Category: Informational

S. Ryckman
SIMS, Inc.

Security Industry Internet Protocol for Alarm Transmission (SIIPAT)

<draft-rfced-info-ryckman-01.txt>

Status of this Memo

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract

This document suggests a method for delivering alarm information over the Internet. All communication shall use an encryption algorithm for transmission of the data. An immediate response from the host will be used for verification of receipt of the message.

This transmission method may be use as a backup transmission method to traditional dial-up or leased line methods, or as a primary transmission method with traditional methods becomming the backup.

Due to the required security of the data being transmitted, the encryption algorithm used will only be released on a need to know basis to software developers in the Alarm/Security Industry.
A non-disclosure agreement will be required. Terms and conditions of the licensing will depend on the intended purpose for use and may require a non-competition agreement or licensing fees.

The Internet Assigned Numbers Authority (IANA) has assigned port 1733 for the registered use of SIIPAT transmissions.

1. Introduction

This transmission protocol was developed to eliminate the need for dial-up communications to send short data bursts of alarm information. Many times, the amount of time it takes to seize the dial-up phone line, dial the number and wait for an answer by the alarm receiving equipment is much greater than the amount of time it takes to transmit the data itself (even at 300 baud). Since many corporations and government agencies as well as alarm companies already have dedicated Internet connections, it seems resonable that it could be used as a quick transmission method. Due to the inherent probability of failures of the network at some point between origination and reception of the alarm signal, it should NOT be used for the sole transmission path for any signal. This transmission method can be treated with the same concerns as a typical radio alarm transmission, quick but not entirely absolute.

Throughout the remainder of this document the following terms will be used.

Port/Socket - Used interchangably to refer to the logical connection created when the client software polls the host on a particular port number, in this case port 1733.

SIIPAT - Security Industry Internet Protocol for Alarm Transmission (Pronounced Si-Pay).

Server - The software running at the Alarm Company which is connected to the Internet and monitoring an IP address port.

Subscriber - The software/device at the protected location.

2. System Philosophy

Proposing an alternative method of transportation of alarm signals is not as easy to implement as it sounds. A very simple adoption of such a feat could be accomplished with normal Email. This would not provide immediate notification of receipt however, and would open the system up to tampering from external sources. Clearly a secured encryption routine must be used, to prevent people from creating false signals or using the protocol for sending non-alarm information, as is possible with existing transmission formats. The principle of SIIPAT is to provide security to the alarm transmission process not found currently. This is security both for the originator of the alarm signal (increased transmission speed) and for the alarm company (reduction of false signals due to tampering). Until every home has it's own direct connection to the Internet, SIIPAT can not be used for every alarm system. It's primary purpose is for commercial applications or where the alarm signal may originate from a non-customary device such as a program on a computer used for monitoring network or environmental conditions, home automation/access control computerized systems or from radio network providers for vehicle location/tracking purposes.

SIIPAT itself does not include definition for the equipment on either end of the transmission, only the format of the data in between. Implementation of SIIPAT may include a dedicated machine to act as the server or use of an automation software package which supports the SIIPAT interface directly. The way the protocol is designed supports simple "generic" transmissions as well as emulating specific receiver signals so that an automation package can pass the message to an existing receiver interface.

3. Why use the Internet to send alarm messages ?

Every day, more and more alarm companies are changing from small "mom and pop" companies, to nationwide or global monitoring stations. With the ever increasing competition from other companies, an alarm company must remain unique to remain in business. Switching from a local geopgraphical area of coverage to a larger scale brings with it increased advantages, but also increased problems. Using customary techniques requires either the use of "800" numbers at the alarm company (at great expense to the company) or long distance calls from the subscriber (where they eat the cost of the phone call). As contracts between large corporations and a single alarm company continue, the ability of one central location to monitor a chain of stores around the world becomes more and more expensive. Sending open and close activity reports from a panel around the world could easily add up to the hundreds or thousands of dollars a month in customary phone long distance charages. Because of this expense most sites do not implement test supervision signals unless maybe they are only once a day. With SIIPAT supervision is a two-way street with the alarm company able to "inquiry" the status of a particular system at any moment, even every couple seconds if high-security warrants it.

4. The SIIPAT Protocol

The SIIPAT protocol is a sequence of commands and replies, and is based loosely on the design of many other Internet protocols currently in use. Please note that the protocol as described does not take into consideration the encryption process which occurs before the data is actually transferred across the Internet, if implemented.

SIIPAT has several input commands (the first 6 characters of each are significant) that solicit various server responses. A "burst mode" transmission is also supported whereas the entire authentication and alarm message can be sent on the initial request for the socket. SIIPAT also supports several status commands which can be used by the server to check the status of a subscriber at any time.

The messages the subscriber equipment may send vary depending on the equipment in use. Not all subscriber equipment may be capable of or have need to transmit all the various types of messages. All servers should be capable of receiving them all however.

Each message transmitted is prefixed by an STX character (Ascii 2) followed by a two character alphabetic 'Message Type' code. The Message Type determines what the remainder of the message contains as well as the length of the entire message. All messages will conform to the following message format:

```
 <stx>    - Start of Transmission identifier (Ascii 2).
 msg type - Two character Message Type.
 length   - Two digit length of variable data to follow (01-99).
 data     - Raw data message of length characters total.
 <etx>    - End of Transmission identifier (Ascii 3).
```

The server sends replies or status inquiries prefixed by an ENQ character (Ascii 5) and terminated by an EOT (Ascii 4).
The messages the server should be expected to return are grouped in the following catagories to make it easier for the subscriber equipment to determine the necessary action based solely on the first character.

```
 1xxx - Success, Proceed, Verified
 2xxx - Accepted but Incomplete
 3xxx - Authentication Error
 4xxx - Protocol Error
 5xxx - Duplicate Transmission
 8xxx - Network Busy/Error
 9xxx - Status Inquiries
```

Typically, the subscriber initiates the connection with the server. Upon opening the connection, the server issues a "1RDY" message (indicating the willingness of the server to accept SIIPAT commands). At that point, the subscriber sends it's data stream and awaits a response from the server indicating the success or failure of the transmission. The subscribers unit should also be capable of determining no response within a set time frame and resort to customary alarm transmision paths or attempt to contact a differant server at a differant IP address.

Status messages can be initiated by the server if the subscriber unit supports it. Each subscriber unit shall at minimum support the type 9999 server response for inquires. The subscriber unit simply needs to respond with a status message with no variable length data supplied. This signifies to the server that this host does not support/want additional status messages to be performed against it. If the subscriber unit supports additional status messages, it will respond with the types of the status messages that it supports in the variable data. This allows for multiple vendors equipments with differant capabilities or for the subscriber to limit the status inquires that can be performed on their unit.

4.1 Examples of "simple" SIIPAT Transmissions

The following are two examples of how an alarm message may be sent to the server using SIIPAT. Note that the data transferred between subscriber and server may be encrypted before it is sent which is not shown in these examples.

Both these examples show the authentication of site 1234 with a password of PASSWORD. Two alarm messages are being sent for the alarm account number of 4321, one is a code 99 and the other is a code 31, both using the SIIPAT 4x2 format.

4.1.1 Standard Transmission

```
Subscriber                         Server
--------------------------         -----------------------------------
Open Connection               -->
                              <--  1RDY17ABC ALARM COMPANYv1.00
ID041234                      -->
                              <--  1PW?14Enter Password
PW08PASSWORD                  -->
                              <--  1BGN18Begin Transmission
AM11!!4X2432199               -->
                              <--  1RCV11!!4X2432199
AM11!!4X2432131               -->
                              <--  1RCV11!!4X2432131
CC                            -->
                              <--  1SNT152 Messages Rcvd
Close Connection
```

4.1.2 Burst Transmission

When a burst transmission is sent, all the data is sent on one stream. This stream can occur at the time of opening the connection or after the 1RDY message is returned depending on the subscriber unit and it's capabilities.

```
Subscriber                         Server
--------------------------         -----------------------------------
```

```
Open Connection              -->
                             <--  1RDY17ABC ALARM COMPANYv1.00
ID041234PW08PASSWORDAM11!!4X2432199AM11!!4X2432131
                             <--  1SNT152 Messages Rcvd
Close Connection
```

4.2 Subscriber Messages

The following sections briefly describe the possible messages that a subscriber unit can send. All these messages are prefixed by an STX character (Ascii 2) and terminated by an ETX (Ascii 3).

4.2.1 "ID" Messages - Logon Information

Each transmission must be authenticated against a table the server maintains to ensure that no tampering is being attempted. Therefore each transmission must include an ID type message before actual messages will be acknowledged from the subscriber unit.

```
ID             - Message Code.
xx             - Length of ID to follow (01-99).
.....          - Actual ID transmitted.
                 (This ID may or may not coincide with the
                  actual alarm number depending on preferance.)
```

4.2.2 "PW" Messages - Password Authentication

In order to determine that a random ID wasn't guessed, a password associated with each ID must also be sent. Whether the server actually verifies this information or not is normally configurable.

```
PW             - Message Code.
xx             - Length of Password to follow (01-99).
......         - Actual Password transmitted.
```

4.2.3 "MA", "MS" and "MV" Messages - Alarm Messages

Transmission of actual data is done with Alarm Messages. The three differant types of alarm messages allows the server to sort the messages by priority before sending them to the host computer system.

```
MA             - Message Code.  (Alarm Messages)
    or MS                       (Status Messages)
    or MV                       (Verification Messages)
xx             - Length of Raw Alarm Data (01-99).
........       - Actual Raw Data.
```

The format of the Raw Data for Alarm Type Messages varies depending on the transmitting and receiving equipment. For propeitary implementations this could be any format desired. It is recommended that the following format be used for compatibility so that automation software can parse the Emulated Data from the string and send it to the existing receiver interfaces for that type of receiver. This should ensure that the most current specifications remain in effect for SIIPAT if the manufacturer makes additions to their protocol.

```
!            - Identifies Emulated Data being sent
xxxx         - Format Identifier
   of !4X1   - SIIPAT 4x1 Format
   or !4X2   - SIIPAT 4x2 Format
   or !4X3   - SIIPAT 4x3 Format
   or !CID   - SIIPAT Contact ID Format
   or ADMC   - Ademco 685 Receiver Emulation
   or DMP1   - DMP SCS1 Receiver Emulation
   or FBII   - FBII CP220 Receiver Emulation
   or ITIC   - ITI CS4000 Comp Emulation
   of ITIG   - ITI CS4000 Generic Emulation
   or RMII   - Radionics Modem II Emulation
   or RSIA   - Radionics SIA Emulation
   or SAFE   - Senses Intl. Safecom Emulation
   or SURG   - Surgard xLR Receiver Emulation
..........   - Emulated Data
               (length varies depending on the format
                and is five less than the length of
                the Length of Raw Data specified for
                the Alarm Message Type.)
```

4.2.4 "CC" Message - Close Connection

Requests a summary from the server and once received closes the connection. All subsequent transmissions from the subscriber on this socket are ignored.

4.2.5 "??" Message - Subscriber Status

The server must have sent a type 9 Status Inquiry in order for this message to be generated. When the server wishes to inquire on a subscriber, it opens the socket with the subscriber at the subscribers IP address and port and sends out a 9999 response. At that point the subscriber unit sends out a type ?? message indicating it's abilities for further commands.

```
??              - Message Code.
xx              - Length of available commands (04-96)
yyyy            - Number of the Server Inquiry that this
                  subscriber is capable of.  This is always
```

a four digit number (9000-9999) that repeats. Ie:9990999199929993 would mean that this subscriber is capable of type 9990-9993 status inquiries.

4.2.6 "CL" Message - Cancel Last Message

When this message is received by the server, the last M type message received is thrown away. This is used by subscriber units that detect the data sent back on the 1RCV message from the server was not the same as it sent. Once a subscriber sends this message, it can then begin to retransmit the message.

4.3 Server Responses

The following sections explain the various responses that a server can sent to the subscriber. All these transmissions are started with an ENQ character (Ascii 5) and terminated with an EOT character (Ascii 4).

1xxx	-	Success, Proceed, Verified
2xxx	-	Accepted but Incomplete
3xxx	-	Authentication Error
4xxx	-	Protocol Error
5xxx	-	Duplicate Transmission
8xxx	-	Network Busy/Error
9xxx	-	Status Inquiries

4.3.1 - Success, Proceed, Verified

1RDY - Tells the subscriber that the server is ready to accept data and provides basic information about the server including the servers name and SIIPAT version number.

1PW? - Asks the subscriber unit for a password if required by the server.

1BGN - Tells the subscriber that it has been authenticated and it should begin transmitting signals.

1RCV - Repeats the data received back to the subscriber.

1CAN - The last message was cancelled as requested by a CL message.

1SNT - Tells the subscriber that the messages were sent to the automation system along with a comment which usually indicates the number of signals received. This message should be recorded by the subscriber unit for display as it may contain other information such as a notice to contact the alarm company regarding an outstanding balance or other informational purposes.

4.3.2 - Accepted but Incomplete

2INC - The message sent was incomplete in some way but enough information was received to pass it on. This is most likely caused by a message length field being set longer than the actual data received.

4.3.3 - Authentication Error

3BID - The ID sent is not on file or is blacklisted on this server.

3BPW - Bad or missing Password data was detected.

3BIP - The ID sent is configured to only be accepted from one IP address, which was not the one this message was from.

4.3.4 - Protocol Error

4ERR - An invalid Message Code was received or a message was missing relavent parts or incorrect data.

4TME - Too Many Errors, closing connection. This will only occur during busy socket usage when the same socket experiences more than three errors in a row.

4.3.5 - Duplicate Transmissions

5DUP - The message sent is exactly the same as the previous message from this subscriber. This can be caused when a server response is lost in replying to an alarm message and the subscriber tries again. A time limit for expiration of this feature can be set, or it can be disabled globally.

4.3.8 - Network/Busy Errors

8BSY - The server is too busy to handle the request now. This could be performance related or by lack of sockets available. Every server must be capable of at least 128 concurrent sockets to be approved with SIIPAT.

8HST - An error has occured with the host computer, thus making it impossible for this server to pass on the alarm information.

8TIM - Timeout waiting for message from subscriber.

4.3.9 - Status Inquiries

All Status Inquiries with the exception of 9999 return type MS messages. The format of the returned message varies depending on what was requested. NOTE: The subscriber units shall normally be configured to only accept status inquiries from a host which has an IP address that the subscriber unit is programmed to send messages to. This prevents anyone from being able to ask a subscriber unit for it's status since only valid servers for that subscriber can request it. Additionally, as proposed in the

optional extensions, programming information can be relayed upon additional authentication of the server by the subscriber.
Items marked with an **** require additional authentication.
Items marked with an !!!! also require a secondary authentication.

9000 - Return subscriber name.
9001 - Check Alarm/Restore Status.
9002 - Check Open/Close Status.
9003 - Sends temporary message to subscriber to be displayed on keypad (displayed until next keypad event occurs).
9004 - Changes the permanent keypad message.
9970 - Check Zone Status ****
9971 - Check Partition Status ****
9980 - Arms the system. **** !!!!
9981 - Disarms the system. **** !!!!
9982 - Bypass zones. **** !!!!
9994 - Return Configuration Switches. ****
9997 - Return IP address list. ****
9998 - Change the IP address list. **** !!!!
9999 - Ask the subscriber for it's capabilities. These are returned in an ?? type message.
9GMT - Asks subscriber for GMT offset.
9PNG - Returns 'PING'.
9TM? - Returns the current date/time at subscriber unit.
9TMS - Sets the current date/time at subscriber unit.
9TST - Returns 'TEST'.

4.4 Illegal Commands

Should the subscriber issue an illegal command, the server may respond in one of the two following ways:

4TME Too Many Errors
4ERR Invalid Message Code

4.5 Timeouts

The SIIPAT server can optionally have an inactivity timeout implemented. At the expiration of the allotted time, the server responds "8TIM Timeout" and closes the connection.

5. Author

Steven M. Ryckman, Technical Supervisor
Security Information & Management Systems, Inc.
3112 Teakwood Lane - C.S.M. Division
Plano, Texas   USA   75075

Voice: 972-964-7019

  Fax: 972-964-0902
Email: sryckman@pobox.com

6. Additional Information

For more information regarding SIIPAT, contact Steve Ryckman by one of the above listed methods (preferably by email). A "home page" has also been established with additional information on SIIPAT at the following URL: http://pobox.com/~sims.support/siipat.html