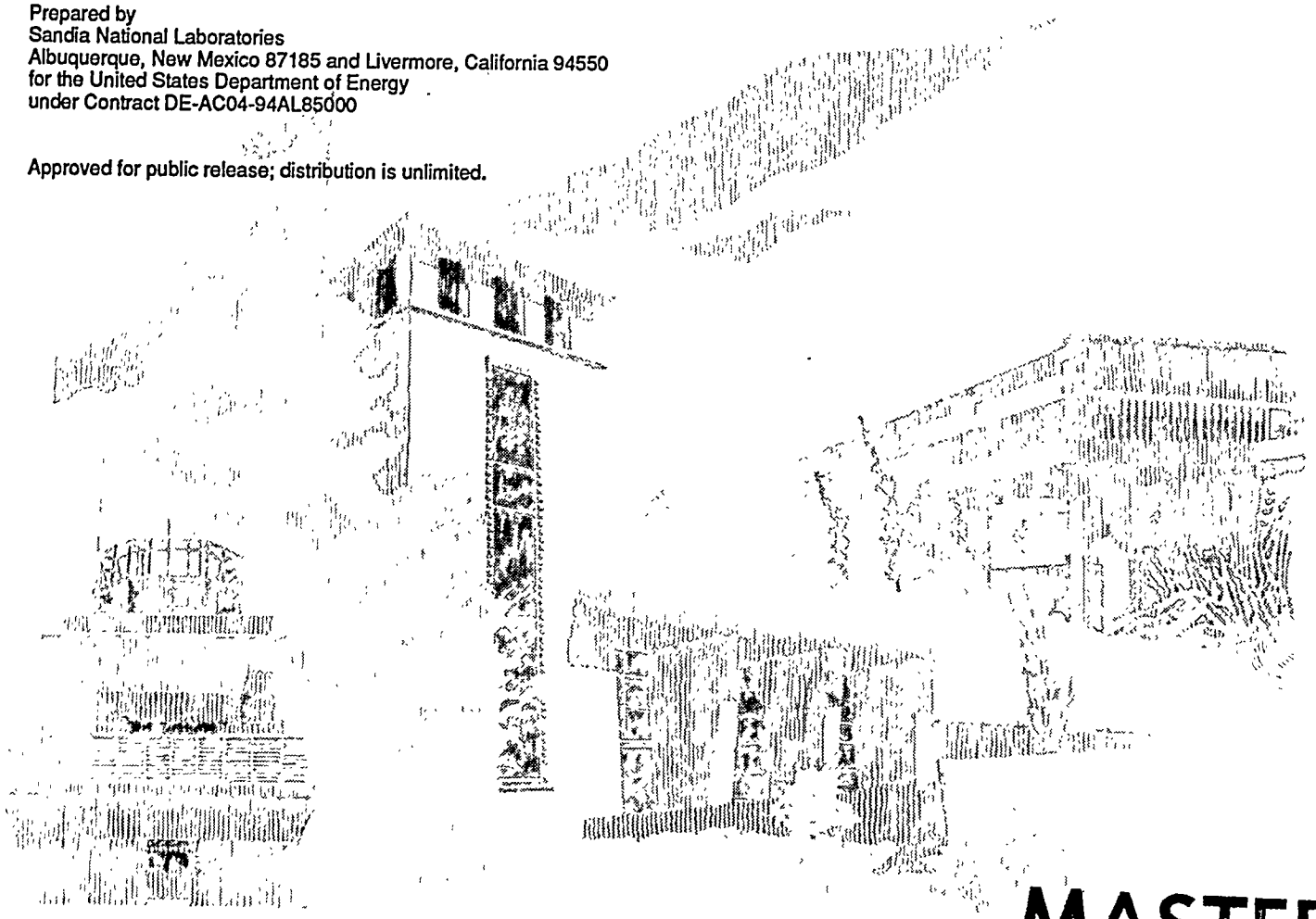
SANDIA REPORT

SAND96–1061 • UC–900
Unlimited Release
Printed May 1996

Authentication of Data for Monitoring a Comprehensive Test Ban Treaty

R. L. Craft, T. J. Draelos

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-94AL85000



Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
Office of Scientific and Technical Information
PO Box 62
Oak Ridge, TN 37831

Prices available from (615) 576-8401, FTS 626-8401

Available to the public from
National Technical Information Service
US Department of Commerce
5285 Port Royal Rd
Springfield, VA 22161

NTIS price codes
Printed copy: A03
Microfiche copy: A01

SAND96-1061
Unlimited Release
Printed June 1996

Distribution
Category UC-900

Authentication of Data for Monitoring a Comprehensive Test Ban Treaty

R. L. Craft
Data Systems Security Department

T. J. Draelos
Cooperative Monitoring Technologies Department

Sandia National Laboratories
Albuquerque, NM 87185

Abstract

The important issue of data integrity in the CTBT International Monitoring System (IMS) is discussed and a brief tutorial on data authentication techniques is offered. The utilization of data authentication as a solution to the data integrity problem is evaluated. Public key data authentication is recommended for multilateral monitoring regimes such as the CTBT. The ramifications and system considerations of applying data authentication at various locations in the IMS, or not at all, are reviewed in a data surety context. The paper concludes with a recommendation of authenticating data at all critical monitoring stations.

Intentionally Left Blank

Table of Contents

List of Figures

Intentionally Left Blank

Authentication of Data for Monitoring a Comprehensive Test Ban Treaty

1. INTRODUCTION

The Comprehensive Test Ban Treaty (CTBT) is intended to provide a framework agreed upon by the international community whereby nuclear testing of any yield will be prohibited. An International Monitoring System (IMS) is proposed to allow the exchange of data relevant to the verification of compliance with the treaty. The CTBT IMS will provide a means by which the international community can effectively monitor compliance with the anticipated Comprehensive Test Ban Treaty. The system is expected to include a global network of seismic, hydroacoustic, infrasound, and radionuclide sensors along with significant event detection and processing capabilities resident at a central international data center (IDC) and, possibly, at national data centers (NDCs).

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 data acquisition systems. When properly implemented, data authentication can provide the assurance that received data came from the expected data source and were not altered. However, imposing data authentication on a monitoring system will have an impact in terms of increased cost, security, and maintenance. In this paper, the pros and cons of utilizing data authentication measures or no authentication at all are evaluated for the few most likely scenarios. Certain attacks on specific equipment or software are beyond the scope of this paper, primarily because the IMS has not been fully implemented. With this in mind, this paper is an attempt to discuss, somewhat independent of specific implementation details of the IMS, the issues surrounding data authentication.

Section 2 of this document introduces the issues of data integrity, authenticity, and non-repudiation in the IMS. For those who don't have a background in data authentication, Section 3 provides an introduction to data authentication concepts and a discussion of private and public key data authentication. Given that public key data authentication offers certain advantages in a multilateral monitoring regime, Section 4 presents the issues involved with implementation of a public key data authentication solution. Section 5 concludes this paper with an evaluation of the two most likely options of data authentication use. Section 6 offers some concluding remarks and makes a tentative data authentication recommendation.

2. DATA INTEGRITY

Data integrity is the ability to determine that a data item has not been altered, deleted, or substituted without detection. It is important to note that this definition does not imply protection of data, but only the ability to ascertain whether data is authentic. Data authentication is a term generally associated with data integrity, but can also address other security attributes. Technically speaking, the term *authenticity* is defined as the ability to establish the identity of a given entity. *Nonrepudiation* is the ability to establish that a given transaction could have been initiated by a given entity and only that entity or that a given entity did, in fact, participate in the transaction. In a CTBT setting, data integrity ensures that data used for nuclear event monitoring is the actual sensed data, authenticity uniquely identifies the source of the data, and nonrepudiation prevents a country from denying that the data originated at their monitoring station. A more in-depth discussion of data integrity, authenticity, and nonrepudiation as well as other data surety issues of concern to the CTBT can be found in [1].

Since integrity is evaluated over data streams, it is helpful to identify the various elements of the IMS from a data oriented point of view. The IMS can be modeled by a network of data processing elements that acquire event data, make it available to end users, and store it in archive. The following diagram depicts the IMS model. The elements of the model are defined immediately after the diagram.

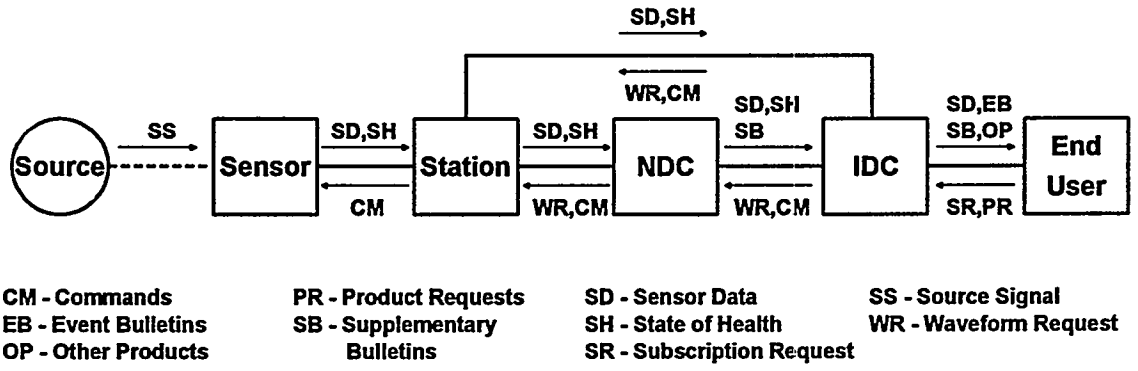


Figure 2.1 IMS Data Flow Block Diagram.

CTBT model elements definitions:

- Source - an observable event or occurrence that is the result of some activity. In the case of the CTBT, the phenomenon of interest is the set of circumstances generated by detonating a nuclear weapon and is called a nuclear event.
- Sensor - a device that converts an observable phenomenon into information that can be collected and analyzed. A nuclear event can occur above ground, underwater, or in the ground. Therefore, radionuclide, hydroacoustic, seismic, and infrasonic sensors are candidates to be used to monitor the CTBT.

- Station - a set of equipment designed to acquire and communicate information about certain activities. The monitoring station consists of a sensor subsystem, a data acquisition subsystem and a communication subsystem
  - Data acquisition subsystem - equipment that converts sensor information into data that can be processed, and communicated.
  - Communications subsystem - equipment that transports data from one point to another
- NDC - the optional facility that collects data from all monitoring stations within a nation or group of nations.
- IDC - the facility that collects data from all monitoring stations and NDCs. The IDC processes event data, publishes event bulletins, archives data, and fills data subscriptions for end users.
- End user - an entity that receives event data and bulletins based on an established subscription. In most cases, the end user will be an NDC.

Data integrity is essential to the IMS to be able to successfully verify compliance. The method of ensuring data integrity however is an area of debate. Small events may be detectable by only a small number of monitoring stations. With large events, particularly teleseismic, self-authentication of event data is possible by virtue of the shear number of monitoring stations able to validate the data. However, self-authentication of sufficiently small events becomes arguably nonexistent. This is all the more true when a minimum number of stations are required to detect an event before it is recognized as legitimate. Therefore, any tampering of data that would prevent an event from being detected could in fact "hide" the event. This discussion has entered into the area of threats, vulnerabilities, attacks and safeguards which are defined below.

- Threat - An objective that an adversary is determined to accomplish.
- Vulnerability - A weakness that allows attacks pursuing a threat.
- Attack - A specific activity that exploits a vulnerability to realize one or more threats.
- Safeguard - A security measure designed to counter attacks.

To be able to evaluate the data surety issues of a monitoring system, it is important to establish a threat statement. In other words, one must define what the threats to the CTBT IMS system are and who is likely to perpetrate them. Four potential threats to the IMS are identified and discussed. For each of the threats, the attackers are suggested along with how they might operate. Along with identifying what the threats to the IMS are, it is important to consider who might attempt to realize a threat and where the threat might be directed.

It should be noted that even though outside hackers are considered potential agents in each threat, the greatest threats to the monitoring system are likely to come from those parties not wanting the system to correctly detect events (e.g., countries wishing to test in violation of the treaty). The threat discussion below is compatible with a similar threat statement [1]. The threats that affect the integrity of the IMS are as follows:

1) **Hiding an actual nuclear event.**
The focus of this threat is an event that is, in fact, detectable by the IMS but that is somehow kept from appearing on an event bulletin produced by either the IMS' International Data Center (IDC) or by any of the National Data Centers (NDCs) serviced by the IMS.

There are many approaches one might take to hide an event. The first step is to determine how many monitoring stations need to be affected to ensure evasion. The number is based on monitoring coverage, the size and propagation characteristics of the event, and the event formation process used at the IDC. Then, for each station, the actual event data can be made unavailable, substituted for, or modified anywhere along the data path. Processes at the IDC could also be disturbed to guarantee failure of detection. The bottom line is that knowledge of an actual nuclear event is not confirmed by the verification community.

The most likely agent for this threat is a country desiring to conduct a test. For a sufficiently small yield, it is conceivable that the stations most likely to detect the test could be within the control of the testing country. Given this, reasonable attack scenarios include disabling the IMS elements in country (sensors, stations, NDCs, etc.) for the duration of the event and leaving the system operational but overwriting event data with previously collected ambient data for that station.

It is also conceivable that an attack intended to hide the data could be launched from the IDC itself by means of an insider erasing source data, altering the processing subsystem in such a way as to avoid detection, or by altering the event bulletin after processing but before distribution. Unless special measures are put in place to prevent this, a credible case can be built for the viability of one man attacks of this sort.

Finally, given the likelihood of using commercially available computers, open networking standards, and commercial networks in the implementation of the IMS, hackers from outside the CTBT community represent real threats to the integrity of the IMS' data. Source data queued up for processing might be destroyed, processing algorithms might be altered, event bulletins might be corrupted, etc..

2) **Altering an event's characteristics.**
Although this threat is related to hiding an event, the emphasis of this threat is on changing the attributes of an event so as to preclude the proper identification and/or attribution. Rather than trying to totally hide the fact that an event occurred, an attacker may simply want to change the perceived characteristics of the event. Among other things, these changes could include making the event appear to be a different type of event (mine blast rather than low yield test), modifying the event's apparent magnitude, or causing it to appear that the event occurred at a different location than where it actually did.

As before, the most likely agent for this threat is a country desiring to conduct a test. Using the same techniques as described for hiding event, the country might launch an attack to modify the event's apparent characteristics. The motivation for this (as opposed to hiding an event) may be that the country's span of control within the IMS is such that it cannot control the data produced by all sensors capable of seeing the event. This kind of threat might be readily realized by a sufficiently skilled insider working for the testing country. It might also be accomplished by a hacker wanting to exert some power by corrupting IMS data.

3) **Creating an event that never occurred.**
Impersonation for the purpose of making it look as though a certain country created a nuclear event is a very real concern under the CTBT. Many of the same techniques for event hiding could be used for event creation. The bottom line here is that the verification community believes that a nuclear event occurred or at least causes a loss of credibility of CTBT verification.

Several ways of realizing this threat might be considered. First, old sensor data from previous events might be injected into the system or new data might be completely synthesized and played into the system. Second, fictitious records might be placed in the incoming data queue at the central point of the system -- the IDC. Third, an insider might also directly modify event bulletins after they are created; however, the source data alleged to have contributed would most likely have to be modified as well in order to create a coherent picture. Finally, a hacker could achieve the same goals as an insider given the assumptions stated above.

4) **Damaging IMS credibility.**
A threat that could affect the entire monitoring system (not just stations in perceived enemies' territory) is to damage the verification credibility of the IMS. This threat might be realized by reducing the availability of the data, corrupting data, or realizing the above threats on a large scale.

While hiding an event may be the most obvious, this final threat might be the most effective. If an adversary is able to create doubt as to the accuracy of the IMS, then it may be easier to initiate a test without consequence. "The system has reported a dozen false alarms already this year. So what justification do you have for wanting to come inspect my site this time?," an adversary might ask.

In practice, this threat might be realized in a number of ways. If the test to be conducted is likely to be detected by only a limited set of sensors and these are largely under that country's control, then the country might corrupt the sensor data on a regular basis in order to create an history of problems with those stations. Similarly, an IDC insider might accomplish the same thing by creating spurious events which cannot be corroborated by inspection or other means and by suppressing events that

clearly should have been detected by the IMS. As before, an independent hacker might accomplish the same thing as an insider.

How these threats affect the IMS and might be countered is discussed in Section 5. However, since data authentication is the primary means of countering many of these threats, a brief tutorial of data authentication is presented next.

3. DATA AUTHENTICATION

Background

When data is transferred between locations where it can be intercepted and/or substituted or where the data source is not sufficiently controlled, the potential for its modification exists. Data authentication is a cryptographic technique used to detect modification of data subsequent to generation and application of its authentication "tag". Note that data authentication does not change the data in any way (i.e., it is not encrypted) , but appends an authentication tag that accompanies the data as long as its integrity is at issue. Figure 3.1 shows a block diagram of a typical monitoring system employing public key data authentication.

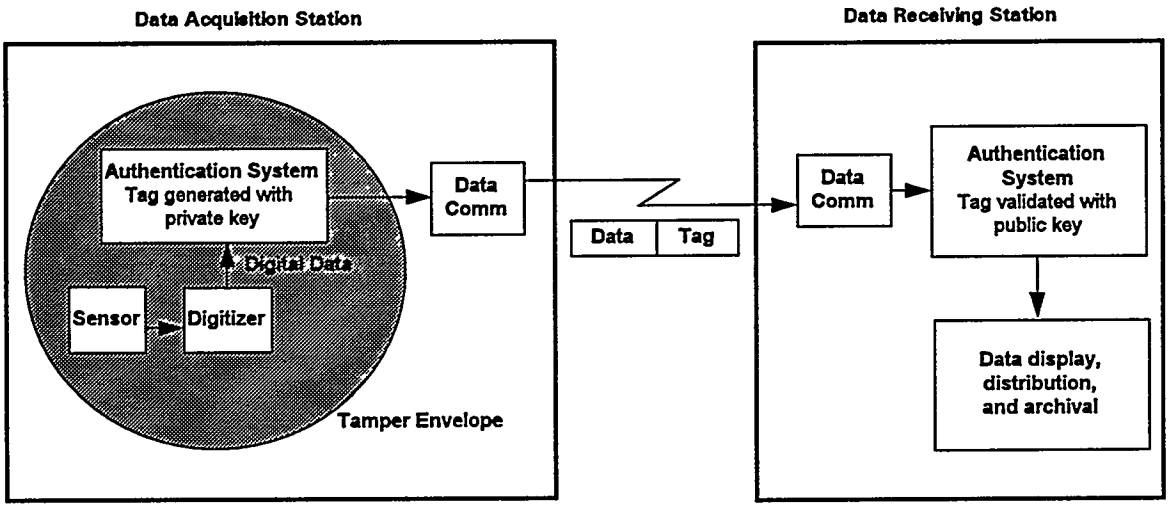


Figure 3.1 Public-key data authentication in a monitoring system.

There are two methods of performing secure data authentication. One method involves private key (symmetric) cryptography and the other is based on public key (asymmetric) cryptography.

Private Key Data Authentication

Private key data authentication involves the use of the identical key by the sender and recipient of the data. The sender generates an authentication tag using the private key and sends the data and the tag to the recipient. The recipient tests the validity of the received data and tag by generating an authentication tag using the received data and the same algorithm and key that the sender used. If the sender's tag is the same as the tag generated by the recipient, then the data and tag are deemed to be valid (have integrity).

The authentication tag generated by private key systems is normally two to four bytes in length. Keys are generally used for a relatively short period of time (e.g., one week) since each use of a key provides an adversary with information from which to ascertain the key (many observations of data and its associated authentication tag are required to guess the key). The symmetry of the key presents a problem for multilateral monitoring because any recipient of the data has the ability, by virtue of having the private key, to modify the data, generate its corresponding authentication tag, and forward both to other data recipients who, using the same key may conclude that the data are authentic. Since this key must be kept secret, some sort of key protection system must be employed in both the sending and receiving systems.

Public Key Data Authentication

In public key systems, the key that the sender of data uses is different from the key used by the receivers of data. The sender utilizes a key known as the private key that must be kept secret. The recipients (unlimited in number) utilize what is known as the public key. The public key cannot be used to generate the authentication tag and thus modification of the data without detection is highly unlikely. The public key is a function of the private key and does not need to be kept secret. When appropriately sized algorithm parameters and tags are used, it is deemed computationally infeasible to compute the private key given the public key. This is because the solution would require factoring of the product of very large (greater than 512 bits) prime integers. Since the security of the algorithm is based on the difficulty of finding the private key from the public key, a key can be used for a long period (years). Public key systems generally have the disadvantage of being computationally intensive and requiring typically 40 bytes in the authentication tag. Recent advances in hardware provide the processing power required for the use of public key algorithms which greatly simplify the key control in systems which require that multiple users of data be allowed to verify its integrity.

In summary, either type of data authentication (public key or private key) allows a data recipient to ensure that received data have not been modified after application of an authentication tag if the private keys have not been compromised. Once the data's authentication tag is generated, both the data and its tag can be left unprotected.

In a multilateral monitoring regime, public key data authentication offers distinct advantages over private key solutions. This is because multilateral monitoring involves many recipients of the same data and public key systems do not allow recipients to generate authentication tags. In addition public key data authentication incorporates features of authenticity and nonrepudiation. Finally since private keys only reside with the sender, key management becomes less difficult. Therefore, the recommendation for the CTBT IMS is to consider the use of public key data authentication.

4. IMPLEMENTATION

The implementation of public key data authentication (see Section 3 for a discussion of its merits over private key data authentication) requires the following elements to be effective. From this point forward, the authentication tag will be referred to as the digital signature.

- An authentication unit that is inserted into the digital data stream to generate and validate signatures,
- A tamper indicating element that protects the sensor, data line, and authentication units until the signature has been generated,
- A virtual error-free communications channel for transferring data, and
- A key management element that generates, distributes, protects and manages keys.

Authentication Unit

Authentication units are required to generate and validate digital signature. While signature generation units are normally constrained to small, low power, tamper protected environments, validation can generally be performed on any type computer. Typically, signature generation and validation can both be done with the same unit without a substantial burden to the equipment.

Several types of signature generation units will be required to interface with monitoring equipment already deployed, existing equipment which has not yet been deployed, and equipment in design. Obviously, it will be easier to integrate data authentication into equipment that is in its design stage. When the equipment already exists (whether deployed or not) a separate module will need to be inserted into the data stream after the data are in digital form.

Tamper Indicating Element

Because data authentication detects data modification only after the signature generation process, it is necessary to detect tampering with the data prior to signature generation. Examples of tamper detecting elements are: 1) a combination of mechanical housings and tamper detecting seals or 2) surveillance of sensors and data lines prior to signature generation.

Monitoring systems which are in the design phase will provide the easiest solutions for tamper detection because it can be designed into the equipment. Existing equipment may require modification or the addition of equipment and/or procedures to provide the required tamper detection.

Tamper indications can be either passive or active. For passive indications, inspection is required for detection. Active tamper indicating systems insert an alarm in the data stream and can issue penalties to the system such as key destruction when tampering is detected.

Borehole seismic monitoring systems are able to use the earth as a tamper barrier. If the seismic data's signature is generated deep in the borehole, then the seismometer can be used as a tamper detecting sensor. Other types of sensors may not enjoy this inherent level of protection.

Guarding against key compromise is of course of primary importance to effective data authentication. In addition to tamper protecting the authentication device where the private key resides, there exist a host of concerns related to keys since the issue of key management spans the entire system. Key generation, distribution, and coordination must all be handled in a secure fashion and may involve tamper protection at locations other than data collection sites.

As will be seen throughout the remainder of this paper, tamper protection of the data to be authenticated is crucial to ensuring data integrity. However, it is recognized that a determined adversary can defeat most any tamper protection if sufficient resources are expended. Therefore, it is important to understand under a given data surety system, who the adversaries are, what are their resources, and what cost at various locations in the system is to be imposed on their attacks.

Communications Element

When the recipient of authenticated data concludes that the data is cryptographically invalid, the entire data message is suspect and may be of limited value. A change in a single bit of any sized message is enough to suspect the entire message since most authentication schemes do not locate, but simply detect, modifications in the message. For this reason, communication of authenticated data must be performed in an error-free manner. Without robust communications, the likelihood of receiving invalid data messages substantially increases. It is important that the recipient be able to rule out naturally occurring reasons for invalid messages. Fortunately, common error detection and correction schemes can be used when communicating authenticated data.

Key Management Element

The use of public key data authentication greatly simplifies key management issues since only the private key needs to be kept secret. However, concerns of key generation (private, public, and associated cryptographic parameters), distribution, usage, and coordination impact the entire IMS. Key management is arguably the most complex issue to be dealt with in implementing data authentication. In a multilateral monitoring regime, key management can be especially complicated. This complication is primarily a result of the difficulty in establishing trust between so many parties. In practice, it is well known that the key management system is a primary target of adversarial attacks.

The private key generation process must be performed in such a manner that each of the parties is convinced that the process was done properly and that none of the other parties has information that would increase the likelihood that any party could have an advantage

in determining the private keys. One approach is to have each authentication unit generate its own private key using a random process that nobody including the designers of the unit would know. Another approach is to have each party provide data that would be used in the generation of the private keys. After the keys are generated, the private key is downloaded into the authentication unit. At this point, the private key would be unique to that unit and all copies of the private key outside the unit would be destroyed. Since the authentication unit would be a sealed, tamper indicating package incorporating multiple security features to ensure that the key could not read from the unit, the unit could then be stored or shipped to the site at which it would be installed without additional security measures. Using either approach, the public key would be output by the unit to be used for data validation.

System Considerations

Operational considerations of data authentication primarily include maintenance of authentication units, keys and tamper systems. A particular system issue relevant to seismic monitoring is the configuration of authentication in seismic arrays. Generally speaking, it is considered quite beneficial to authenticate even a single element of an array. It certainly should not be necessary to authenticate the data from all sensors in seismic arrays because of the expected correlation across the array.

A significant concern to the use of authentication anywhere within the IMS is that of data hiding. The concern can be posed as the question, "can the private key be communicated without detection in a data stream?" A typical scenario might be to "hide" a single bit of the private key in the noise (least significant bit) of a seismic data stream. If one bit of the key is communicated each hour, then an entire standard 160 bit key can be communicate in less than a week.

5. AUTHENTICATION LOCATION OPTIONS

The placement of authentication in the IMS has important ramifications to the overall integrity of data. Placement also impacts the cost of implementation as well. In this paper, three authentication scenarios are evaluated. These three options are 1) no external data authentication, 2) authentication of data as it arrives at the IDC, and 3) authentication at the monitoring stations. All of the options have support within the U.S. community and each possesses particular strengths and weaknesses. It is important to note that the addition of authentication does not necessarily eliminate the need to trust part of the IMS or its users, but rather moves the domain of trust to a more manageable setting. Listed below are the data authentication options under consideration, presented in order of lowest cost/lowest security. Naturally, the primary tradeoff between the choices is that of cost and security. As the assurance of data integrity increases, the cost also increases and vice-versa.

1. **No authentication** - This option clearly offers the lowest cost option while offering no cryptographic data integrity solutions. However, system design measures besides data authentication may be considered to raise the data integrity within the IMS (e.g. secure communications channels, more monitoring stations, etc.). These measures would surely increase the IMS costs.

2. **Authentication at arrival into the IDC** - Option 2 offers the best opportunity for minimizing the cost and impact of data authentication while still offering minimal data integrity to the IMS. Data would be authenticated upon arrival into the IDC and would therefore offer integrity safeguards to archived data. End users could then be assured that received data is a genuine version of that residing at the IDC. However, there would be obvious questions as to the credibility of the data at the IDC due to potential tampering prior to arrival.

3. **Authentication at the monitoring station** - This option offers the best opportunity for ensuring data integrity throughout the IMS with the primary concern being the cost of implementation and operation. Each monitoring station would require an authentication unit with tamper protection/detection around it as well as the sensor system. Seismic stations can offer tamper detection advantages if the authentication units are placed deep in a borehole.

In summary, Option 2 is intended to reduce cost and impact to the existing monitoring systems (primary seismic stations) by performing authentication on data arriving at the IDC. The option intended to offer the highest level of data integrity, Option 3, is to place authentication at the monitoring stations themselves as close to the sensors as possible. The following discussion presents various arguments for and against each option. Future effort will be dedicated to an in-depth evaluation of cost, impact, and effectiveness of each option.

OPTION 1. No authentication

STRENGTHS:

- The primary argument in favor of requiring no external data is that of cost. Obviously if there is no compelling reason to add authentication mechanisms to the IMS, then why take the time and trouble to do so? The counter argument is of course to question why an IMS is even being considered if the data acquired by it can't be trusted. This issue leads to the following potential strength.

- The argument that places trust in IMS data without data authentication says that data integrity can be maintained through corroboration by other monitoring means. The idea is that an adversary would have to spoof multiple monitoring sites and systems within and outside of the IMS to ensure that an event goes undetected. Apart from the IMS monitoring systems, corroboration might come from independently operated monitoring stations in the vicinity of the event or data from various other sensor systems such as satellite imagery.

WEAKNESSES:

- Corroboration is possible from multiple monitoring stations only for events of magnitude surpassing a certain threshold. The actual number of stations able to contribute to validation of events of a given size varies throughout the world. If events are recognized only when detected by a specific number of stations, then the adversary needs only to disrupt detection by enough stations to cause the specified number to fail to be reached.

- There is a concern as to the formal mechanisms of validating events and the time necessary to do so, especially if non-IMS data is utilized. Without authentication, all data under consideration is suspect until the body of evidence reaches convincing proportions. This of course would always be open to personal judgements resulting in an ad hoc validation process at best.

- The other weakness of utilizing authentication in the IMS is that the adversary has complete freedom as to where to attack the system. This may be different places of the IMS for different threats and for different adversaries.

ISSUES:

- One potential way to redeem some measure of data surety for this option is to tighten the security of the IMS using other means besides data authentication. This might include more secure communications or increased physical security. Of course, these measures would likely result in additional costs as well.

- The critical issue at stake in considering this option is that there exists no reasonable basis for trusting any of the data in IMS which questions the credibility of the IMS itself.

OPTION 2. Authentication at arrival into the IDC

STRENGTHS:

- The main potential advantage of Option 2 is that of providing a limited measure of data surety at a limited cost. The cost will be less than that of authenticating at the monitoring station primarily because authentication and tamper detection equipment do not have to be integrated into the sensor systems in the IMS. This problem is complicated by the fact that there are many differing configurations of seismic stations, not to mention the differing requirements of hydroacoustic, infrasound, and radionuclide systems. However, the implementation of authentication in the IMS has a certain base cost due to key management, data throughput, and unit costs regardless of where it is placed.

- Assuming authentic data prior to the IDC, archived data can be maintained and distributed with integrity.

WEAKNESSES:

- An argument in favor of authenticating at arrival into the IDC that is often made assumes the primary threat to the IMS to be the IDC itself. However even if this were the case, the fact that the IDC is the threat does not prevent that threat from being realized prior to signature generation. Only data in archive at the IDC maintains integrity. Of course, if the archived data is corrupted, modified, or substituted prior to arrival into the IDC, then integrity does not exist in the first place and certainly cannot be maintained.

- Data is vulnerable to tampering at the monitoring stations, the NDCs, or via a man-in-the-middle attack where data is intercepted along its communications route and modified before passing it on.

- Authentication at the IDC "blesses" potentially tampered data. With a reasonable chance of tampering with data prior to the IDC, authentication may only add a false sense of security to the IMS.

ISSUES:

- The critical nature of tamper protecting the data prior to signature generation can drive the design of other elements of the IMS. Essentially, the following assumptions are made for the Option 2 to be credible. These assumptions may be inherent to the IMS or may be supported by explicit enhancements to the system.

    1. The primary threat to IMS data integrity is within the IDC where the data is centrally located and easily modified.
    2. The cost to the adversary of attacking data at the stations or NDCs is prohibitively high.

3. The cost of applying data authentication at every monitoring station is prohibitively high.

Acknowledgment of these assumptions drives the design of the IMS in the following way:

1. Accept assumption 1 and maintain integrity of data located within the IDC with authentication upon arrival into the IDC.
2. Enhancing the IMS to make assumption 2 as true as possible. This results primarily in focusing on designing a communications system that makes it difficult to attack the necessary station data and designing a tamper protection system to make it difficult to attack the data at the IDC prior to authentication.
3. Assumption 3 is definitely the most critical area of debate. If costs of extending data authentication to the monitoring station are indeed prohibitively high, then Option 2 becomes the primary authentication option.

- The addition of data authentication to the IMS will require trust to be placed in a cryptographic authority for key management. Although the trust in this authority can have various forms (distributed, central, etc.), it will known and agreed upon by treaty participants.

- The main argument against the credibility of Option 2 as data surety solution is that the basic assumptions are errant. Therefore, no reasonable basis for trusting data prior to the IDC exists. However, this argument cannot be held up without accurate cost figures of data authentication.

OPTION 3. Authentication at the monitoring station

Before this option is evaluated, "authentication at the monitoring station" must be defined. Authentication at the station is intended to imply full data integrity or data integrity across the entire IMS, from source phenomenon to end user. In practice, signature generation is applied as soon after the data is in digital form as possible. Therefore, the source phenomenon must be sensed and converted to digital form before authentication can take place. The implication here is that the source information must be protected (guaranteed not to be changed) until its signature has been generated. A tamper boundary is typically established around the sensor, data acquisition equipment, and data authentication equipment to ensure data integrity prior to signature generation. Of course, the authentication equipment must also be protected against tampering to ensure proper authentication.

STRENGTHS:

- The strength of Option 3 is its provision of data integrity throughout the entire IMS from source to end user. This means that there are no obvious holes that an adversary can exploit. The adversary will most likely be forced to attack the IMS at the source of data and the key management system.

WEAKNESSES:

- As compared to authenticating at the IDC, the cost associated with authenticating at the monitoring station will be higher. The key management costs will be similar with key distribution costs increasing. Authentication units may be of a different design than that for Option 2 due to the environmental nature and space concerns of each monitoring station. The highest additional cost may be in the development of effective tamper detection/protection mechanisms for the various stations.

ISSUES:

- The purpose of authenticating at the monitoring station is to ensure data integrity from the point of data acquisition to the IDC and beyond. In other words, the intent is to offer data integrity to the complete IMS. In order to ensure data integrity at the point of data acquisition, effective tamper protection must be in place to guarantee that the original, pre-authenticated data has integrity. As one can imagine, effective tamper protection can be a substantial technical challenge, especially against a dedicated adversary, and can result in substantial costs. However, without effective tamper protection, fraudulent data can be authenticated which may be a worse situation that offering no authentication at all because the monitoring community may result in a false sense of security.

- The addition of data authentication to the IMS will require trust to be placed in a cryptographic authority for key management. Although the trust in this authority can have various forms (distributed, central, etc.), it will known and agreed upon by treaty participants.

- Authentication of data at the monitoring stations provides a reasonable basis for trusting data throughout the IMS.

AUTHENTICATION OF OTHER SENSOR SYSTEMS

At the writing of this paper, the feasibility of authenticating data at monitoring stations other than seismic is under investigations. A critical issue in applying an authentication system is that of providing adequate tamper protection to the sensor system. Borehole seismic systems offer the advantage of using the earth as a tamper barrier and the seismic sensor itself as a tamper detector. In contrast, the non-seismic sensor systems do not inherently detect intrusion into the critical areas of the sensor system. A preliminary evaluation of radionuclide, infrasound, and ultrasonic monitoring systems indicates that authentication could be integrated with the sensor electronics and standard tamper detection mechanisms put in place. As is often the case, the cost of employing the proper steps to ensure trust in the authenticated data becomes a crucial issue. Cost estimates of utilizing data authentication in each sensor system are forthcoming.

6. CONCLUSIONS

Data authentication offers a method for providing confidence to a large number of users that the data they receive is authentic. However, the cost, impact, and introduction of new security issues (e.g. key management) limits the effectiveness of external data authentication as a method of ensuring data integrity. Future work will attempt to quantify the nature of the data integrity problem by measuring the severity and likelihood of various attacks and the effectiveness, impact and costs (short term and long term) of safeguard options. The conclusion drawn from this paper is that there exist two credible data authentication options that favor differing characteristics of the IMS. Option 2 in the paper places an emphasis on trust prior to the IDC and low cost while offering negligible data integrity safeguards. Option 3 provides a high level of data integrity throughout the system at a higher cost relative to Option 2. The higher cost of Option 3 reflects the realization that if data authentication is used at all, it must be implemented with a complete system approach that addresses all the data surety concerns that accompany data authentication. In other words, if data authentication is to be used, it cannot be employed haphazardly and a system security approach to the design of the IMS is essential (see [1] and [2]).

It is hoped that the information presented in this paper helps to focus the current discussions and leads to more informed decisions in anticipation of the CTBT. Based on our estimate of the importance of data authentication as a data surety measure and a rough estimate of costs, it is recommended that public key data authentication be applied at all critical monitoring stations (Option 3). However, it is clear that investigation into the costs of this data integrity solution in more detail is necessary. This effort is recognized as being crucial and is forthcoming.

REFERENCES

[1] T. J. Draelos, R. L. Craft, "Comprehensive Test Ban Treaty International Monitoring System Security Threats and Proposed Security Attributes", *Sandia National Laboratories Report SAND96-0536*, March, 1996.

[2] R. L. Craft, T. J. Draelos, "Initial CTBT International Monitoring System Security Findings and Recommendations", *Sandia National Laboratories Internal Report*, February 7, 1996.

Distribution:

1 AFTAC/TT
Center for Monitoring Research
Attn: Dr. Robert Blandford
1300 North 17th Street
Suite 1450
Arlington, VA 22209-2308

3 Air Force Technical Applications Center
Attn: Frank Pilotte, TT
David Russell, TTR
Bruce Varnum, TTD
1030 S. Highway A-1A
Patrick AFB, FL 32925-3002

1 DC/ ACIS
Attn: Larry Turnbull, 4W03
New Headquarters Building
Washington, DC 20505

2 Department of Energy
Attn: Leslie Casey, NN-20
Dave Watkins, NN-40
1000 Independence Avenue SW
Washington, DC 20585

2 Lawrence Livermore National Laboratory
Attn: Dave Harris, L-205
Jay Zucca, L-205
P.O. Box 808
Livermore, CA 94551

3 Los Alamos National Laboratory
Attn: Wendee Brunish, MS F659
Mark Hodgson, MS D460
Rod Whitaker, MS F665
P. O. Box 1663
Los Alamos, NM 87545

2 DATSD (NCB)/NT
Attn: Dr. Ralph Alewine
Dr. Steven Bratt
1901 N. Moore Street
Suite 609
Arlington, VA 22209

2 Pacific Northwest Laboratory
Attn: Rich Hanlen, MS K6-48
Ray Warner, MS K6-40
P.O. Box 999
Richland, WA 99352

1	MS 0458	Laura Gilliom, 5133
1	0419	Bob Gough, 5336
1	0979	Dale Breding, 5704
1	0979	Larry Walker, 5704
5	0655	Tim Draelos, 5736
1	0655	Pres Herrington, 5736
5	0451	Rick Craft, 9415
1	0451	Judy Moore, 9415
1	1138	Ralph Keyser, 9432
1	0619	Tammy Locke, 12615
1	9018	Central Technical Files, 8523-2
5	0899	Tech. Library, 4414
1	0619	Print Media, 12615
2	0100	Document Processing, 7613-2, for DOE/OSTI