*Pre-presentation copy. Paper to be presented at IMSC '97, Pasadena CA on 18 June 1997*

# Improved Coast Guard Communications using Commercial Satellites and WWW Technology

LT Gregory W. Johnson and ET1 Mark D. Wiggins
USCG Research and Development Center
1082 Shennecossett Rd., Groton, CT 06340
Phone: 860-441-2671 Fax: 860-441-2792
gjohnson@rdc.uscg.mil http://comms.rdc.uscg.mil/

## Abstract

Information collection and distribution are essential components of most Coast Guard missions. However, information needs have typically outpaced the ability of the installed communications systems to meet those needs. This mismatch leads to reduced effectiveness of Coast Guard operations. One current need is for Coast Guard aircraft to communicate information on vessels sighted to the shipboard commander quickly and efficiently. The shipboard commander needs to be able to access this information in real-time as well as retrieve related information from historical databases. This paper describes an R&D initiative to demonstrate a new concept of operations to meet this need using COTS technology. A database server installed at the R&D Center which can be accessed via the Internet collects the information and provides it to authorized users using web-based forms. A sighting report (from aircraft and cutters) is entered using the minimum amount of information; this information is then combined by the server with information from historical databases to make a complete record. The users (Coast Guard aircraft, stations, and cutters) access the information using standard WWW browser software. All users connect to the server using either fixed network connections to the Internet, Coast Guard Intranet, or dial-up PPP connections into a remote access server. Commercial satellite systems (AMSC and Inmarsat) provide the communications links for the mobile users (aircraft and cutters). This system was demonstrated in the New England area during March of 1997. This paper describes the concept, implementation, demonstration, and a preliminary analysis of the performance of the communication links to the mobile users.

## Background/Problem Statement

The U.S. Coast Guard's law enforcement operations in the First District (New England area—Figure 1) utilize a medium-endurance cutter (WMEC) to provide the operational control for patrol boats (WPB) and other surface and air units within the District Area of Responsibility (AOR). During these operations, aircraft conduct flyovers of fishing vessels and report the identity, activity, and position of all vessels sighted to the WMEC, which then makes decisions as to which vessels to board and inspect. The accuracy and timeliness of the these sighting reports varies widely depending upon the type of aircraft, range to the WMEC, and weather conditions. Frequently there is no active communications path between the aircraft and the WMEC. Sometimes the information is not reported until the aircraft lands and uses shore-based communications systems. When the sighting information is received by the WMEC, the operational commander makes use of information in operational databases as factors in his boarding decision. [1]

To make effective use of the available resources, the aircraft must have a mechanism for capturing information about the sighted vessels. The aircraft must also have a "real-time" communications path to transmit the sighting information to the WMEC and shore-based operational databases. In addition to the sighting information, the operational commander needs access to the information in the operational databases ashore (historical information as well as current lists of wanted vessels).


*Figure 1— Map of USCG Districts [2]*

## Concept

The Coast Guard has complex communications requirements in that most of the operational units are mobile (ships and aircraft) separated from the information they need to have access to by many, sometime hundreds of miles of open water. Although the amount of data that needs to be moved is relatively small by today's standards, it is bridging the gap to the mobile users that provides the challenge to Coast Guard communications. Under current scenarios, it is a tedious and time consuming task to retrieve law enforcement information from various databases located on shore. It is even harder to add information to these databases. Many times, the process is reduced to handwritten notes being manually entered into the database

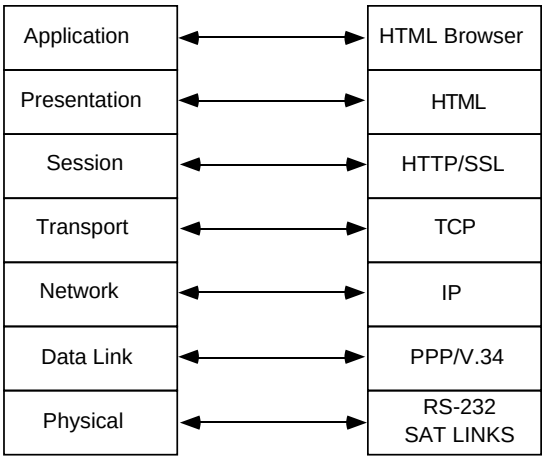


***Figure 2—OWL Project mapped to the OSI model***

after the information is gathered, adding hours to the latency of the information. The retrieval of the information by the mobile client, when possible, is most often by means of an RF link that is at best slow and unreliable. Also the presentation and usability of the information is a challenge since there are many different platforms being used to store, transmit and retrieve the data.

In today's austere budgetary climate, commercial off-the-shelf (COTS) solutions are very much in favor since they are usually the lowest cost to the government. This applies as well to communications, especially satellite communications. In fact, commercial satellite solutions are often the cheapest communications solution, and sometimes the **only** solution to meet Coast Guard communications needs [3].

For this proof-of-concept demonstration, a system was needed to provide over-the-horizon communications to Coast Guard aircraft and ships. The system needed to provide moderate data speeds and be economical to use. The system also needed to be installed and operational on these units in a short period of time. These requirements lead to the selection of the SkyCell™ system from American Mobile Satellite Corp. (AMSC) for the aircraft and patrol boats, and the use of the already installed Inmarsat Standard-A on the medium endurance cutters.

Once the satellite system was determined, the methodology of the data retrieval and transmission and its presentation had to be decided on. A user-friendly environment that required as little end-user training as possible was necessary since Coast Guard personnel are already tasked with performing multiple jobs and have many responsibilities. Most units cannot afford to dedicate one or more person to operate and maintain the communications equipment.

A dial-up Point-to-Point Protocol (PPP) connection using Hyper-Text Transfer Protocol (HTTP) to a world wide web (WWW) server that presented the data in a Hypertext Mark-up Language (HTML) protocol was selected for this project. In other words, providing Internet access to the mobile users and using a web server to collect, store, and distribute the data. The database resides on a server that is accessed via a Transmission Control Protocol/Internet Protocol (TCP/IP) connection and distributed in a Common Gateway Interface (CGI) environment. The TCP/IP connection is provided by a PPP dial-up link via the commercial satellite systems (Inmarsat-A and AMSC). A laptop with an HTML browser such as Netscape™ Navigator or Microsoft Internet Explorer™ is the user interface for the mobile units. The OSI Seven Layer Model [4] mapped fairly well to the communications network established for this project (Figure 2).

The proof-of-concept project is named Operational Web Link (OWL) and the system concept is illustrated in Figure 3. Some of the goals of the project were to:

- minimize user actions (minimal typing, quick, easy)
- provide onetime data entry; eliminate voice relays and multiple entries
- minimize the amount of data to be transferred (utilize links to static databases)
- provide a simple user interface for the mobile users (user shouldn't need to memorize or lookup codes)

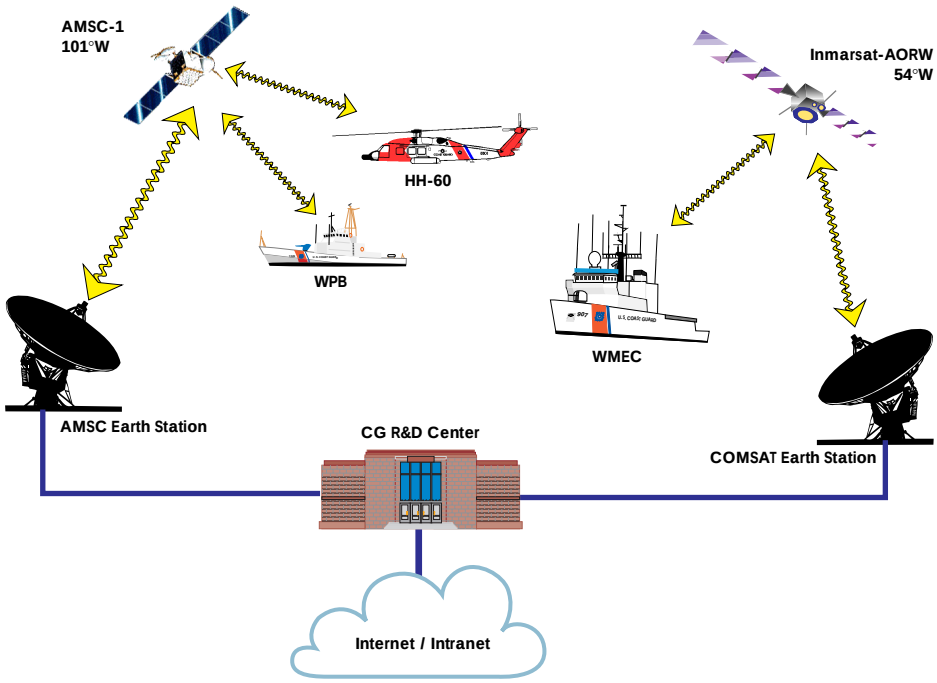


***Figure 3—Operational Web Link Proof-of-Concept Demonstration***

***The United States Government does not endorse products or manufacturers. Trade or manufacturers names appear herein solely because they are considered essential to the object of this report..***

- develop a system that is easy to modify as needed, keeping complexity at a central server
- provide real-time response
- give users only the information they need, when they need it
- provide automatic data transmittal into the main Coast Guard law enforcement database (LEIS)

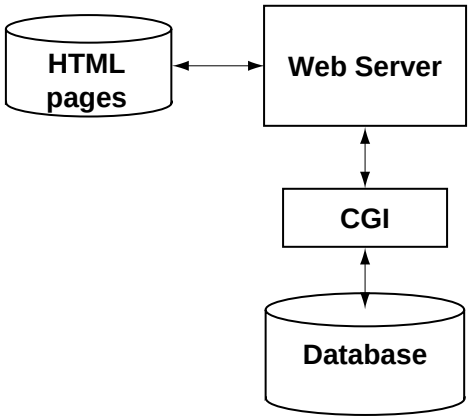


***Figure 4—Generic web server configuration. Each box is a separate application or file(s). They could all reside on the same computer or be running on separate machines.***

## Implementation

With the concept described above, all of the "intelligence" resides in the server; each client (ship, aircraft, or station) merely uses a simple web browser. The server is actually several linked parts as illustrated in Figure 4. The web server is an application that serves up (transfers upon request) various pages (files), typically text files in hypertext markup language (HTML) format. The functionality of the web server is extended using small programs known as CGI (common gateway interface) scripts. The final component, and the most important part for this experiment, is the database. Each of these components is described in more detail in the following sections.

*Web Server*

The web server is the heart of the system. The information in the database is worthless unless it can be distributed and updated with ease. A Macintosh platform was chosen for this rapid-prototype project due to the ease of software configuration and development. The hardware consisted of a 7500/100 PowerPC running System 7.6 with 64 MB of RAM. The web server application used for this experiment was StarNine's WebSTAR™ SSL. The server actually ran two versions of WebSTAR concurrently: one version non-secure and the other secure. The non-secure side serves as our general Advanced Communications Project site [5] and is also used for the training data base that was used to test and train end-users. The secure side was the server used for the experiment.

The database program used was Claris's FileMaker Pro™ 3.0 (discussed in detail below). A CGI acts as the interface between the web server and the database application. The recent trend has been to implement CGIs as plug-ins to the web server software which allows for better performance. There are many COTS solutions to interfacing a FileMaker Pro 3.0 database with the WebSTAR server. The WebFM™ plug-in was used because it provided the ability to use the calculation fields in FileMaker Pro™ to manipulate the HTML which allowed extremely flexible access to the database. Since the HTML is generated "on the fly" as the "GET" and "POST" commands are carried out, the presentation of the data can be tailored according to it's content.

The HTML pages control most of the "look and feel" of the application. The structure of the web site for this application, as defined by the web pages is illustrated in Figure 5. The top level of the site is a designated main page which serves as an entry point for the site. This page offers the user four choices; each choice leads to a different linked page. Each linked page is actually a web form that specifies some interaction with the database—either adding new records (vessel sightings) or searching the database. The pages in the level below this are actually generated by the database in response to the web form. At the bottom of most of the pages is a navigation bar which can be used by the user to go directly to any of the pages.

*Sighting Entry Forms:* The first two choices both relate to the entry of vessel sightings. There are two forms; a short form (Figure 6) designed primarily for the aircraft to enter the minimum amount of information quickly and easily, and the full form which allows for a full information report to be entered. Each of these two forms contains hidden fields which specify various attributes and the database name. The rest of the form consists of the information fields that the user can fill in. Pull-down menus have been used as much as possible to minimize the amount of typing by the user. In all cases where the entry needs to be coded for transmission into the main Coast Guard law enforcement database (LEIS), a pull-down menu has been used so that the user is shielded from the codes. The user is presented with a plain language list, which the form translates into the appropriate code.

The form is posted by the user clicking on the SUBMIT button (labeled "Send Sighting" on the form). This directs the

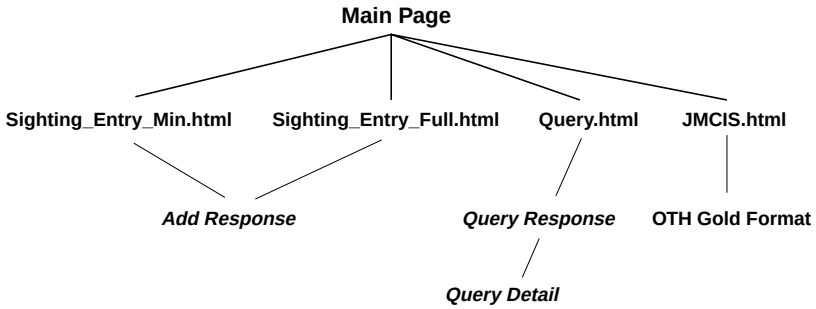


***Figure 5—Web site structure.***

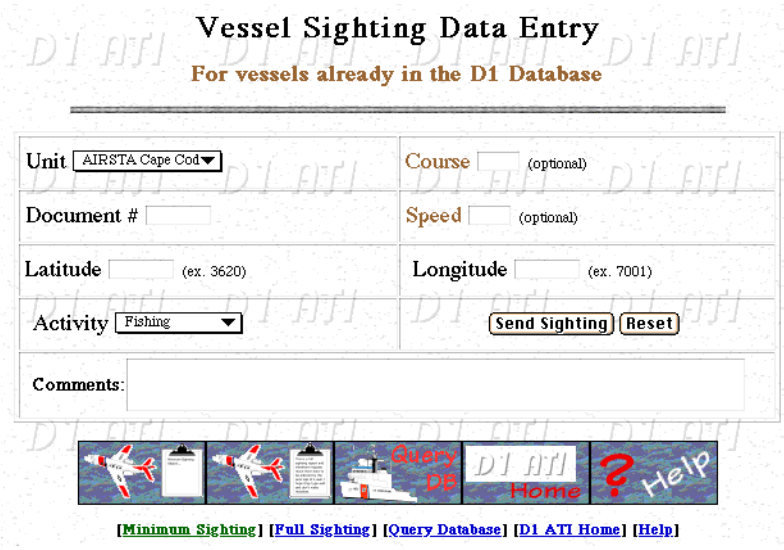


***Figure 6– A screen shot of the Minimum Sighting Entry page. The appearance will vary slightly depending upon the computer platform and browser software.***

browser to transfer the data from the fields of the form (not the entire form) to the web server which hands the information off to the database through the CGI. The database then generates the appropriate reply (actually this is specified by one of the hidden fields on the form), hands off the HTML formatted text to the web server, which then transfers the data to the browser. Generally, the response is simply the statement that the sighting has been successfully added to the database and the record number. However, if an error occurs, the response is the error code and description. Also, when the sighting is added to the database, checks are made of the linked databases (described below). If the vessel is on the Lookout List, that fact is returned to the user. If the vessel has been previously boarded by the Coast Guard, the date the vessel was last boarded is also indicated. This gives the user instant feedback on the success of the entry as well as pertinent law enforcement information.

*Query Form:* The other main form is the Query form (Figure 7) which is used to request information from the database. Like the sighting entry form, the query form also contains hidden fields which specify various attributes such as database name and sort order for returned records. The visible fields on the form are used to specify the search criteria, such as all vessels of a certain type. If multiple fields are used the search is performed using a logical AND of all the criteria. Again, pull-down menus are used as much as possible to minimize typing—especially for fields in the database that are coded. In this case the pull-down menu contains plain language which is converted to the appropriate code behind the scenes.

The query is sent to the database by the user clicking on the SUBMIT button (labeled “Find Sightings”). This directs the browser to transfer the data from the selected fields to the web server which hands it off to the database through the CGI. A search of the database is done using the specified criteria and the records found are returned to the browser in the format specified by the query form. In order to minimize the amount of data transmitted, only a small amount of information is returned for each found record (Vessel Name, Type, Document Number, Position, Date and Time of Sighting, and whether the vessel is on the Lookout List). Part of the data returned for each record is a web link (through the vessel number) which the user can click on to retrieve the full record from the database. This allows the user to quickly see all of the vessels in the database meeting the search criteria and then download a full report only on the vessels desired.

*JMCIS Download form:* The final form was included to enable the large Coast Guard cutters to transfer the information from the database into their Command and Control ($C^2$) systems. The $C^2$ system used on these cutters is the same as used in the Navy; the Joint Maritime Command Information System (JMCIS). This system only accepts vessel reports in a certain format (OTH Gold). This form has a single button on it; all of the functionality is specified in hidden fields. When the user clicks on the button, a special search of the database is done, and all of the vessel sightings that have not been downloaded yet, are found and transferred to the browser in OTH Gold format. This information is then saved as a text file by the user and transferred to the JMCIS computer.

*Database*

The operation of this experiment is controlled by the database. FileMaker Pro works with several database files that are linked together (Figure 8). The OWL main database contains all of the information for this experiment. The sighting information is entered into this database by the WebFM CGI, and this is the database that is queried by the user. The linked databases are used to reduce the amount of data that the user needs to

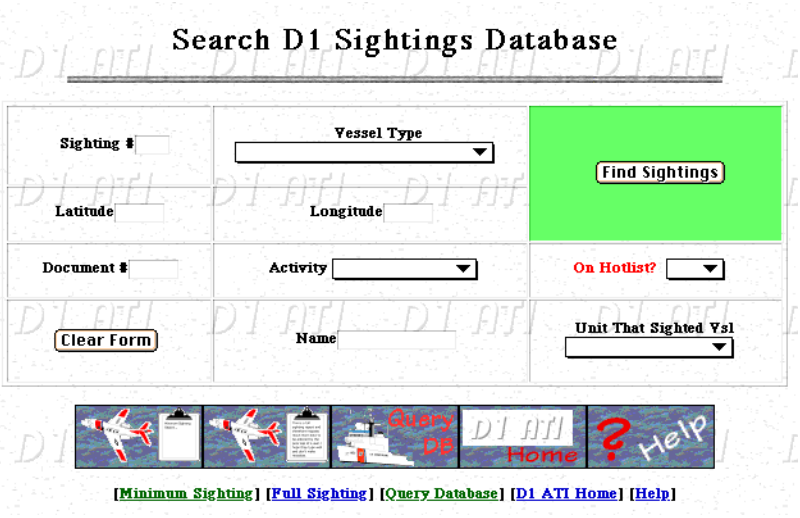


***Figure 7—Screen shot of the Query Database page.***

enter, since much of the information about a given vessel is static, and is already known. The user simply enters the dynamic data (position, course, speed, and activity) along with the vessel's document number. The document number is the unique identifier which is used to retrieve the static information from the linked databases. Currently, each of these linked databases resides along with the main database. Ideally, in the long-term, these database would be linked over the Internet or an Intranet, with each database being maintained by the appropriate agency.

*NMFS Database:* This is a database of fishing vessels obtained from the National Marine Fisheries Service (NMFS) which contains information on all documented fishing vessels (about 8000 entries). The database contains fields for document number, name, homeport, state, length, and the fisheries permits and gear codes issued to each vessel. When a vessel is sighted, all of this information for that vessel is transferred into the OWL database.

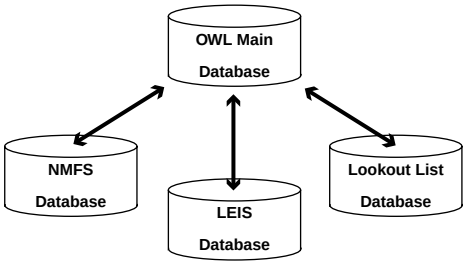


***Figure 8—Linked databases used in this experiment.***

*LEIS Database:* This is a database of information obtained from the USCG law enforcement database (LEIS) which contains information on all vessels sighted and boarded by the Coast Guard. The information duplicated locally is a subset of the corporate database. The database is used to supply the following fields into the main database: hull and superstructure color, vessel type, flag, and the date last boarded by the Coast Guard.

*Lookout List Database:* This is a database of all vessels of interest to the First Coast Guard District. Each time a vessel sighting is entered into the main database, it is cross-checked with this database to see if it is of interest (a "hot" vessel).

*Database Fields:* There are several types of fields in the database. In addition to those that are manually entered or looked-up in the linked databases, some fields are automatically entered and some are calculated by the database. The auto-entered fields are date and time of sighting entry and the sighting number. The calculation fields are used as program flags, internal calculations for special formatting, and most importantly, to create the HTML code returned to the user. Many of the web pages viewed by the user are actually created "on the fly" by the OWL database. The main ones (described above) are the Add Response, Query Result, Query Detail, and OTHG Format pages.

*Communications Links*

Providing the mobile units with a "real-time" communications link was one of the major goals of this experiment. For the medium endurance cutters (WMEC) the existing Inmarsat Standard-A terminals were used. Inmarsat-A is a commercial L-Band mobile satellite system that provides analog voice and data capability for about $6/min. The maritime antenna is 1.244m in size, and tracks in both azimuth and elevation [6]. External V.34 modems (Supra 33.6 external models) were used with the analog channel that Inmarsat-A provides, for the data connections. The patrol boats (WPB) do not have the topside real estate to mount an Inmarsat-A antenna, so we installed an AMSC terminal on board. This is also an L-Band mobile satellite system, but with a smaller antenna (.6m) and usage cost of approximately $1.50/min. It is a digital system that initially provided a data rate of 2400 bps, and is now transitioning to 4800 bps [7]. For the aircraft (HH-60 Jayhawk helicopters) an aeronautical version of the AMSC terminal, manufactured by CAL Corp. was used.

Each of these terminals was connected to a Toshiba P75 laptop running Windows 95™ via the RS-232 serial port. The end user would dial into one of the Remote Access Servers (RAS) located in our lab in Groton, CT. Two different RAS's: a SonicSystem Quickstream™ which has three ports, and a Shiva LanRover™ with eight ports were used. The LanRover was chosen because it supports all of the platforms and protocols we were using and it had some proprietary features that improve performance such as PowerBurst™ technology and STAC™ compression [8].

There were several challenges to be overcome due to the delays inherent with all satellite communications. The Inmarsat-A connection had a very long delay before the call went through and the Windows 95 dial-up networking application could not be configured to take this delay into account and would drop the connection before the modem connection could be established. With the help of Shiva technical support, we were allowed to use a beta version of Shiva's new PPP dial-up application which is more configurable and provides additional features such as detailed session statistics. This software allowed for a successful dial-up PPP connection through Inmarsat-A. The units using the AMSC terminals are required to dial into the QuickStream RAS because they were unable to successfully connect through the Shiva RAS using the AMSC terminals. This issue is still unresolved.

*Security*

Since this experiment involved actual law enforcement operations, security was a very important issue. The web server used is in general, very resistant to outside manipulation. The root level of the system is not accessible; whatever directory the application resides in appears to be the root level, and only files in the same directory or subdirectories are accessible. The system is also configured to reduce vulnerability by denying all FTP, TELNET, and SMTP connections which are respon-

sible for some of the most common server security breaches. Also, the system does not allow file uploads or directory indexing.

In order to restrict access to the sensitive law enforcement information, additional security layers were added to the system in three levels. The first is access protection. The secure web server is configured to only allow certain users to access the OWL web site. Any user can access the main page, but to go deeper into the site requires authorization. This is done using IP address filtering; the server is configured to only recognize authorized IP addresses. Any other user, with an IP address not on the authorized list will not be granted access to the web pages unless they have a valid user name and password. All others attempting to connect to the site will receive an Access Denied message. Dial-up access to the RAS is also protected by user name and password.

The second level of security is to protect the information during transmission. This is accomplished using standard software data encryption. Since the encryption is end-to-end, protection is provided both across the terrestrial network and the two satellite systems (AMSC & Inmarsat-A). The secure server is implemented using Netscape's Secure Socket Layer (SSL) protocol [9] to encrypt each session using RSA [10] encryption algorithms. The secure server supports DES (56 bit), 40 bit (international) and 128 bit (domestic) algorithms; the 128 bit version which provides the highest level of security is used for this experiment. Each session is encrypted separately so breaking one session does not allow other sessions to be decrypted. Netscape 3.0.1 domestic version was used as the web browser because it supports the high-grade encryption key (128 bit).

The third level of security is server authentication. Server authentication uses RSA public key cryptography in conjunction with ISO X.509 digital certificates [11] and lets the user (client) verify that the server is valid and not an imposter. Each connection to the secure server checks the secure server's site certificate with a trusted third party; for this server the security certificate was provided by Verisign™.

## Demonstration/Results

The system described above is currently undergoing testing on several ships and aircraft in the First Coast Guard District. The operational units participating in the experiment are the *USCGC Monomoy*, a 110 ft. patrol boat (WPB) operating out of Woods Hole MA, the *USCGC Escanaba*, a 270 ft. medium endurance cutter (WMEC) based in Boston MA, the *USCGC Vigorous*, a 210 ft. WMEC out of Cape May NJ, and several HH-60 Jayhawk helicopters flying from Air Station Cape Cod, MA. Each unit received a laptop running Windows 95 and Netscape Navigator for the client software. Since the testing is ongoing at the time this paper is being written, final results are not available. Some information on the communications links is provided in the table below; additional information will be available at the conference.

In general, the system has worked as desired, and been well received by the operators. All of the project goals are being met. The system is easily used by Coast Guard personnel from junior Seamen up to senior Commanders and Captains. The

| | **Inmarsat-A** | **AMSC** |
|---|---|---|
| **Typical time required to:** | | |
| Connect communications channel | 67 sec | 25 sec |
| Accomplish RAS log-on | 10 sec | 20 sec |
| Enter sighting and receive response | 7 | 14 sec |
| Perform query and receive response | 15 | 20 sec |
| **Typical connection bit rate** | 12,000 bps | 2,400 bps |
| **Link data compression?** | Hardware (V.34) | Software (STAC) |

work required by the user to enter sightings into the LEIS database has been reduced considerably—a savings of 10–15 minutes for **each** sighting! Data can be shared between the aircraft, cutters, and Operational Commanders ashore in a real-time fashion without requiring extensive user actions or voice relays. In addition, the web-based architecture allows the client-side software to be very simple (a COTS web browser) while all of the complexity is in the central server. This allowed the HTML code to be quickly and easily modified in response to input from the end-users and the changes automatically distributed to all users.

## References


[1] USCG R&D Center proposal for Pulse OPS Communication Project to First Coast Guard District, 12 December 1996.

[2] USCG web site, http://www.dot.gov/dotinfo/uscg/units.html.

[3] *Technology Assessment of U.S.C.G. Long-Range Communications Alternatives*, USCG R&D Center Advanced Communications Technology Report, March 1995.

[4] W. Stallings, *Data Computer Communications 5th ed.*., New Jersey: Prentice Hall, 1997, pp. 19–21.

[5] USCG R&D, Advanced Communications Technology web site, http://comms.rdc.uscg.mil/.

[6] Inmarsat web site, http://www.inmarsat.org/inmarsat/.

[7] AMSC web site, http://www.skycell.com/

[8] Shiva web site, http://www.shiva.com/

[9] Netscape's web site, http://home.netscape.com/newsref/std/SSL.html.

[10] RSA Data Security, Inc. web site, http://www.rsa.com/.

[11] Verisign's Web Site, http://www.verisign.com/pk_intro.html.