LA-UR- 98-3163

Approved for public release; distribution is unlimited.

Title: RadNet: Open Protocol for Radiation Data

CONF-980733--

Author(s): Brian Rees, ESH-1
Keith Olson, ESH-1

J. Beckes-Talcot, S. Kadner, T. Wenderlich, M. Hoy, W. Doyle. Aquila Technologies Group, Inc., Albuquerque NM

M. Koskelo, Canberra Industries, Meridian CT

Submitted to: Institute of Nuclear Materials Management annual meeting, July 1998

Los Alamos
NATIONAL LABORATORY

DISCLAIMER

RadNet: Open Network Protocol for Radiation Data

B. Rees, K. Olson, Los Alamos National Laboratory
Los Alamos, NM 87545
E-mail: brees@lanl.gov

J. Beckes-Talcott, S. Kadner, T. Wenderlich, M. Hoy, W. Doyle
Aquila Technologies Group, Inc.
Albuquerque, NM 87113
E-mail: wendyd@aquilagroup.com

M. Koskelo, Canberra Industries
Meriden CT 06450

ABSTRACT

Safeguards instrumentation is increasingly being incorporated into remote monitoring applications. In the past, vendors of radiation monitoring instruments typically provided the tools for uploading the monitoring data to a host. However, the proprietary nature of communication protocols lends itself to increased computer support needs and increased installation expenses. As a result, a working group of suppliers and customers of radiation monitoring instruments defined an open network protocol for transferring packets on a local area network from radiation monitoring equipment to network hosts. The protocol was termed *RadNet*.

While it is now primarily used for health physics instruments, RadNet's flexibility and strength make it ideal for remote monitoring of nuclear materials. The incorporation of standard, open protocols ensures that future work will not render present work obsolete; because RadNet utilizes standard Internet protocols, and is itself a non-proprietary standard. The use of industry standards also simplifies the development and implementation of ancillary services, e.g. E-mail generation or even pager systems.

NEED FOR A UNIFORM COMMUNICATION PROTOCOL

A computer protocol is a method to communicate between two devices. It specifies the order of specific information contained within it, and in the case of RadNet, provides numeric codes for various conditions that an instrument may experience and its measurement units.

Until RadNet, communication protocols for radiation detection instruments have been proprietary. Proprietary protocols are usually expensive to purchase and maintain and offer limited, if any flexibility. Modification of proprietary protocols usually requires the original programmer or extensive work to reverse engineer the protocol. In the rapidly changing computing environment we live in, protocols must be easily modified in order to stay connected to rapidly evolving computer operating systems.

Proprietary protocols are usually designed for a single instrument, system, or manufacturer. Once a particular system is installed, the cost to add capabilities can be prohibitive. This limits the potential for incorporating the best available technology in the future.

Proprietary protocols are usually designed to do a few tasks, with little or no ability to add capabilities in the future. As other technologies advance, unforeseen capabilities may become feasible if a protocol is open for modification.

Using a proprietary protocol involves specialized computer programming for data storage, display, and manipulation. As the programs for data storage and manipulation are upgraded, these capabilities may degrade or even become obsolete. The provided program may not match the look and feel of other programs used, necessitating costs for training and time for familiarization. The program may not include desired capabilities or may force payment for undesired capabilities.

When an open, standard protocol is used, devices can be exchanged with very little trouble; a computer keyboard is a good example of this. Instruments that use the RadNet protocol can be changed out without concern for "downstream" services.

DEVELOPING RADNET

The RadNet protocol specifies the order of specific information contained within a communication. The protocol provides (a) numeric codes for various conditions an instrument may experience and (b) the units of the measurements the instrument conducts.

The RadNet protocol was developed at Los Alamos National Laboratory in collaboration with Eberline Instruments of Santa Fe, NM. The protocol has been adopted as a national standard by the Nuclear Suppliers Association, and is an open standard, available to all. RadNet is available at http://drambuie.lanl.gov/~radnet. It has been in use at the Los Alamos National Laboratory Plutonium Facility since March 1997, has been installed in nuclear power plants, and is being considered by more nuclear power plants and other Department of Energy facilities. It is also a subject of interest at the IAEA.

The RadNet protocol is open to all manufacturers, so the best available technology can be used; regardless of who makes or sells it. Any RadNet software can be used with any RadNet compliant instrument, making each an independent purchasing decision. RadNet has been designed to use other standard protocols, so future growth and improvement is fully enabled. There are a number of programs written to use RadNet information, some commercially available, and some written by the Information Services (IS) staff of facilities in order to match their corporate computing look and feel.

COMMUNICATION METHODS

The Internet's distributed communication architecture is ideal for communicating between numerous instruments and computers. The speed of communication across a local area network (*Intra*net) is also considerable when compared to current RS-232 and RS-485 serial-based networks.

Instruments can communicate data using wires, or using wireless methods such as Radio Frequency (RF) or Infrared (IR). The data can be transmitted on dedicated (network) connections [the instrument(s) alone] or the connections may be shared with other services. There are applications that require dedicated wire lines, but the flexibility to use any method can be useful. The ability to use computer networks and standard network protocols reduces costs and enables flexibility and future enhancements. Unfortunately, most systems that use proprietary methods lack the flexibility to use wireless systems or to share data lines with other services, resulting in increased initial and overall costs.

RadNet permits instruments to communicate measurement data across networks using the User Datagram Protocol (UDP). The UDP protocol is a standard Internet protocol that allows greatly reduced network overhead and increased simplicity. Many Internet communication methods use a considerable amount of the network to communicate, which limits the amount of information that can be passed. The UDP protocol

uses a small fraction of the bandwidth of the more commonly known TCP/IP protocol and is well suited to this application.

With standard networking protocols, ancillary services are easy to add and implement. For example, the paging system at Los Alamos National Laboratory uses E-mail to send pager messages (most paging systems do). We were able to use the existing system to send pager messages when an instrument alarms or malfunctions.

USING THE DATA

Retrieving and communicating data from an instrument is not enough. Timeliness and quality assurance issues are important to ensure that the data is useful.

With RadNet, instruments ship data onto the network at some user-set time, and during any change in instrument status. This results in "*I'm OK*" messages being sent by the instrument at a time interval less than some critical time interval.[1] For instrument status changes (alarms, malfunctions, etc.), the time interval can be set for any rate, usually less than the normal status rate. If a normal status message is not received within some user-set time, notification can be sent of a communications failure.

Having "*I'm OK*" messages demonstrates that the instrument was functioning when an alarm occurs or if its operability is questioned.

RadNet allows instruments to remotely conduct source response checks, a feature which is available on some instrumentation. A computer program can source check instruments and report results as specified by the user.

Programs used with RadNet can be configured to display and store data in any format specified by the user (database, spreadsheet, etc.).

REMOTE MONITORING APPLICATIONS

Remote monitoring systems have typically been unique and limited in flexibility. Therefore, costs for design, installation, start-up, and maintenance are often considerable. RadNet protocol allows radiation detection instruments to communicate across computer networks without (a) significant impact on the network or (b) the need to configure monitoring computers.

RadNet was designed for health physics applications, but is ideally suited for other remote monitoring applications. RadNet is also designed to utilize off-the-shelf equipment in order to leverage some of the billions of dollars spent to capitalize on network capabilities. When considering remote monitoring, the RadNet protocol, its infrastructure, and end uses should be considered.

SECURING THE DATA

Successful implementation of remote monitoring systems hinges on the demonstration of sufficient reliability in the technical means to guarantee message authenticity and security in data transmission. This

---

[1] If you must have data every 10 minutes to ensure a material manipulation cannot occur, the critical time would be 5 minutes, this allows one message to be "lost" (less than 0.1% probability), and if two messages were not received an alert could be issued.

creates the need for implementing authentication and encryption techniques to validate the source of data and ensure privacy of data in safeguards applications.

The current plan is to transfer cryptography technology that is operational and approved by the IAEA to the RadNet standard. This transfer provides for a well proven implementation with minimal development. The IAEA approval transfers the benefit of 3rd-party vulnerability assessments and the confidence in the implementation that those assessments provide.

In this way, both authentication and encryption can be implemented in a way that is (1) exportable, and (2) minimizes the complexity of the key management system. Both of these implementation features are extremely important to the legal delivery of the systems abroad, and to make such systems administratively feasible to organizations like the IAEA.

Significant attention must be paid to key management and distribution in order to preserve the long-term integrity of the data. Public-key cryptography is the key management method proposed as it significantly eases the key management burden when compared to other options.

Signing and Signature Verification (Authentication)

The objective of authentication is to allow anyone to verify the signature and thus be sure that the attached data (message) is valid and has remained unaltered since the signature was attached. A digital signature does not hide data from anyone; it is still plain text. Consequently, the entire original message is available for use by other applications as if the signature were not present. To the extent that the original document contains information that verifies the source of the data, then the digital signature also certifies that the data originated from a specific sensor.

As illustrated in Figure 1, the signature is provided in two steps. In the first step, the transmitter's *public* key is appended to the message and the resulting combination is processed through a secure hash function such as RSA's MD5 algorithm . These functions are available from certified libraries and produce a 128-bit representation (digest) of the input that is sensitive to a change of only one bit in the entire input. The second step is to encrypt the digest with the transmitter's *private* key to produce the signature. The signature is then appended to the compound structure to form an authenticated message.

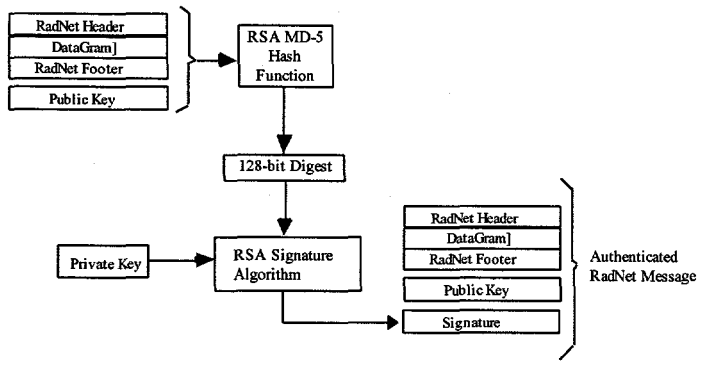

Figure 1: Authentication Process

Because the public key is appended to the signed document, any receiver can verify the authenticity of the message without access to the transmitter's private key. Furthermore, since no one has access to the private key, the signature cannot be forged.

The signature is verified by repeating the signing process. That is, the signature is decrypted with the public key. Then the compound message without the signature is submitted to the same hash function as the transmitter's. If the resulting digest matches the decrypted signature, the document is valid. Verification of messages can be centralized in a server before distribution to the message processing clients; or each client can verify the signatures. The choice of implementation would depend upon the system as a whole and the actual end use. The signing and verification process remain unchanged.

In the RadNet domain, each UDP packet of a compound message would be independently signed.

Encryption and Decryption

The encryption process is intended to prevent any unauthorized person from viewing the data. However, encryption does not necessarily authenticate the data. Encryption introduces a complication into the normal flow of data. Any part of the "message" that is encrypted cannot be read by any application that does not decrypt it first. This can become problematic if services are used to sort, route, store, or otherwise operate on the data or the packet header. Consequently, encryption is not transparent, as is authentication.

Conceptually, encryption operates like authentication run backwards (see Figure 2). The *recipient* of the data generates the key pairs, keeps the private key secret, and distributes the public key to every device that will send data to the recipient. (In principle, there could be a key-pair for every device) The public keys can be distributed over the Internet if desired. Each device uses the public key for encryption. Once data is encrypted with the public key, only the holder of the corresponding private key (the desired recipient) can decrypt and read the data.

Because anyone with the public key can send data to the recipient, it is possible to "forge" data. Therefore, it is always advisable that data be signed (authenticated) before it is encrypted; and furthermore, that the keys used for encryption and authentication be different.

Unfortunately, there is a pragmatic problem with encryption. Secret-key methods are fast; but impose a nearly impossible key management burden on the user. Public-key methods reduce the key management problem but are very slow and compute-intensive. In general practice, a combination of the two methods is used. As shown at the top of the figure below, each message is encrypted using a secret-key algorithm with a key that is uniquely generated for each data package. Once the ciphertext is produced, the unique secret key is encrypted using public key methods to produce a "cipher-key" The encrypted secret key and the public key are pre-pended to the encrypted message to produce a "packet". In common practice, this technique is known as an "RSA envelope."

The result is that the data is encrypted using a fast algorithm and the key for decrypting it is distributed with the data in a way that can be recovered using the more complex public-key algorithm. Further, each data object uses a unique key, so that an attacker would have to cryptanalyze every data item independently; i.e. the key from one data item would have no value for the next.

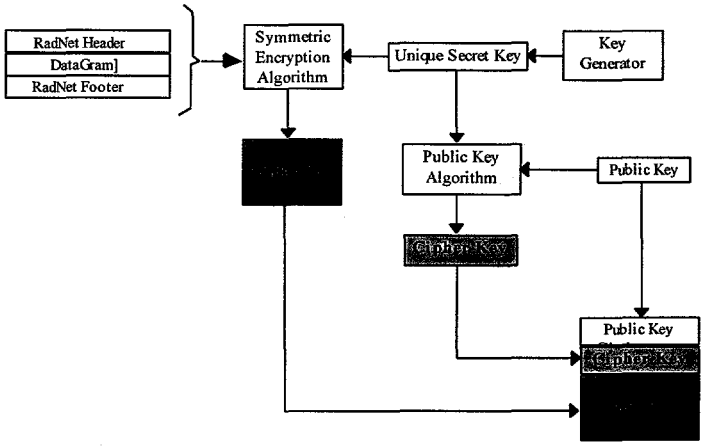

Figure 2: Encryption and Decryption Process

SETTING-UP RADNET SYSTEMS

The simplicity and standardization provided by RadNet allows for a remote monitoring system that is as large or small as desired, from one to thousands of instruments, without trouble.

Setting up instruments to communicate with RadNet is not complex, and can be performed by instrument personnel that have experience with computer Intranets, or with the assistance of corporate network personnel. Legacy instruments can be adapted in a number of ways, and as the protocol gains acceptance it is expected that additional methods will become available. An article in Radiation Protection Management (Rees and Olson, 1997), available on the RadNet website (http://drambuie.lanl.gov\~RadNet) describes the basics of RadNet systems is greater detail. A second article, discussing setting up a RadNet system is in press (Radiation Protection Management).

As shown in Figure 3, a variety of instruments may be observed in operation at the NN-SITE (http://www.nn-site.com). This site allows manufacturers to demonstrate their compliance with the RadNet protocol, and to allow testing of RadNet programs by programmers.

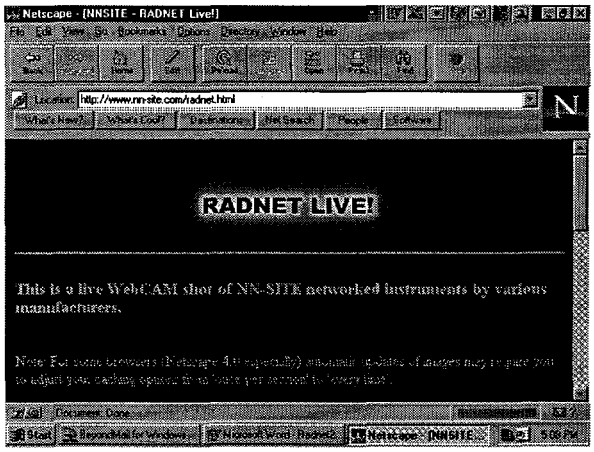

Figure 3: RadNet Demonstrations on the Internet

SUMMARY

By providing the structure for information that is passed to and from instrument and computer, the RadNet protocol enables a variety of instruments to communicate with any computer or group of computers. The advantage of a standard, open protocol is that a RadNet-compliant instrument may be updated or replaced with an instrument from a different manufacturer and the program that uses the instrument's data will continue to function. In addition, a RadNet-compliant instrument can be replaced without changing the setup of client computers. This flexibility lends to decreased computer support needs and decreased installation expenses, both essential in the current safeguards environment.