IDA Authenticated Communication Protocol (IACP)

Last modified: June 20, 2007

Introduction

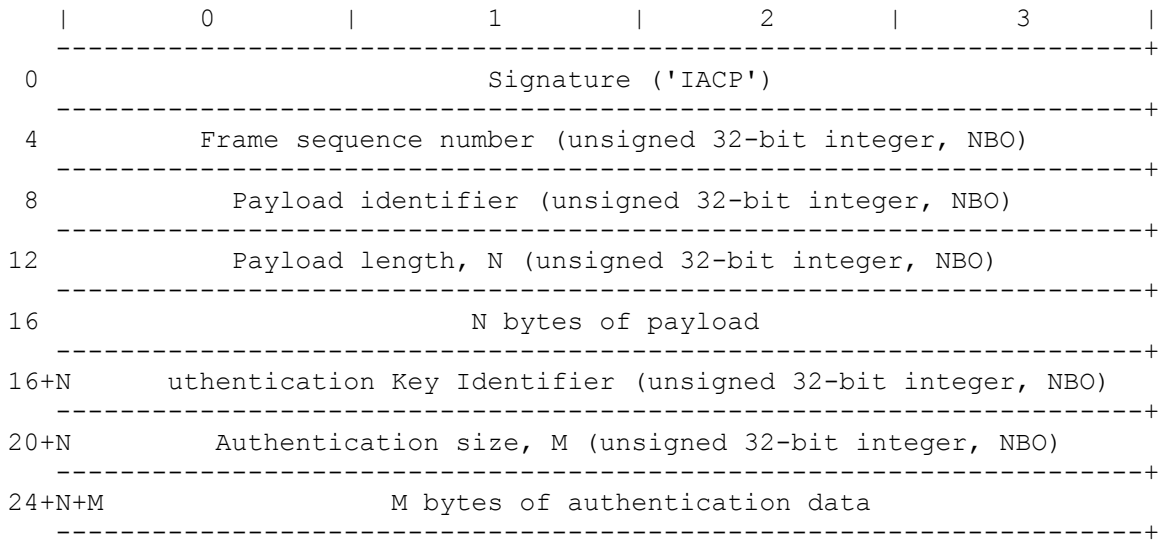
The IDA Authenticated Communication Protocol (IACP) is a TCP/IP based protocol designed for communication between IDA seismic stations, data collection hubs, and TCP/IP enabled digitizers. It allows for, but does not require, the inclusion of digital signatures for authentication of frame contents. The design is meant to be simple and sufficiently general that it can be used for both data communication as well as command and control applications. It is easily extensible to allow for support of new data formats and TCP/IP aware digitizers.

The IDA System Interface (ISI) Toolkit is a C language implementation of the formats and protocols described in this document. Client side source code is available for pickup at

```
ftp://idahub.ucsd.edu/pub/pickup/ISI_Toolkit.tgz
```

IACP Frame Format

IACP communication is done via the exchange of variable length frames over a TCP/IP socket. These frames consist of a 16-byte preamble, followed by a variable length payload, followed by an optional digital signature. The basic frame format follows.



Frame Signature

The 4-byte signature appears at offset 0, and is for IACP frame identification. It is useful for locating IACP frames while snooping the network, and for rejecting casual port probes.

Frame Sequence number

The frame sequence number is inherited from the CD1.1 specification, which requires a unique "serial number" for each frame ever sent from a particular frame creator. It was usefule as a debugging aid during intial development, but is no longer used in the current IACP implementation. It has been retained only for compatibiltiy with deployed systems.

Payload Identifier

The payload identifier is an assigned number that uniquely identifies the type of payload to follow. Identifier values 0 through 1999 have been assigned or otherwise reserved. Identifier values 2000 through 4,294,967,296 are available upon request.

Identifiers 1 through 99 are reserved for the IACP handshake. Identifier 1 is used for the IACP handshake frame:

```
#define IACP_TYPE_HANDSHAKE                    1 /* handshake */
```

Identifier values 100-999 are for reserved IACP I/O control (post-handshake). Of these, the following control frames have been defined:

```
#define IACP_TYPE_ALERT                  100 /* peer disconnect notification */
#define IACP_TYPE_NOP                    101 /* i/o heartbeat */
#define IACP_TYPE_ENOSUCH                102 /* rejected frame notification */
```

Identifier 0 is the IACP "null" frame, and is used to send breaks to the peer process.

```
#define IACP_TYPE_NULL                       0 /* break */
```

All other identifier values are of interest only to the various applications that use IACP as the underlying protocol. For example, identifier values 1000 through 1999 are reserved for use by the IDA System Interface (described in a companion document).

Payload Length

This is simply the number of bytes to follow. Zero is a valid length, in which case the payload identifier is itself the message.

IACP Payload

The IACP payload consists of a block of data. All frames with payloads in the range 0- 999 contain information related to the IACP session, and are interpreted and acted on by the IACP client or server. The contents of all other frames are opaque to IACP and are passed to the user application.

Authentication Key Identifier

The 4-byte authentication key identifier is the identifier of the certificate with the public key required to verify the digital signature. This is the convention used by CTBTO CD1.1.

Authentication size

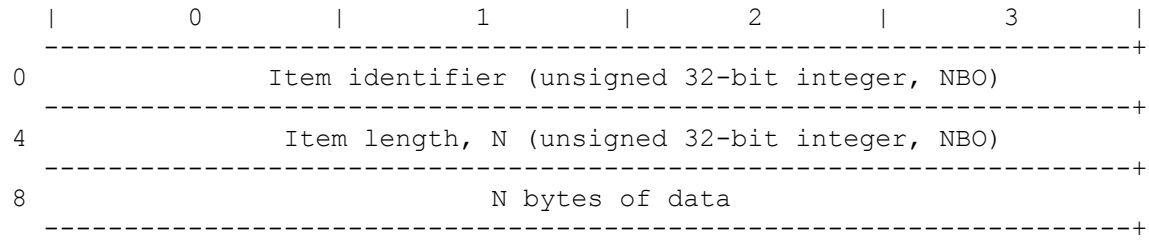
The authentication size is the number of bytes of authentication data to follow. If the frame is not signed then this field would be zero.

Authentication data

This is the digital signature.

IACP Handshake Frame

The IACP handshake frame is a frame with a payload identifier of 1. The format of the IACP handshake frame payload consists of 0 or more subframes that are used to define the connection attributes (timeout interval, buffer lengths, etc). The format of these subframes consists of (length, identifier, value) triples as follows:



The concatenation of these subframes constitutes the payload of the IACP handshake frame. The following handshake subframe identifiers are presently defined:

```
#define IACP_TYPE_PID                           2 /* peer process id */
#define IACP_TYPE_TO                            3 /* i/o timeout */
#define IACP_TYPE_SNDSIZ                        4 /* TCP/IP send buffer len */
#define IACP_TYPE_RCVSIZ                        5 /* TCP/IP receive buffer len */
```

The value field for each of these 4 items is also an unsigned 32-bit integer, however the format allows for the definition of new items which have some other size and type.

Peer process id

The peer process id is tagged with an item identifier of 2 (IACP_TYPE_PID). The peer process id is not required for IACP dialogs to take place, but is sent as a "courtesy" to the peer process. Including the process id of the peer in log messages has been a convenient debugging aid.

I/O timeout interval

The I/O timeout interval is tagged with an item identifier of 3 (IACP_TYPE_TO). The I/O timeout interval is the number of milliseconds to allow for network reads and writes to complete.

TCP/IP Send and Receive buffer lengths

The TCP/IP send buffer length is tagged with an item identifier of 4 (IACP_TYPE_SNDSIZ), while the TCP/IP receive buffer length is tagged with an item identifier of 5 (IACP_TYPE_RCVSIZ). The buffer lengths are given in bytes. A value of 0 is interpreted to mean that the default TCP/IP buffer length, as defined by the underlying operating system, is to be used. Normally that will always be the case, however, this option is provided as it can sometimes aid in improving throughput over certain types of circuits.

IACP Heartbeat Frame

The IACP heartbeat frame can be sent by either side of the connection, but is normally only sent only by the server. The heartbeat frame is an IACP frame with a zero length payload and a payload identifier of 101 (IACP_TYPE_NOP).

IACP Alert Frame

IACP alert frames are sent by the peer immediately prior to terminating the connection. The payload is an unsigned 32-bit integer in network byte order that describes reason for the disconnect. The following cause codes are currently defined:

```
#define IACP_ALERT_NONE              0 /* never sent */
#define IACP_ALERT_DISCONNECT        1 /* normal disconnect */
#define IACP_ALERT_REQUEST_COMPLETE  2 /* request complete */
#define IACP_ALERT_IO_ERROR          3 /* i/o error */
#define IACP_ALERT_SERVER_FAULT      4 /* server error */
#define IACP_ALERT_SERVER_BUSY       5 /* too many active connections */
#define IACP_ALERT_FAILED_AUTH       6 /* invalid frame signature */
#define IACP_ALERT_ACCESS_DENIED     7 /* access to server refused */
#define IACP_ALERT_REQUEST_DENIED    8 /* client request refused */
#define IACP_ALERT_SHUTDOWN          9 /* shutdown in progress */
#define IACP_ALERT_PROTOCOL_ERROR   10 /* illegal frame received */
#define IACP_ALERT_ILLEGAL_DATA     11 /* unexpected frame data */
#define IACP_ALERT_UNSUPPORTED      12 /* unsupported IACP frame type */
#define IACP_ALERT_OTHER_ERROR      99 /* other error */
```

IACP Null Frame

The IACP null frame is a frame with a zero length payload and a payload identifier of 0 (IACP_TYPE_NULL). It is used to indicate the end of a sequence of frames.

IACP session dialog

IACP sessions are done in a client-server fashion. The client establishes a TCP/IP socket connection with a server process listening at some known port. The port number currently used for IDA IACP servers is 39136, an arbitrary value.

After the connection is established, the client sends an IACP handshake frame (payload identifier 1) that *suggests* desired connection attributes to the server. The server replies to the IACP handshake frame with its own handshake frame that describes the *actual* attributes which will be used during the session.

Among the connection attributes is the timeout interval, specified in milliseconds. If no traffic occurs during this interval then each side should declare the connection lost and disconnect. The server is guaranteed to send IACP heartbeat frames (payload identifier 101) at half this interval so some traffic should always be present over a healthy connection.

After the handshake frames have been exchanged, the server waits for commands from the client. IACP commands and responses are frames whose payload identifiers are mutually recognized by both the client and server. Normally these commands will generate a response from the server to the client, but the protocol does not explicitly require this. While the server is waiting for commands from the client, or waiting to generate or send responses, it must also ensure that heartbeats are sent at appropriate intervals, if required to maintain the connection.

How long a connection is maintained is implementation dependent. The server may chose to break the connection after it has received and processed a single request from the client, or it may chose to wait for a new request from the client after it is done with the current request. In any event, if the server detects an I/O error, or encounters an internal error, then it will break the connection. IACP alert frames should be sent by the peer when it has decided to terminate the connection, and its payload includes a code that gives the reason for the disconnect. The protocol does not *require* the use of IACP alert frames, and it is acceptable for either end to simply close its socket without notification. The use of IACP alert frames in initiating disconnects is only to aid in distinguishing between normal disconnects and those due to other problems with the peer. It is up to the client to decide how to respond to a disconnect from the server.

If the client sends a command frame that the server does not recognize, the server will respond with a "no such frame" message. This is an IACP frame with payload identifier 102. It is up to the client to decide the appropriate response to this reject.