CONF-9609185--7

SAND96-1902C

Initial CTBT International Monitoring System Security Findings and Recommendations

R. L. Craft and T. J. Draelos
Sandia National Laboratories
Albuquerque, NM USA

Sponsored by U.S. Department of Energy
Comprehensive Test Ban Treaty Research and Development Program, ST485D

ABSTRACT

An initial security evaluation of the proposed International Monitoring System (IMS) suggests safeguards at various points in the IMS to provide reliable information to the user community. Modeling the IMS as a network of information processing nodes provides a suitable architecture for assessing data surety needs of the system.

The recommendations in this paper include the use of public-key authentication for data from monitoring stations and for commands issued to monitoring stations. Other monitoring station safeguards include tamper protection of sensor subsystems, preservation of data (i.e. short-term archival), and limiting the station's network services.

The recommendations for NDCs focus on the need to provide a backup to the IDC for data archival and data routing.

Safeguards suggested for the IDC center on issues of reliability. The production of event bulletins should employ "two-man" procedures. As long as the data maintains its integrity, event bulletins can be produced by NDCs as well.

The effective use of data authentication requires a sound key management system. Key management systems must be developed for the authentication of data, commands, and event bulletins if necessary. It is recommended that the trust placed in key management be distributed among multiple parties.

The recommendations found in this paper offer safeguards for identified vulnerabilities in the IMS with regard to data surety. However, several outstanding security issues still exist. These issues include the need to formalize and obtain a consensus on a threat model and a trust model for the IMS. The final outstanding security issue that requires in-depth analysis concerns the IDC as a potential single point of failure in the current IMS design.

Key Words: security, data surety, data authentication

This work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000.

INTRODUCTION

The success of the CTBT is critically dependent on the availability of trustworthy data appropriate for compliance decisions. The International Monitoring System (IMS) will be used to collect, distribute, and analyze sensor data. Effective utilization of shared data in an international monitoring environment depends on the participants believing the integrity and authenticity of the data even though they may have had no control over the design, installation, or operation of the monitoring system. When properly implemented, data surety measures such as data authentication can provide assurances of credible sensor data.

In this paper, a brief system overview of the IMS is provided. The core of the paper discusses the data surety issues and safeguards associated with particular elements of the IMS. The paper concludes with general statements about the current state of data surety in the IMS.

SYSTEM OVERVIEW

Figure 1 depicts a notional view of the IMS used to discuss the security issues and safeguard recommendations. Note that the partitioning into blocks represents partitioning of functionality and may not represent the physical partitioning of particular elements of the IMS. The **source** is an event capable of creating **signals** that are detectable by one or more of the IMS **sensor** subsystems (e.g., seismic or hydroacoustic). The sensor subsystem converts these signals into electrical or optical energy and conveys the information to the associated **station**. The station converts the electrical or optical signals into digital format and packages the digitized data into **sensor data** messages bound for the **International Data Center** (IDC). The station also provides time stamp information with each message. On its way to the IDC, a sensor data message flows over communications channels either directly to the IDC or through a **National Data Center** (NDC).

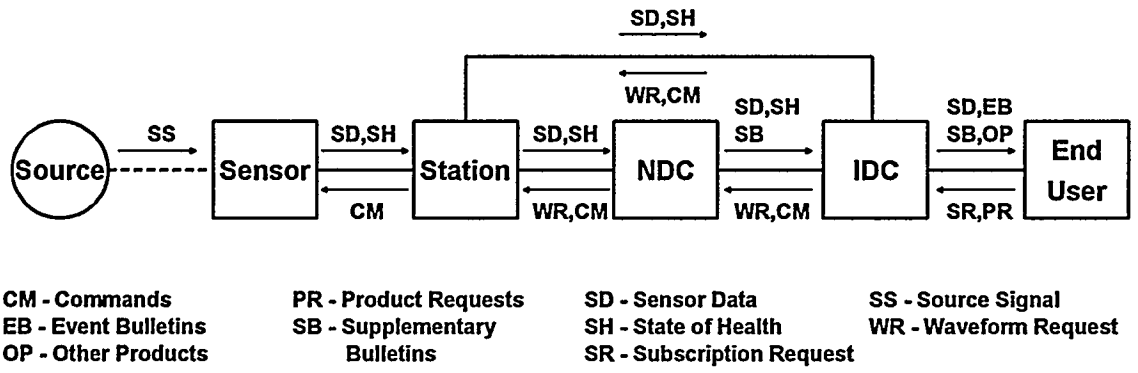

Figure 1. System Architecture and Major Information Flows

The IDC processes worldwide sensor data to determine event locations and to extract other features. If needed, the IDC may issue **waveform requests** to specific stations to retrieve sensor data to help refine the accuracy of location and feature estimates. At regular intervals, the IDC distributes an **event bulletin** listing location and feature information gleaned from sensor data.

To monitor and control the operation of the IMS, two additional information flows are built into the system. The first, the **state of health** message, flows from the sensor to the IDC. These

messages can come from sensors or stations. This information is compiled regularly for the entire system to guide IDC processing and should be available as one of the **other products** produced by the IDC. The second flow, **commands**, originates in the IDC or an NDC and may be used to control certain aspects of station or sensor performance (e.g., when calibrations are performed or how often a station is to sample data).

RECOMMENDED SYSTEM SAFEGUARDS

In this section, recommended system-level safeguards are discussed. The safeguards listed here are ordered first by the node to which there apply (e.g., station or NDC) and then by specific element within that node (e.g., commands, sensor data, etc.). The use of multiple safeguards for each element is intentional, as one goal of these recommendations is to provide "protection in depth".

- **Safeguards at the Sensor and Monitoring Station:**
  There are two primary security objectives to be realized for a station and its sensor(s). First, the integrity and authenticity of signal information must be assured. The possibility of an adversary or environmental factors being able to alter detected signals before they enter the IMS network must be minimized. Second, the availability of this signal information must be guaranteed. Once the information is captured by the sensors and stations, it must be retained until it is securely held within the bounds of the IMS network (i.e., at the NDCs and the IDC). To ensure these objectives, the following sensor and station elements should be addressed with the safeguards specified below:
  - **Sensor Data**
    In order to protect IMS sensor data at the sensor/station, the IMS must:
    - Authenticate the sensor data
    - Protect the integrity of the sensing process
    - Physically protect the authentication mechanisms
    - Deter and detect tampering with sensor/station operation
    - Ensure preservation of sensor data

    In authenticating sensor data, the following design elements should be included:
    - **Authenticate sensor data as soon as possible.** Three options have been proposed for authenticating sensor data -- authenticating at the sensor or station, authenticating it upon arrival at the IDC, and not authenticating it at all. DOE recommends authenticating at the sensor/station as this provides users of the data with greatest assurance that the data has not been corrupted since its creation. As long as a packet of sensor data exists in the IMS its authenticator should never be removed (i.e., even if data must be reformatted for efficient retrieval in the IDC, the user must still be able to go back to the original sensor data packet to ascertain the data's authenticity).
    - **Use public key techniques for this authentication and assign unique keys to each sensor/station**. Two fundamental approaches to authentication can be used: private key and public key. In private key, a secret key is shared between the entity authenticating (or "signing") the data and the entity verifying the signature. In this technique, the ability to verify also gives the verifier the ability to sign. Public key techniques make use of two keys -- a private key held by the signer and a public held

by the verifier. While the public key gives the verifier the ability to ascertain the authenticity of a set of data, it does not give the verifier the ability to forge a signature. If this technique is used and a unique private key / public key pair is assigned to each sensor, users of the sensor data will have the ability to uniquely identify the source of that data.

- **Include a time stamp in the data that is authenticated.** The presence of the time stamp makes it impossible for an adversary to record a packet and to replay it later in place of another packet. Including the time stamp as part of the data to be authenticated binds the time stamp to the sensor data such that neither can be altered without detection.

Protecting the integrity of the sensing process requires the following guidelines:

- **Physically protect the sensor data prior to authentication**. While the details of how to provide the physical protection are properly part of component design, the notion to be gleaned from this recommendation is this: from the time that the signal is captured by the sensor's transducer until it is authenticated, it is vulnerable to potentially undetectable changes. Steps must be taken to assure that these changes cannot be introduced. For the radionuclide detector, this may be realized by simple physical protection of the detector housing. Given the geographically distributed nature of the remaining sensors, this may be a more significant task. For example, if the transducer of a hydroacoustic sensor is placed underwater and its digitizer and authenticator are placed in its station on land, then conduit or other means must be employed to ensure that an adversary cannot inject noise into the signal prior to digitization without detection.
- **Use impartial parties to inspect these physical protection measures during installation**. As a station is being installed, IMS representatives should have the ability to inspect the installations to ensure that they are free from corrupting devices and will faithfully execute their intended functions.
- **Calibrate sensors and stations with great care**. Once stations are operating but before they are validated as part of the IMS, they should be calibrated by IMS representatives (other than the installers) to ensure that the data collected serves as an accurate baseline for that station. To safeguard these baseline readings, the collected calibration data should be signed by the same authentication mechanism that will sign the operational data used by the IMS. As sensor data is received by the IDC, it should be compared against the baseline readings to detect potential tampering.

To physically protect the authentication mechanisms:

- **Create a secure zone around the authentication element**. Rather than giving an adversary direct access to the authentication element, a secure zone should be created that averts (or at least detects) incursion into the zone. For seismic sensors, this may include placing the authentication unit down the borehole and tamper detecting (see next safeguard) the borehole cover. For other sensors, this may require emplacement in a secured housing.

- **Use tamper indication and detection on the authentication element and its physical safeguards.** To protect the integrity of the authentication unit, tamper mechanisms should be employed. Two levels should be considered:
  - Tamper indication (e.g., seals that cannot be removed without destroying them) is useful for limiting access to physical elements of the system. This should be applied to the housing of the authentication unit and should be accompanied by visual inspection during on-site visits.
  - Tamper detection (e.g., door switches or light sensors) is useful for immediate indication of violation of a tamper boundary. This should be applied both to the authentication unit and to physical safeguards used to provide a secure zone around this unit. Detection of tampering should insert indicators into the sensor data message stream.

To deter tampering with sensor/station operation:

- **Trigger short notice, on-site inspections as a result of suspicious sensor/station behavior.** If the countries that host monitoring stations are also responsible for the maintenance of those stations, the IMS must closely monitor station data for any indications of abnormal behavior. This could include loss of data packets, changes from baselines established during calibration, or the presence of tamper indicating bits in the sensor data stream. If tampering is suspected, then on-site inspection of the site should be initiated.

To ensure preservation of sensor data:

- **Put the sensor data into long term storage as soon as possible.** As soon as a sensor's data has been digitized and authenticated, it should be stored in some sort of buffer (hard drive, non-volatile RAM, etc.) at the station. This data should remain in the buffer until received and stored the IDC. In sizing this buffer, the primary consideration will be the length of possible communications outages.
- **Provide alternate means of data retrieval.** In the case where a communication outage might be unusually long, provision should be made for physical recovery of the data from the buffer. The buffer should be sufficiently large to retain its data until a physical recovery can be completed.

- **Sensor/Station Commands**

The use of public communication networks and standard communication protocols to control station operation opens stations to network-based attacks. If an adversary can gain access to a station, then the ability of the station to correctly operate will be in jeopardy. If the adversary can gain this access through the station's network interface, then the possibility exists that the adversary can establish a significant span of control in the IMS.

In order to protect IMS stations from these attacks, the design of the station must:

- Ensure the authenticity of commands received
- Fastidiously control the station's capabilities
- Monitor the effectiveness of these safeguards

In ensuring the authenticity of commands received, the following design elements should be included:

- **Authenticate each command received.** The station must verify (by authentication) the identity of users sending commands as a condition for executing these commands. This verification should be performed on a command by command basis and not on a session basis (i.e., login with password, execute a series of commands, and logout).
- **Use public key techniques and user-unique key assignments to authenticate commands.** In order to facilitate auditing, public key techniques should be employed in authentication. When used with unique key assignments, this will permit the station to uniquely identify the user issuing commands.
- **Time stamp commands from each authorized user.** More than one entity (to include the host nation) will be able to control a given station and its associated sensors. For each such entity, a unique public key / private key pair should be assigned. Each command should be time stamped. The station should not respond to commands whose time stamp is older than a specified period of time. The use of time stamping along with a "live message window" assures that an adversary cannot capture and replay commands at times that suit the adversary's purposes.

To fastidiously control the station's capabilities:

- **Limit the station's network interface to a minimal, well-controlled set of services.** These are component-level design issues, but the goal must be to make sure that only the transactions allowed to occur across this interface are occurring. These design techniques are the same as for firewall designs and may rely, in part, on a small set of custom developed communications utilities written to replace those supplied by the vendor of the station's computer.
- **Limit the number of IMS users able to issue commands to a station.** The motivation behind this is to limit an adversary's points of entry into the station command structure.
- **Limit the functionality available on the station's computer.** When computers are attacked from a network connection, the attacker often starts by gaining access in some way and then continuing to increase his access by using programs/utilities that are resident on the computer. For this reason, the software resident on the station's computer should be reviewed to assure that it has a valid reason for existing. Utilities provided by the computer's manufacturer should be stripped out if not absolutely essential.

To monitor the effectiveness of these safeguards:

- **Audit security critical events at the station.** Certain functions and certain events (e.g., the receipt of commands by a station) must be tracked to ascertain whether legitimate operations are being conducted or whether attacks are being launched. Audit mechanisms should be built into the station software to record these events to an audit file. It should be noted that large amounts of audit data can be generated quickly by audit processes; therefore, care must be exercised in order to ensure enough

information is gathered for adequate monitoring but not so much that the auditor is swamped.

- **Safeguards at the NDC**
  An NDC has two primary roles in the IMS. First, it is a relay point for IMS communications flowing between stations and the IDC. Second, it is the primary user of IMS product data. In addition to these IMS roles, an NDC can be tasked with additional national.

  0f the NDC roles, only the first levies a security requirement (the assured delivery of sensor data) on the IMS architecture. As its user's primary interface to the IMS, the NDC may also have certain requirements for protecting these users' information systems from the rest of the IMS; however, the IMS will take no steps to realize this goal. This responsibility properly resides with the users. To ensure these objectives, the following NDC elements should be addressed with the safeguard specified below:
  - **Sensor Data**
    The IMS design must ensure that the NDC can securely route sensor data. To accomplish this:
    - **Retain the sensor data until it is securely stored in the IDC.** As data from the stations is forwarded through an NDC, the center should retain a copy of the data long enough to ensure that it has been received and stored at the IDC.
    - **Focus on the reliability of the IDC's data storage and routing capabilities.** In support of IMS reliability, the NDC must take those steps necessary to ensure that loss of a storage device or of communications does not result in the loss of sensor data.
    - **Restrict external access to the assets responsible for relaying sensor data.** The goal here is to assure that entities external to the IDC cannot corrupt the relay function of the NDC. Techniques discussed earlier for limiting network access to the station apply here (e.g., limited sets of authorized users, limited, well-studied sets of services available on the interface).

- **Safeguards at the IDC**
  There are two primary security objectives to be realized at the IDC. First, as the IDC will be the ultimate repository of sensor data collected by the IMS, it must be able to guard against the loss of this data and to assure its timely delivery to users in response to subscriptions and requests. Second, the IDC must be able to guard the integrity of the event bulletins that it produces. To ensure these objectives, the following IDC elements should be addressed with the safeguards specified below:
  - **Sensor Data**
    At the IDC, the primary security need, with respect to sensor data, is that the IDC ensure availability of sensor data to itself and to IMS users. To accomplish this:
    - **Focus on the reliability of the IDC's data storage and routing capabilities.** In support of IMS reliability, the IDC must take those steps necessary to ensure that loss of a storage device or of communications does not result in the loss of sensor data. This can be achieved through redundancy (e.g., dual communication paths) or high reliability components.
    - **Backup the data stored at the IDC.** As the IDC is the permanent repository for all IMS sensor data, this data should be backed up as soon as possible and at a location

independent of the IDC itself (to avoid common mode destruction). This should be accomplished in such a way that failure of the IDC still permits sensor data to continue to be stored at the backup site.

- **Limit IMS access to IDC data storage and communication mechanisms.** There are two aspects to this. First, limit the number of IMS users (including IDC operators) who have more than "read access" to the sensor data. Second, make sure that a given user never has other than read access to both the IDC storage and the backup site storage. If a user is able to administer storage at the IDC, he should only be allowed read access to the backup site.

- **Event Bulletins**

  For many treaty signatories, the event bulletins produced by the IDC will be their principal means of assessing compliance. For this set of users, the integrity of the IDC's event bulletins is paramount. In order to protect bulletins from corruption, the design of the IDC must:

  - Protect the processes used to create event bulletins
  - Employ "two man" concepts in bulletin production
  - Control the IDC's external interfaces

  To protect the processes used to create event bulletins:

  - **Limit the number of IDC staffers able to access processes and data critical to event bulletin integrity.** Access to those items that are critical to the proper production of event bulletins (e.g., the pipeline's parameter files) should be kept to the least number of people possible. The goal here is to minimize the exposure of these files.
  - **Audit events that adversely affect these processes and data.** Operations related to these security critical items (e.g., writing/replacing or deleting of parameter files) should be closely monitored by means of audit files. Review and management of these files should be assigned to IDC staff other than those staff members who are authorized to work with these security critical items.
  - **Limit the functionality available to each IDC staffer to only that which is needed in order to execute job responsibilities.** A skilled insider may be the IDC's greatest threat; therefore, no more tools should be placed into his hands than are absolutely required. Analyst workstations should be stripped of any utilities not essential to the analysts' mission. Access to resources and files on network should follow the same principle.

  To employ "two man" concepts in bulletin production:

  - **Make analysis assignments that avoid regional conflicts of interest.** When selecting an analyst to monitor events in a given region, care should be taken to ensure that the analyst is motivated to perform the assigned job in an even-handed manner.
  - **Require independent review of detected events.** To guard against the possibility of an analyst "detecting" an event that does not really exist, a second analyst with different political affiliations should review the events detected by the first analyst.

To control the IDC's external interfaces:

- **Limit the IDC's interface to a minimal, well-controlled set of services.** This is another way of saying "use firewalls, where appropriate, to guard the IDC perimeter." Ideally, this will involve a "proxy server" that sits between the open networks and the IDC computer(s) and that runs a very limited number of custom written (as opposed to vendor supplied), highly inspected programs in order to deliver a very limited set of services to outside entities.
- **Limit the services provided to those that can be satisfied with message passing.** In support of the previous recommendation, the services available should be handled in a request/response fashion. No provision should be made to permit direct access to IDC computing resources.

To make all data, software, parameters, etc. available for inspection:

- **Specify the pedigree of each event in an event bulletin.** Event bulletins published by the IDC should be expanded to include two sets of information for each event. The first set is the parametric data currently published in these bulletins. The second set, available on request, is a specification explaining how these parameters were produced. This specification should include a listing of the source data used at each step in the process, a statement of which programs were used and in what order, and a specification of what parameters were used to control each of these programs. In addition, certified (i.e., signed) versions of these programs and their associated data files should be made available for use by any states party interested in independently verifying results.

- **Other Safeguards**
  - **Split responsibilities in key management.** Authentication does not "solve" any problems; it merely moves the problems to another location -- key management. The intent in doing this is to move the problem to a place where it is more easily managed. Most key management systems centralize the trust in a party trusted by all users of the system's cryptographic capabilities. As no such party appears to exist in the IMS, DOE recommends that a distributed key management approach be employed where trust is spread across multiple parties such that no one party is capable of subverting the key management.
  - **Establish designated chain of succession for use in loss of IDC.** Plans should be made for alternate routing and processing of the IMS data, to handle the event that the IDC becomes inoperable for an extended period of time.

OUTSTANDING IMS SECURITY ISSUES

Work done to date by DOE in assessing the security needs of the IMS and in analyzing the related work that has been performed by the CTBT community points to several key IMS security needs.

First, the kinds of topics that have been discussed in this paper as well as system threats, desired security attributes, probable attacks and associated threat agents need to be discussed by the CTBT community as a whole.

Second, while sensor data authentication is important (even critical) to meeting the security objectives of the IMS, it is not sufficient in itself to safeguard against threats to the system and to realize the desired security features. Other technical and procedural safeguards besides data authentication have been considered by both DOE and NPTO. These need to be discussed within the CTBT community.

Third, no authentication scheme should be accepted as "the answer" until the details of the associated "key management" infrastructure are understood. Authentication is not a "solution"; it merely moves the problem to key management. Assessment of any IMS key management system must accompany assessment of the authentication mechanisms before the security of the solution can be judged.

Fourth, every "secure" system invests "trust" in one or more roles (e.g., system administrator) or entities. It is not clear that a "trust model" has been developed that states how trust is invested in the IMS. The de facto model seems to place a high degree of confidence in the IDC. This can be problematic if the IDC represents the location in the system where certain attacks may be both easy to accomplish and high payoff for an adversary. For this reason, a "distributed trust" approach may be more effective.

Fifth, the current IMS design makes the IDC a potential single point of security failure. Loss of the IDC's routing capability could lead to a complete inability of the IMS to function. Recovery would then seem to be dependent on the NDC's backup capability.

APPENDIX

Additional Reading: Information on the following reports are available on the DOE CTBT web page at URL http://www.CTBT.rnd.doe.gov.

[1] **CTBT International Monitoring System Security Threats And Proposed Security Attributes**, Sandia National Labs Report SAND96-0536, March 1996.

[2] **Authentication of Data for Monitoring a CTBT**, Sandia National Labs Report SAND96-1061, May 1996.