REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
8-03-2011	Final Report	6/10/05-9/30/09

4. TITLE AND SUBTITLE
Advanced Development Associated with the Glider Technology Transition Initiative

5a. CONTRACT NUMBER
N00024-02-D-6602, order 61

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Dr. Craig Lee, and Neil M. Bogue

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Applied Physics Laboratory
University of Washington
1014 NE 40th Street
Seattle, WA 98105

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)
ONR

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Glider TTI had two primary impacts: it accelerated the transition of underwater gliders to operational status at the U.S. Naval Oceanographic Office, and it supported the Littoral Battlespace Sensing Fusion and Integration (LBSF&I) Program of Record in its acquisition program Littoral Battlespace Sensing – Gliders (LBS-G).

In addition to the improvements to gliders achieved under the tasks outlined in the report, the Glider TTI directly supported the LBS-G acquisition program. The Glider TTI supported the preparation and review of glider specification, requirement, and test documents in the early stages of the acquisition process. The Glider TTI contributed to the commercialization of the first generation glider technology: each glider type had at least one commercial provider capable of bidding on the LBS-G solicitation.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Craig M. Lee
U	U	U	UU	17	19b. TELEPHONE NUMBER *(Include area code)* (206) 685-7656

Advanced Development Associated with the Glider Technology Transition Initiative

Final Report
N00024-02-D-6602, Delivery Order 61

Submitted to

Mr. Randy Case, Mr. Kim Koehler, and Dr. Ed Mozley
Space and Naval Warfare Systems Command
PEO C4I, PMW-120

As part of the

Operational Gliders for Battlespace Reconnaissance and USW Surveillance Technology Transition Initiative

Also supported by

Office of the Secretary of Defense
Acquisition, Technology, and Logistics
Office of Technology Transition

Office of Naval Research, Code 32

In transition to

U.S. Naval Oceanographic Office

SPAWAR PEO C4I PMW 120
Littoral Battlespace Sensing Fusion and Integration Program

By

Dr. Craig Lee
Glider TTI Principal Investigator
Applied Physics Laboratory
University of Washington

Neil M. Bogue
Glider TTI Program Manager
Applied Physics Laboratory
University of Washington

6JUL2010

1 Introduction

The first generation of underwater gliders was developed with funding from the Office of Naval Research, starting in the mid-1990's. The developers were academic institutions or small businesses closely associated with such institutions. By 2004, ONR was supporting the use of underwater gliders in Navy fleet exercises: RIMPAC04, TASWEX04, and SHAREM151, for example. Experienced scientists and engineers at academic institutions operated the gliders. Vertical profiles of tactically relevant properties of seawater (sound speed profiles, optical backscatter, etc.) were relayed in near real time to the U.S. Navy Oceanographic Office (NAVOCEANO) for assimilation into their tactical oceanography products.

The Operational Gliders for Battlespace Reconnaissance and USW Surveillance Technology Transition Initiative (Glider TTI) was created and governed by a Technology Transition Agreement (TTA) signed by the Oceanographer of the Navy (N7C), Commander Naval Meteorology and Oceanography Command (CNMOC), the Office of Naval Research (ONR, Code 32), and SPAWAR PEO C4I (PMW-180, now PMW-120). The TTA was signed in 2006.

The goal of the Technology Transition Agreement was "…to ensure a successful transition of technology from the Office of Naval Research (ONR Code 32) to the PMW 180 Littoral Battlespace Sensor Fusion and Integration (LBSF&I) program." The program plan was to make improvements to the first generation of underwater gliders to enhance their usability by NAVOCEANO (the ultimate customer of the LBSF&I program) and to provide common operating software so that NAVOCEANO could safely and efficiently operate all three types of underwater glider. The agreement provided technical goals and deliverables, funding profiles, and a management structure.

The Glider TTI program began with a kick-off meeting in June, 2005. It successfully concluded on 30SEP2010. This report will describe the participants, the accomplishments, and the transition results and impacts of the Glider TTI.

More detailed information is contained in various documentation submitted as deliverables to NAVOCEANO, or in the records of program reviews and subcontractor final reports as submitted.

2 Funding

Funding for the Glider TTI program came from three sources: the Office of Naval Research Code 32, the Office of the Secretary of Defense Office of Technology Transition, and SPAWAR PMW-120. The funding split and sequence was as directed in the TTA.

The Glider TTI funding sources and timeline are shown in Table 1 below.

	FY 2005	FY2006	FY2007	FY2008
ONR Code 32	604	400		
SPAWAR PEO C4I PMW 120	318	450	400	
OSD OTT TTI		1,900	1,900	800

Table 1. Glider TTI funding in $1000s.

3 Performers

The Applied Physics Laboratory of the University of Washington (APL-UW) was the prime contractor and program manager for the Glider TTI. APL-UW subcontracted with the other glider developers and operators included in the program. Total subcontract funds equaled $2,429,052.

A list of the performers, the Principal Investigators, and their technologies, is shown in Table 2 below.

Institution	Principal Investigator	Technology	Role	Funding $1000s
Applied Physics Laboratory University of Washington	Dr. Craig Lee	*Seaglider*	Program manager, Developer	3,171
Webb Research Corporation (Teledyne Webb Research)	Mr. Clayton Jones	*Slocum*	Developer	993
Scripps Institution of Oceanography	Dr. Russ Davis	*Spray*	Developer	566
Rutgers University	Dr. Scott Glenn	*Slocum*	Operator	360

OASIS, Inc.	Mr. Phil Abbot	*Slocum*	Operator	369
Woods Hole Oceanographic Institution	Dr. Dave Fratantoni	*Slocum*	Operator	141

Table 2. Glider TTI performers.

4 Program Plan

The Glider TTI program plan was built around a task structure. Task lists were built on the experiences of ONR, NAVOCEANO, and the glider developers and operators during the Navy fleet exercises described in the Introduction. Nine tasks were specified at the program kick-off. These are listed below.

1. Obtain NAVSEA/NOSSA battery approvals for glider operations from T-AGS ships, including development of rechargeable batteries and systems.
2. Harden gliders against rough handling. Develop launch and recovery systems.
3. Develop common glider user interface and control program. Develop common data formats.
4. Develop algorithms and display tools to aid in glider deployment and routing (visualization and adaptive sampling).
5. Deliver first prototypes.
6. NAVSEA (PMS-399) approvals for gliders as carry-on equipment on Navy platforms.
7. Develop glider CONOPS and participate in fleet exercises.
8. Deliver final prototypes.
9. Deliver documentation and configuration management packages.

The task execution matrix is shown in Table 3 below.

Task	1	2	3	4	5	6	7	8	9
Applied Physics Laboratory-University of Washington (APL-UW)	X	X	X		X		X	X	X
SIO-Instrument Development Group (SIO-IDG)	X	X	X		X			X	X
Teledyne Webb Research (TWR)	X	X	X		X			X	X
Woods Hole Oceanographic Institution (WHOI)		X	X	X					
Rutgers University (RU)		X	X	X			X		
Ocean Acoustical Services and Instrumentation Systems (OASIS)			X	X			X		

Table 3. Glider TTI task execution matrix, keyed to the task list shown above.

In addition to support provided for the main Glider TTI task list, PMW-120 added several additional tasks, primarily in support of preparation of the LBSF&I solicitation for gliders, the Glider TTI program itself, and enhancements to the NAVOCEANO *Seaglider* fleet. These additional tasks are listed below.

- Write a report comparing the capabilities of the original three battery-powered gliders: *Slocum*, *Spray*, and *Seaglider.* This report was submitted to PMW-120 (then PMW-180) in August 2005, and was subsequently published at Applied Physics Laboratory Technical Memorandum TM-4-05, dated September 2005.

- Prepare a Glider TTI Program Plan. This plan was prepared and first briefed on 15DEC2006. It was subsequently briefed at all Glider TTI annual program reviews.

- Deliver *Seaglider* operating software with Iridium RUDICS capability to NAVOCEANO with the second TTI prototype *Seaglider.* This was done. NAVOCEANO has been successfully operating their *Seaglider* fleet using RUDICS for several years. A brief description of the RUDICS implementation is given in the Appendix.

- Investigate the computational impact of AES encryption on the Seaglider. See the Appendix for the results of this investigation.

- Examine the options for upgrades to the Seaglider CPU. This task grew out of operational experience at NAVOCEANO and APL-UW, and was partially motivated by the investigation of the computational impact of AES. The Appendix also contains the results of this investigation.

5 Accomplishments

Summaries of the Glider TTI accomplishments are given below, described by task.

Task 1: Battery Approvals

TWR developed rechargeable Li-ion battery packs for *Slocum.* The second prototype was delivered with Li-ion packs at the end of April 2009. These Li-ion packs were evaluated and tested by the Navy Lithium Battery Safety Program, Naval Surface Warfare Center (NSWC), Carderock Division.

APL-UW designed extended-range Li primary battery packs for *Seaglider,* with about 50% more stored energy than the original standard Li primary battery packs. This change was enabled by a new design of the mass shifter assembly to accommodate the heavier mass of the extended-range packs. The first TTI prototype *Seaglider* was delivered to NAVOCEANO with these extended-range packs.

APL-UW also designed Li-ion rechargeable battery packs for *Seaglider*. These were first flown in September 2008, and the second TTI prototype Seaglider was delivered to NAVOCEANO with rechargeable batteries in April 2009. The NSWC Carderock Safety Assessment of these Li-ion batteries was published in September 2009, as NSWCCD-61-TM-2009/37.

SIO-IDG implemented changes to the endcap of *Spray* to incorporate a pressure-relief valve at the request of NSWC Carderock as part of the NSWC safety review of the *Spray* Lithium primary batteries.

SIO-IDG did not propose development of Li-ion (secondary) batteries.

Task 2: Hardening and Launch and Recovery Systems

TWR worked with Rutgers and WHOI for field test and evaluation. A ruggedized fin (DigiFin) was developed, tested and incorporated into production *Slocum*s in January 2008. A ruggedized CTD mount was incorporated into production units in

March 2008. TWR also developed a pop-off nose and line payout system to aid in *Slocum* recovery. It was successfully tested in October 2008.

APL-UW designed a stronger *Seaglider* mass-shifter mechanism, to improve reliability and handle larger-weight extended-range Lithium primary batteries. A pressure relief valve was added to the aft endcap. The ITC-3013 transducer mount in the nose of the pressure hull was adapted to be held on with spring-tension, such that under sufficient internal pressure, it will separate from its mounting plate and provide a large-diameter vent.

Externally, a stronger, shorter *Seaglider* antenna mast was developed, along with externally attachable wings, a rugged, cost-effective rudder, CTD guard, and a panelized aft fairing.

APL-UW designed a hoop-and-pole recovery system to use from T-AGS class ships. Several of these systems were delivered to NAVOCEANO for test and evaluation. This proved successful, and an additional seven units were provided to NAVOCEANO to equip all the T-AGS ships.

SIO-IDG redesigned the *Spray* wing structure and manufacturing technique for strength and cost-effectiveness. The *Spray* tail was also redesigned for strength, with an aluminum recovery loop on the lower half, and an Argos beacon antenna in the upper half. The attachment of the flooded section to the pressure hull was also redesigned and entered production in mid-2008. The CTD mount was ruggedized and incorporated into production units in late-2008.

Internal to *Spray*, SIO-IDG developed and extensively tested an active air-removal system for the hydraulic buoyancy system. New actuators and gear-motors were designed and implemented for increased reliability of pitch and roll mechanisms.

SIO-IDG also designed and built the *Spray* Recovery Vehicle (SRV), a radio-controlled tethered catamaran directed from the deck of the recovery vessel to scoop a *Spray* at the surface and hoist it aboard the vessel. The SRV was successfully tested in open-ocean conditions. Two SRVs were delivered to NAVOCEANO in October 2008.

Task 3: Common Command and Control User Interface

APL-UW was the lead developer of the common command and control interface, named GLMPC, for Glider Monitoring, Piloting, and Communications.

GLMPC was first deployed at NAVOCEANO in 2007, and was immediately put into operational service to support NAVOCEANO's fleet of *Seaglider*s (purchased independently of the Glider TTI). This early operational use resulted in a close relationship between the glider operations group (pilots) at NAVOCEANO and the

GLMPC developers at APL-UW. Consequently, GLMPC was continuously upgraded throughout the life of the Glider TTI.

At the end of the Glider TTI, GLMPC was a tested piece of operational software, able to display data from *Seaglider*, *Spray*, and *Slocum.* GLMPC could fully control *Seaglider*, and perform basic command and control on *Slocum* and *Spray*.

Task 3A: Develop Common Data Format

At the beginning of the Glider TTI, the program agreed with NAVOCEANO that all glider data would be converted from their native format to KKYY format for CTD profiles, and NetCDF (*.nc) for everything else. During the Glider TTI, NAVOCEANO moved to WMO BUFR format, so a conversion capability was added into GLMPC.

Task 3B: Sensor Data Format and Requirements Study

Mr. Marc Stewart of APL-UW and Ms. Elizabeth Creed of OASIS completed this study in January, 2008. It was published at APL-UW Technical Memorandum TM4-07, "Glider Sensor Requirements and Data Format Study for the Glider Technology Transition Initiative".

Task 4: Visualization and Adaptive Sampling

Dr. Pat Cross of OASIS managed task 4. The work was divided into two main parts. Rutgers University updated their REMAP glider data visualization tool, and ported it to work on a system they purchased and supplied to NAVOCEANO. OASIS upgraded their EMMP algorithm for adaptive sampling, and integrated EMMP with NRL-supplied cost functions. The Task 4 team supported the Navy's Valiant Shield 2007 and RIMPAC08 exercises.

Task 5: First Prototypes

TWR delivered their first TTI *Slocum* prototype in April, 2008, and included AUV-B optics packages at NAVOCEANO's request.

APL-UW performed a long series of development tests on SG128. These tests culminated in a mission of 1080 dives in October, 2007. These tests validated the reliability of the new mass shifter, the extended range batteries, some operating code enhancements for reliability, and were the first test of the externally attachable (and longer) wings. Ms. Angela Wood and Mr. Keith Van Thiel documented the results of this test sequence as APL-UW Technical Memorandum TM1-08, "Field Tests of the Glider Technology Transition Initiative Prototype Seaglider". SG128 was refurbished and tested prior to delivery to NAVOCEANO in April, 2008.

SIO-IDG delivered their first TTI prototype *Spray* to NAVOCEANO in September, 2008, which included a portable *Spray* workstation and required parts and tooling. SIO-

IDG also provided *Spray* operator and pilot training at NAVOCEANO in September, 2008.

Task 6: NAVSEA Approvals for Carry-on Use on Navy Platforms Plan

At the direction of the ONR Glider TTI program manager, this task was deferred.

Task 7: CONOPS and Participation in Navy Exercises

All performers supported NAVOCEANO on request.

Special attention was paid to glider participation in Navy exercises during the Glider TTI: RIMPAC06, Valiant Shield07, and RIMPAC08. Various Glider TTI participants were in the NAVOCEANO Glider Operations Center (GOC) during these exercises to assist with CONOPS, piloting, data interpretation and visualization, and to guide the deployment and operational evolution during the exercises.

OASIS, with support from APL-UW, wrote a series of standard glider operating procedures for use by NAVOCEANO.

Task 8: Second Prototypes

SIO-IDG delivered their second Glider TTI prototype *Spray* in September, 2008, concurrent with the delivery of their first prototype.

TWR delivered their second Glider TTI prototype *Slocum* glider, which included rechargeable Li-ion batteries, in April, 2009.

APL-UW delivered SG159, their second Glider TTI, in April, 2009. SG159 was delivered with Li-ion rechargeable batteries, following successful sea trials in February and March, 2009.

Task 9: Documentation and Configuration Management

TWR trained NAVOCEANO glider operators and pilots at the TWR facility prior to delivery of their first TTI prototype *Slocum*. A complete set of documentation was provided to NAVOCEANO with the first TTI prototype.

An SIO-IDG engineer presented a one-week training class on *Spray* preparation, maintenance, and operation at NAVOCEANO in September, 2008. On-the-water deployment and recovery training was provided at SPAWAR Systems Center Pacific, San Diego. A *Spray* Operator's Manual was created and delivered to NAVOCEANO.

APL-UW provided an updated set of all *Seaglider* manuals with the delivery of the first TTI prototype *Seaglider*, SG128.

6 Transition Results and Impact

The Glider TTI had two primary impacts: it accelerated the transition of underwater gliders to operational status at the U.S. Naval Oceanographic Office, and it supported the Littoral Battlespace Sensing Fusion and Integration (LBSF&I) Program of Record in its acquisition program Littoral Battlespace Sensing – Gliders (LBS-G).

In addition to the improvements to gliders achieved under the tasks outlined above, the Glider TTI directly supported the LBS-G acquisition program. The Glider TTI supported the preparation and review of glider specification, requirement, and test documents in the early stages of the acquisition process. The Glider TTI contributed to the commercialization of the first generation glider technology: each glider type had at least one commercial provider capable of bidding on the LBS-G solicitation.

Mr. Richard Myrick, Director, Ocean Measurements Department, NP3, NAVOCEANO, stated,

"[With respect to] TTI, having an operational glider capability at NAVOCEANO is a direct result of the TTI program. There is no question in my mind that TTI accelerated the transition of this operational capability to NAVOCEANO by 3-5 years. Also, the TTI provided extremely valuable insight to the development of PMW-120's Littoral Battlespace, Sensing, Fusion and Integration (LBSF&I) POR glider specification development."

The LBS-G solicitation was awarded in March, 2009, to a partnership of Brown Engineering and Teledyne Webb Research (TWR). This award represented the culmination of a the glider development effort begun by the Office of Naval Research with basic research funds in the mid-1990s, and supported through the Glider TTI to complete the transition to a Navy acquisition program of record.

7 Acknowledgments

The Glider TTI would not have been successful without the efforts of a large group. The author acknowledges the support and leadership of Dr. Terri Palusziewicz at ONR, whose vision, energy, and skill created the Glider TTI and ensured its success. CAPT Douglas Marble, USN, PhD, Mr. Robert Houtman, and Mr. Richard Martinez at ONR Code 32 were instrumental in the success of the program. The Principal Investigators and their technical staffs designed and implemented the improvements to the gliders that were the heart of the program. The glider team at

NAVOCEANO was exceptional: Mr. Richard Myrick, Mr. Dan Berkshire, Mr. Bruce Bricker, Ms. Danielle Bryant, Mr. Steve Crossland, and Mr. Marc Torrez. All provided a great deal of help, feedback, and willingness to try new (and sometimes crazy) things. Mr. Dan Altobelli of the OSD Office of Technology Transition was supportive and helpful during the review and reporting processes. Mr. Kim Koehler and Dr. Ed Mozley of SPAWAR PMW-120 were patient and understanding in managing the interfaces between the Glider TTI and the LBSF&I acquisition. And finally, at APL-UW, Dr. Craig Lee was thoughtful and supportive as the Principal Investigator; Ms. Nancy Sherman administered the Glider TTI program with her rare mix of skill and humor; and Ms. Angela Wood did the hundreds (or thousands) of things that have to be done for a program like this to succeed.

8 Appendices

The following Appendices contain the results of three tasks assigned by SPAWAR PMW-120 in support of NAVOCEANO's *Seaglider* operations.

Appendix 1: Implementing RUDICS on *Seaglider™*
Appendix 2: Upgrading *Seaglider™* onboard computing
Appendix 3: Implementing AES on *Seaglider™*

Appendix 1: Implementing RUDICS on *Seaglider™*

Jason Gobat and Geoff Shilling
Applied Physics Laboratory
University of Washington

Introduction

As part of the Glider TTI program, we implemented support for Iridium RUDICS communication on *Seaglider™.* RUDICS (Router-based Unrestricted Digital Internetworking Connectivity) is a method of Iridium connectivity whereby the traffic from the ground station to the host (*Seaglider™* basestation) is routed on the Internet instead of the public switched telephone network (PSTN). This eliminates the need for a modem pool attached to the *Seaglider™* basestation. Traditionally, the *Seaglider™* dials a PSTN number to connect via a modem to a *Seaglider™* basestation. With RUDICS, *Seaglider™* dials a specially provisioned number that routes traffic to a specified port at the IP address of the basestation.

Results

Initial support for RUDICS on *Seaglider™* consisted of setup and initialization on *Seaglider™* and provisioning of a RUDICS daemon program on the basestation. Extensive field-testing revealed that the system worked at a level of reliability sufficient to recommend operational use. *Seaglider™* operating code with full RUDICS capability was delivered to NAVOCEANO with the Glider TTI second *Seaglider™* prototype. However, the initial implementation, communications performance with RUDICS did not reach the level routinely achieved with PSTN communications. That is, while the system worked well enough, it did not work as well as the PSTN system. For that reason, we continued to use PSTN communications for our own *Seaglider™* missions. More recently, we have found and fixed several timing and synchronization problems in the communications protocol and are now achieving performance with RUDICS that is comparable or better than PSTN performance.

Appendix 2: Upgrading *Seaglider™* onboard computing

Jason Gobat, Craig Lee, and Geoff Shilling
Applied Physics Laboratory
University of Washington

Introduction

In order to provide an extensible, robust architecture that will allow *Seaglider™* to be modified to meet a large variety of mission requirements, reduce *Seaglider™* power consumption to extend mission duration, and address concerns about availability and support for the exiting TT8-based solution, we investigated replacing the *Seaglider™* main processor with a modern design that offers greatly expanded capabilities. The *Seaglider™* onboard computer consists of an Onset Tattletale Model 8 (TT8) single-board computer (SBC) mated to a Persistor CF-8 compact flash expansion board. The TT8 is based on the Freescale (formerly Motorola) 68332 microprocessor. The TT8 design is more than 10 years old; the 68332 has been in production for more than 20 years. Concerns about availability have become particularly acute since Onset issued an end-of-life notice for the TT8. Persistor continues to supply the CF-8 but has stopped providing updates to the PicoDOS file system software, focusing instead on updates to their own 68332-based computer, the CF-2. Citing lack of interest from the marketplace, they have no plans even to bring the latest version out of beta status, where it has been for at least three years.

Limitations

The TT8/CF8/PicoDOS stack imposes several significant limitations on the *Seaglider™* 's software architecture and capabilities. The CF-8 file system is an implementation of FAT16 without directory support. Performance significantly slows as large numbers of files are added to the disk over the course of missions. The file system has no high-reliability or onboard maintenance or repair features. Neither the TT8 nor the CF-8 software libraries are open. We frequently push the limits of this hardware and often encounter behaviors that are extremely difficult to debug without access to the underlying libraries. Further complicating debugging, neither of the supported development environments for the TT8 includes a debugger.

Results

We investigated several candidate hardware architectures including Analog Devices Blackfin, Freescale Coldfire, Intel Xscale, ARM-9 and ARM Cortex-M3. We considered both SBCs built around and these devices and integrating CPUs directly into the custom built *Seaglider™* electronics. We also considered software architectures

including Linux, a variety of real-time operating systems, and running “bare-metal” without an operating system kernel as we do on the TT8.

Of the considered options, we concluded that an ARM-based solution offered the best combination of tool chain support, onboard peripherals, and flexible low-power operation. In order to have total control over low-power operation, we have chosen a bare-metal, direct integration of an ARM Cortex-M3 processor for the *Seaglider™* control computer. An outgrowth of this study, however, is that SBCs with ARM-9 based processors from NXP, originally evaluated as candidates in this study, are now the basis for several embedded instrumentation and control projects within the laboratory, including two glider-based acoustic systems.

Appendix 3: Implementing AES on *Seaglider™*

Geoff Shilling
Applied Physics Laboratory
University of Washington

26JUN2007

Introduction

This report describes a study of the computational time implications of encrypting typical *Seaglider™* data payloads using an implementation of the Advanced Encryption Standard (AES).

This study does not address a large number of issues that would be part of actually implementing and deploying an end-to-end encryption strategy for a *Seaglider™*. Some of these issues are listed below.

• The particular AES implementation used in this study was selected for availability only. Specifically, it has not been independently reviewed for completeness or conformance with the AES standard.

• Only the time to encrypt the core scientific and vehicle engineering data payload was considered (that is, the payload that represents the largest on-disk footprint). No consideration was given to command input to the glider, nor to the output communications traffic the glider routinely generates and sends during data transfer.

• This study does not consider key management, vehicle physical security integrity (tamper-proofing), operational implications of encryption, shore-side processing security, or the design of an overall security and threat model for *Seaglider™* data security.

• This study does not consider implications of encryption on the vehicle's operation beyond the limited scope of computational time to encrypt. These implications include, but are not limited to, power consumption, storage consumption and transmission impact.

Technical Background

The *Seaglider™* Onset TT8 single board computer employs a M68332 processor, 1 megabyte of RAM, and a 256Mb compact flash card for data storage. There is no operating system in the modern sense of the term; there is derivative of DOS (called PicoDOS) that delivers rudimentary system services. The *Seaglider™* operational

code is a monolithic application, approximately 440K in size, written in C, and highly tuned for low-power operations.

A typical *Seaglider™* mission consists of a loop of surface operations, followed by dives (of up to 10 hours in length). During the dive, data and vehicle engineering data is collected from the on-board instruments and systems. The data is stored in three main files, two of which are typically uploaded on every surface operation. Surface operations are deliberately optimized for time because the vehicle cannot maneuver while on the surface and the air-sea interface is generally less safe for the vehicle than the underwater realm.

Surface operations are highly variable in length and largely dominated by the quality of Iridium phone communications and data-engineering file sizes to be uploaded. For full 1000-meter dives with a typical instrument sampling schedule and good communications, 10 minutes at the surface is a typical value. For the same data-engineering files but poor Iridium communications, 30 minutes at the surface may not be unlikely.

Approach

To study the time implications of adding encryption to the *Seaglider™* , an implementation of the AES encryption algorithm was ported to a TT8 and a variety of typical *Seaglider™* data and engineering files were encrypted. The time to perform the encryption was recorded.

The implementation selected was from the website:

http://www.progressive-coding.com/tutorial.php?id=0 and
http://www.progressive-coding.com/tutorial.php?id=3

(See Note 1.)

This particular implementation is not especially optimized for time, but fairly optimized for space. As mentioned above, it has not been vetted for compliance with the AES standard by an independent source. It was confirmed that it is compatible with an independent AES implementation (from the Python 2.4 distribution) to the extent that data that was encrypted on the TT8 could be decrypted.

Optimizations

I performed two optimizations for time that were not present in the original code, but that were applicable for the TT8.

Results

Here are some typical file sizes and the times and rates of encryption:

Battery (445 bytes) - 0.94 secs (484.04 bytes / second)
sg0090dz.r (19200 bytes) - 34.21 secs (561.21 bytes / second)
sg0311du.r (46592 bytes) - 81.77 secs (569.79 bytes / second)
sg0090du.r (102153 bytes) - 179.33 secs (569.63 bytes / second)

To understand the time implications, consider a typical single dive data and engineering set from a typical *Seaglider™* mission (SG122 in the Western Pacific). (See Note 2.)

sg0040kz.r - 21940 bytes
sg0040dz.r - 18058 bytes
sg0040lz.r - 4078 bytes
Total: 44076 bytes

At a rate of 570 bytes/sec, we can encode the three files in 77.3 seconds.

Conclusion

This study suggests that encrypting the largest data and engineering files from a typical *Seaglider™* dive would add 1.25 minutes to each surface operation, or about 6% increase in time. This increase is well within the typical variability of *Seaglider™* surfacing times due to Iridium performance. It does not represent any operational limitation.

As stated above, this study does not include the time to encrypt the input command and control files, nor does it include the time to include the routine communication output traffic that the *Seaglider™* sends to its basestation during its communication session.

Notes

1. The copyright and license on this code is unknown at this time.
2. These files have been compressed via *gzip* prior to encryption.