *Symposium on International Safeguards – Addressing Verification Challenges,* Vienna, Austria, October 16-20, 2006.

[3] "Authorization of Instruments for Inspection Use", SGTS-P01/Rev.9-2004.

[4] SMR 2.20 - POLICY PAPER 20: JOINT USE OF SAFEGUARDS EQUIPMENT BETWEEN THE IAEA AND AN EXTERNAL PARTY - DATE OF ENTRY INTO FORCE: 2006-04-26