ARMY RESEARCH LABORATORY

Information Assurance Tasks Supporting the Processing of Electronic Records Archives

**by Binh Nguyen, Glenn Racine,
Brian Luu, and John Cole**

ARL-TR-4064 **March 2007**

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

Army Research Laboratory
Adelphi, MD 20783-1197

ARL-TR-4064 **March 2007**

Information Assurance Tasks Supporting the Processing of Electronic Records Archives

Binh Nguyen, Glenn Racine,
Brian Luu, and John Cole
Computational and Information Sciences Directorate, ARL

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED (From - To)
March 2007	Final	Fiscal Year 2006

4. TITLE AND SUBTITLE
Information Assurance Tasks Supporting the Processing of Electronic Records Archives

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Binh Nguyen, Glenn Racine, Brian Luu, and John Cole

5d. PROJECT NUMBER
6FG0RC

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Research Laboratory
ATTN: AMSRD-ARL-CI-CN
2800 Powder Mill Road
Adelphi, MD 20783-1197

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-TR-4064

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Archives & Records Administration
Elect Records Archives Prog Mgmt Ofc
8601 Adelphi Rd
College Park MD 20740-6001

10. SPONSOR/MONITOR'S ACRONYM(S)

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

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This document reports the results of three (3) information assurance tasks that support the distributed processing of electronic records archives during FY06: (1) transfer network intrusion detection technologies to NARA, (2) analyze the performance costs of security products deployed in a web server, and (3) evaluate a secure virtual private network (VPN) product.

15. SUBJECT TERMS
Information assurance, intrusion detection system, electronic records archives

16. Security Classification of:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	SAR	22	Binh Nguyen
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER (*Include area code*) (301) 394-1781

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

Contents

List of Figures

List of Tables

1 Introduction

1.1 Background

To support the distributed processing of sensitive electronic records archives (ERA) of the U.S. National Archives and Records Administration (NARA), the U.S. Army Research Laboratory (ARL) was engaged to perform the following information-assurance (IA) tasks:

- Transfer network intrusion detection technologies to NARA,
- Analyze the performance costs of security products deployed in a web server, and
- Evaluate a secure virtual private network (VPN) product.

The objectives of the tasks were to find ways to provide for protection of sensitive ERA when they are placed in systems that are connected to public networks. The first task concerns the transfer of time-proven ARL-developed technologies and methods capable of detecting unauthorized access to networked ERA systems. The second task determines the performance costs incurred from the use of security products to protect ERA in transit between two authenticated entities. The last task assesses the functional behavior of a VPN product that is potentially capable of providing secure communications among networked ERA systems.

1.2 Scope

This document (a) summarizes the results of the findings of each task that ARL conducted during the reporting period, (b) reports encountered technical barriers and strategies for overcoming them, and (c) recommends research activities to be conducted in the future.

The intended audience of this report includes ARL and NARA administrators and managers, ERA and IA researchers, and information technology personnel.

The next section reports the status of each task, including its accomplishments and recommendations for future activities, and describes the method by which each task was accomplished. Section 3 reports encountered technical barriers and resolutions. Section 4 concludes the report and recommends research activities to be accomplished during the next phase.

2. Tasks

The IA tasks to be performed during the reporting period include three subtasks: (1) technology transfer of ARL-developed intrusion detection systems and methods, (2) measurement and analysis of the performance costs of the deployed security protocols and algorithms, and

(3) empirical evaluation of a VPN product. The results and the planned activities of each task are separately described and discussed in the following paragraphs.

2.1 Technology Transfer of Intrusion Detection Systems and Methods

This task was conducted to transfer intrusion detection systems (IDS) technologies and methods from ARL to NARA. ARL's Center for Intrusion Monitoring and Protection (CIMP) installed a sensor at NARA to collect data; however, it was not turned on because of potential issues of data monitoring and transfer between civilian and military agencies. Consequently, CIMP has adjusted its approach and concluded that a stand-alone version of the Interrogator Architecture dubbed "Gator Junior" would need to be developed with a reduced hardware set that is capable of providing the same level of intrusion detection and effective, timely defensive responsiveness without ARL monitoring and storing any collected data.

The "Gator Junior" with a stand-alone capability does not require remote access and keeps data local. ARL will gain the capability of serving other Government customers with similar requirements and will help resolve an information sharing problem among Government agencies. Designing a system that is self-contained but has the full capabilities of a distributed IDS based on the Interrogator Architecture will be a technical accomplishment. The challenge is to provide collection, analysis, and database capabilities with less hardware while providing timely information for defensive actions, and it is unknown if the required capabilities can be achieved with a reduced hardware set.

ARL's CIMP has just started to develop "Gator Junior" by performing three vital subtasks: gathering requirements, training NARA analysts, and modifying the Interrogator Architecture to fit the NARA environment. A significant aspect of this project is discovery of NARA requirements. A NARA computer scientist will receive training at NARA and ARL in analytical techniques. A reduced Interrogator Architecture for NARA can be accomplished in six Dell computers running the Linux® operating systems. Three of these systems will function as sensors and be installed at three geographically dispersed NARA locations on various places in the country. Three other systems will serve as the "Gator Junior" installation serving functions as a combined web server-database, data store, and analysis engine. Further details of the "Gator Junior" development are included in the proposal that has been submitted to NARA for consideration and approval.

2.2 Performance Costs Measurement and Analysis

This task was conducted to support the building of a distributed processing environment in which sensitive electronic records archives (ERA) are processed and a secure web portal operates. The objective of the task was to measure and analyze the performance costs associated with the use of the transport-layer-security protocol version 1.0 (TLSv1) (*1*) to secure and protect ERA in transit between two networked computers running in a public network.

Determining these costs was a research subject of previous studies focusing on improving the TLS protocol (*2*-*3*) or on the impact of the security protocol on a typical web server (*4*). This task focused on measuring and analyzing the performance costs of using the protocol from the perspective of a user interacting with an atypical web server emulating the future secure ERA web portal. The main differences between how the target portal differs from a typical secure web server are summarized in table 1.

Table 1. A comparison between a typical web server and a hypothetical web portal of electronic records archives.

	Secure Web Server	**Secure ERA Web Portal**
Protocol	TLSv1 and predecessors	TLSv1
Strength of cipher suites	Low – High	High
Government-approved cryptographic protocols, algorithms, and modules	Optional	Mandate
Average page size	18.7 kilobytes (*5*)	Megabytes, gigabytes, or as large as the system can handle
Authentication	Only the server is often authenticated	Mutual authentication – the server and the client authenticate each other
Number of users	Various	Hundreds of users at most

All the experiments were conducted in a newly established test bed at ARL. The test bed is a gigabit network of five homogeneous Dell Latitude D810 notebook computers. Each runs an identical version of the Red Hat Linux Enterprise 4.0 operating system and has two network interface cards (NICs), thus enabling each to function as a physical subnetwork (subnet). Having a local test bed minimizes traveling and provides a convenient high-performance network environment facilitating the conduct of empirical research, now and in the future. Figure 1 shows a picture of the test bed environment in which the experiments were conducted.

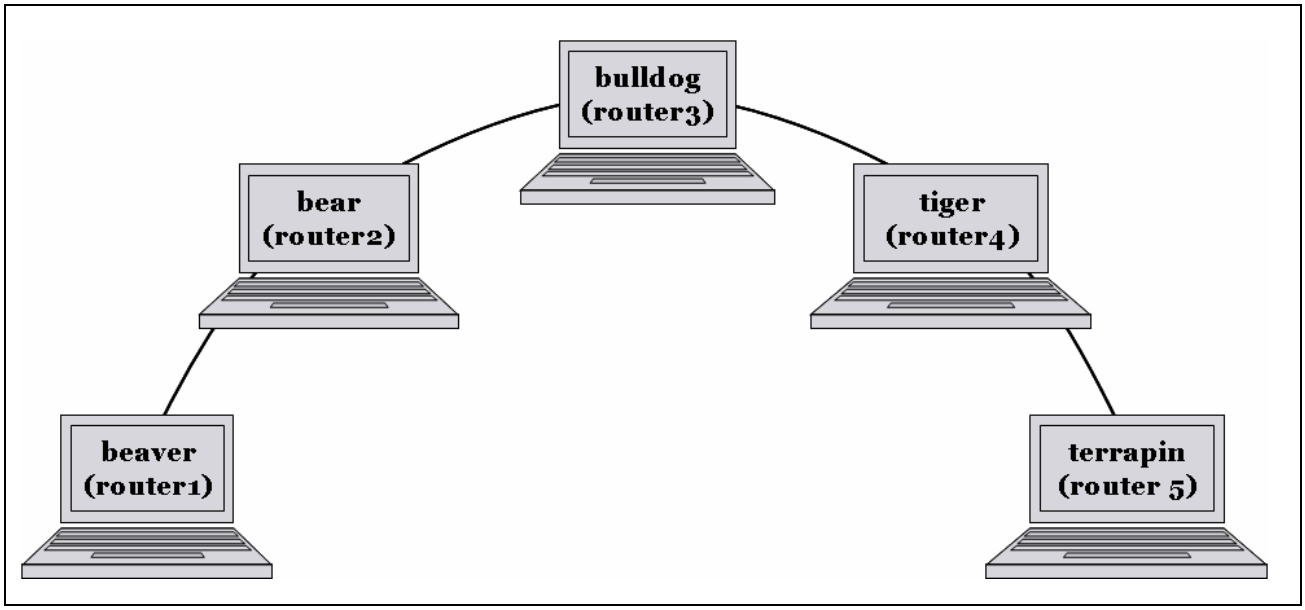

Figure 1. The configuration of the test bed for experimenting with the TLS protocol.

Besides establishing the gigabit network test bed, ARL successfully created a local certificate authority (CA) using the *openssl* tool-set (www.openssl.org). The CA was then used to issue and to sign the certificates that were required for mutual authentication between the server and its clients. This accomplishment enabled ARL to experiment with various cryptographic options such as cipher suites, protocols, and key sizes. Being able to create an internal CA increases the flexibility and the capabilities of ARL to meet current and future needs for conducting empirical IA research concurrently with the building of a secure distributed computing repository of sensitive ERA. Moreover, since ARL anticipated that the use of certificates will be very likely to recur in the future, it documented the tested procedure for creating a local CA in an internal memorandum record (*6*). No sooner had the document been prepared than it was used by the investigator of task 2.3 to generate certificates necessary for the evaluation of a VPN product.

The emulated ERA web portal ran in the host named *beaver* using the Apache web server version 2.0.52. The client of the portal ran in other hosts (*bear*, *bulldog*, *tiger*, and *terrapin*). ARL-generated test data files were placed at the ERA portal, thereby emulating a set of typical ERA. The information about data-transfer rates was captured each time the client fetched a file from the portal using the *curl* web client tool (curl.haxx.se). Running concurrently with the portal was the *ssldump* network protocol analyzer (www.rtfm.com) that recorded the timing information associated with two distinct phases of a TLS session: hand-shaking phase and application-data transfer phase. The timing information was later extracted from the output of the *ssldump* to determine the overhead costs. The data transfer rate information and the captured timing information were used to establish a baseline performance of the test bed. Preliminary results are depicted in figures 2 through 4.

Figure 2 shows data transfer rates (effective throughput) for secured and unsecured transfer of files from the ERA portal to its clients. The figure shows the measured throughput as a function of file sizes and used cipher suites. Such throughput is the upper boundary of the test bed, obtained in a scenario in which the server had only one client that was located at only one “hop” away from the server.

The graphical data shown corroborate an efficiency claim of the advanced encryption standard (AES), which is the current Government-endorsed encryption algorithm (*7*). The measured throughput was higher whenever the AES algorithm was used (AES256-SHA and DHE-RSA-AES256-SHA) and lower whenever the triple data encryption standard (3DES) algorithm (*8*) was used. The 3DES algorithm is also a Government standard, but it is being phased out and replaced by the AES algorithm. In summary, securely transferring data via the AES algorithm is faster than using the 3DES algorithm.

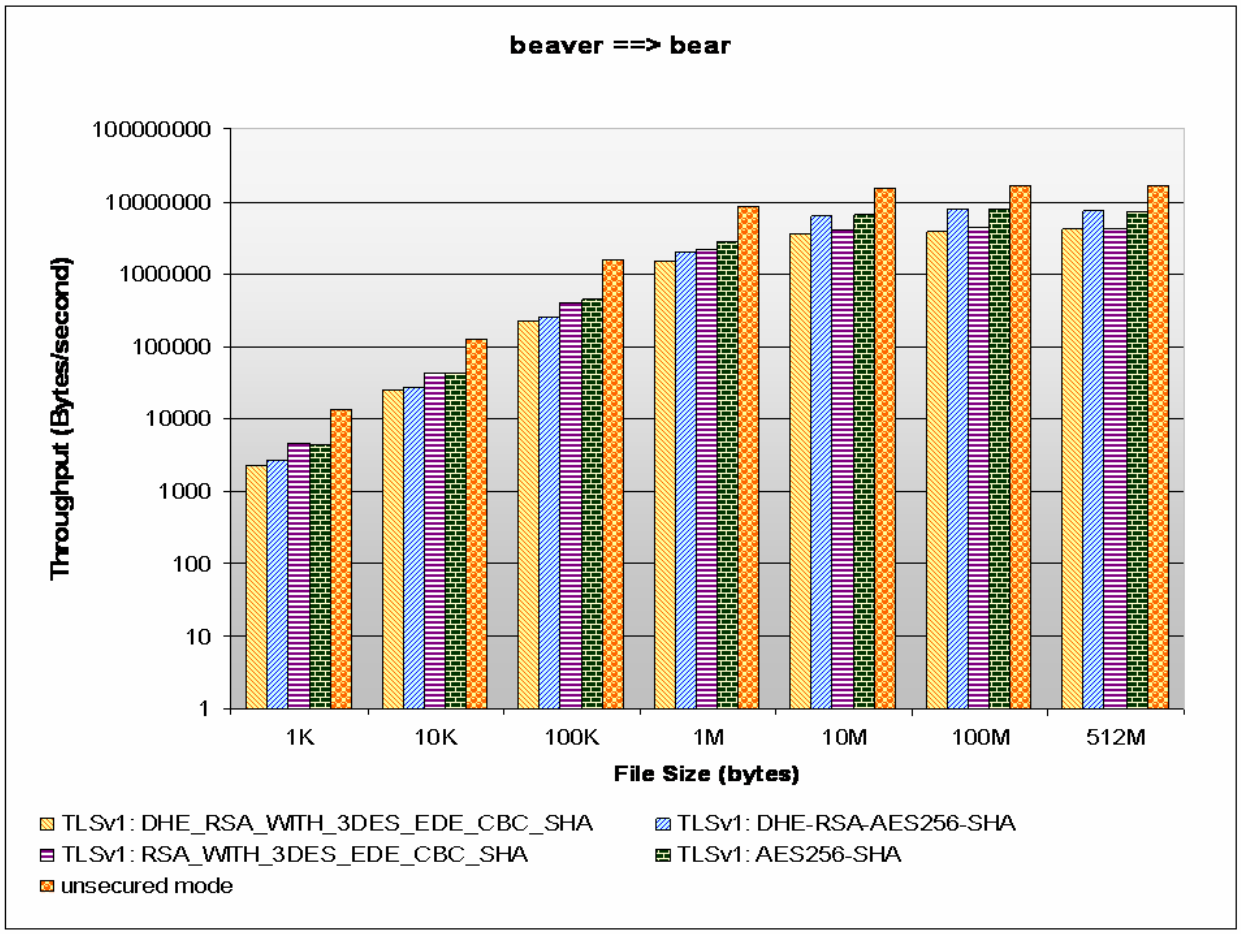

Figure 2. Comparative throughput for various high-strength cipher suites.

As seen from the figure 2, the use of the cipher suite AES256-SHA yielded highest throughput among the four high-strength cipher suites. The AES256-SHA cipher suite specifies the use of the AES algorithm with 256-bit key for data confidentiality, the standard hash algorithm (SHA) for data integrity and message authentication, and the Rivest, Shamir, and Adleman (RSA) algorithm for authentication and for exchanging the secret key.

In addition to the comparative throughput for various cipher suites, we computed the time overhead that was considered as a cost of using the TLS protocol. Figure 3 shows this overhead as a function of various cipher suites and file sizes. For example, transferring a 512-megabyte data file in secure mode with a cipher suite that includes the 3DES algorithm would take almost three times longer than transferring it in an unsecured mode. However, if one is using a cipher suite that requires the use of the AES algorithm, then this overhead would be halved. The figure, along with figure 2, illustrates a benefit of using the AES algorithm instead of the 3DES algorithm: faster transfer of data files.

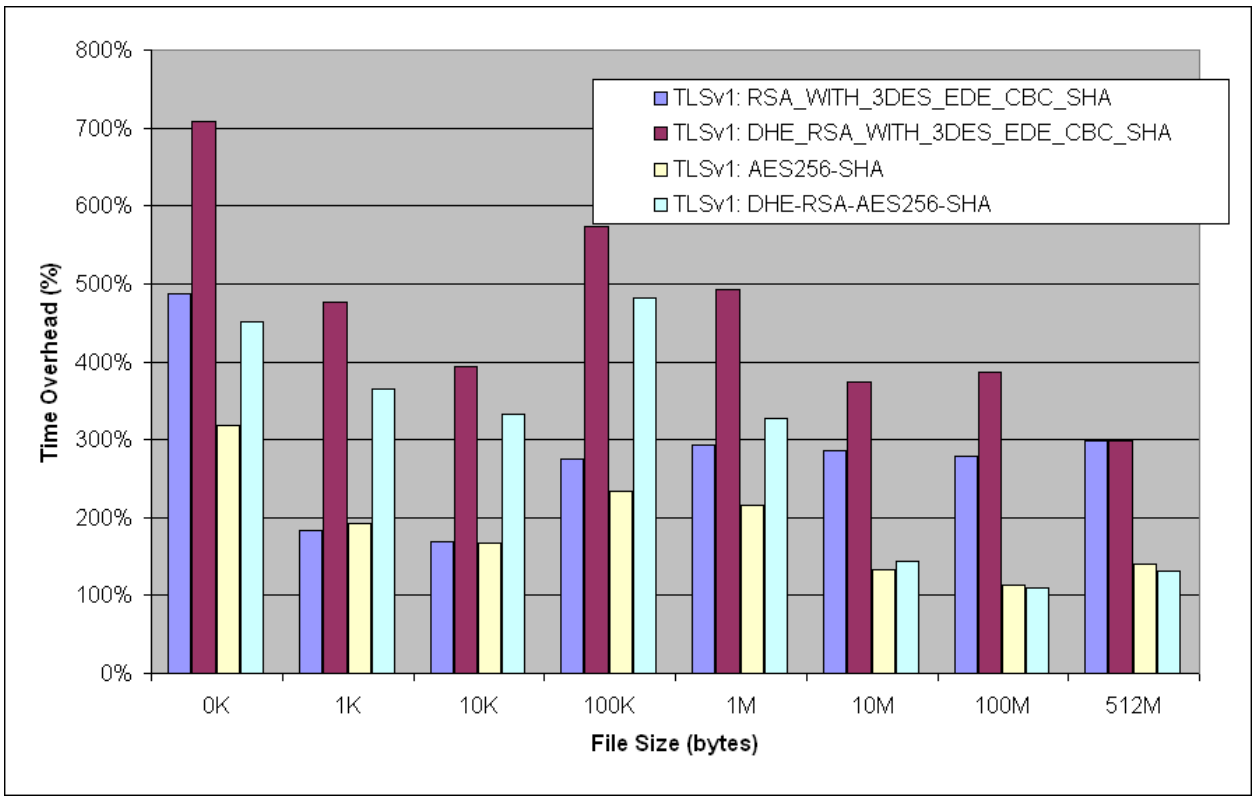

Figure 3. Overhead costs incurred by the TLS protocol and high-strength cipher suites.

Since the TLS protocol has two phases, the last experiment computed the percentages of time that each phase requires to transfer a data file securely. The first phase is the *handshake* phase during which the server and the client authenticate one another, negotiate for an appropriate cipher suite, and exchange the secret key. The second phase is the data transfer phase during which the requested data file is securely transferred from the server to the client via the mutually agreed cipher suite. The time required for the *handshake* phase was expected to be independent of the size of the data file. The time required for the secured data transfer phase was a function of the size of the data file given the same cipher suite.

Figure 4 shows the percentages of time taken during each phase. Keeping the *handshake* phase relatively short in terms of total elapsed time (e.g., 20% or lower) requires that the size of future ERA files be 10 megabytes or larger.

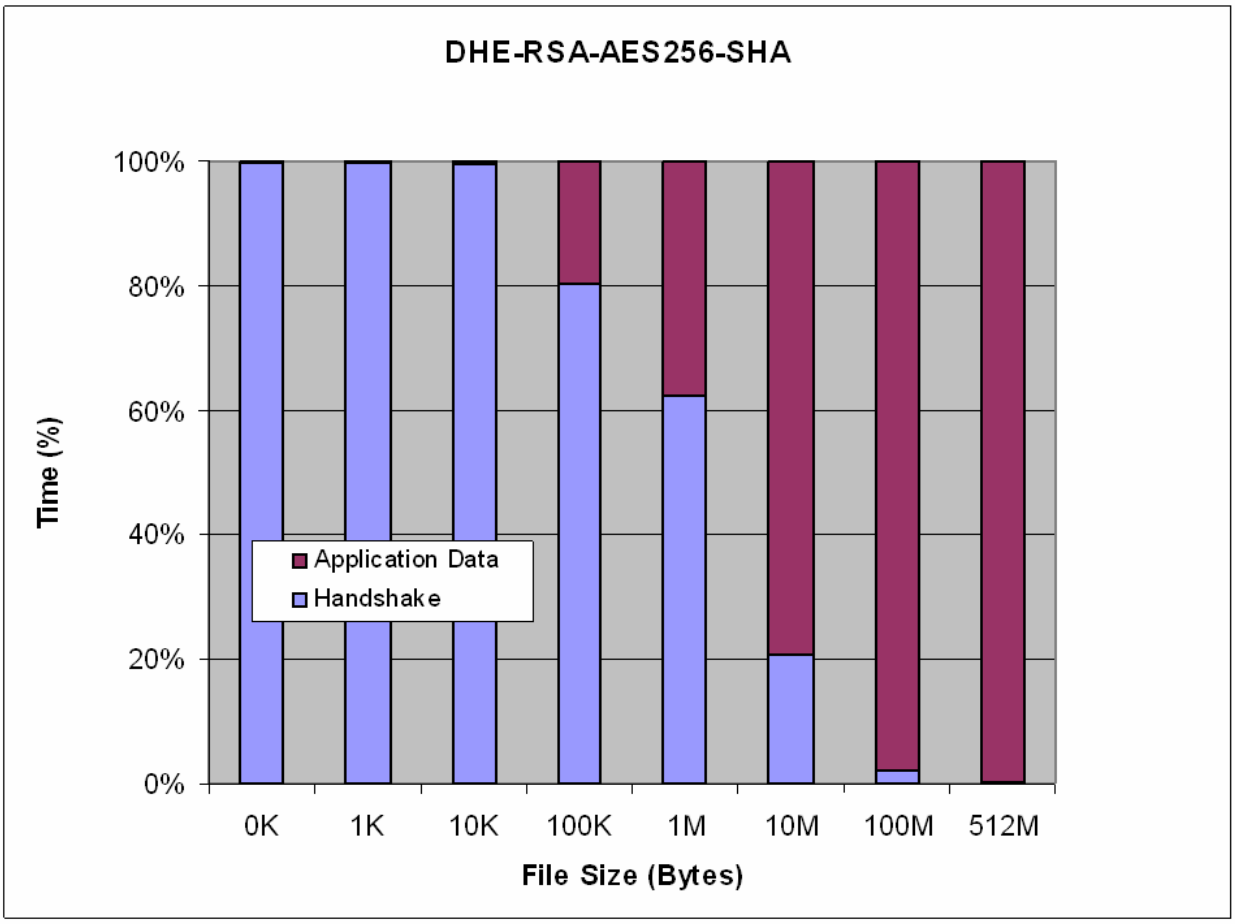

Figure 4. Percentages of time required during each phase of the TLS protocol.

The system throughput was also measured and analyzed when the client was running at other hosts (*bulldog*, *tiger*, and *terrapin*), and the results were similar to those obtained when the client was only one hop away from the server. This peculiar phenomenon was not expected, and thus additional tests were conducted to search for its causative factors. When each client ran in a separate host computer concurrently, the throughput was observed to be reduced inversely to the number of concurrent clients. The system basically reached its limits, and the measured throughput was indeed the upper boundary performance of the server.

In summary, the TLS protocol is undoubtedly effective and highly suitable for securely transferring sensitive ERA in public networks. Using the protocol together with cryptographic certificates and Government-approved high-strength cipher suites, basic information assurance can be reasonably provided for sensitive ERA.

Cryptographic certificates provide mutual authentication and non-repudiation services whether they are internally issued or obtained from a trusted third party. With certificates, only authorized clients having valid certificates are allowed to access the sensitive portal of ERA,

effectively precluding unauthorized users from connecting with the secure portal. Being able to establish an internal CA increases the flexibility and the capabilities of ARL to conduct empirical IA research potentially capable of supporting the building of a secured distributed computing environment in which sensitive ERA are processed.

2.3 Evaluation of Virtual Private Network (VPN) Technologies

The objective of this evaluation was to verify the operation of necessary security features and compare the network performance under OpenVPN (openvpn.net) operation with the network performance under no VPN operation (non-VPN) in a gigabit network environment. The reason for selecting OpenVPN product was based on the previous findings of Khanvilkar and Khokhar (*9*), which report that OpenVPN provides all the necessary security features and has an above-average network performance rating compared to all other VPN products that the authors tested.

This task has two subtasks. The primary subtask was the evaluation of OpenVPN. The other task was to build a gigabit network test bed environment in which all empirical IA research studies were conducted. Since the test bed is an isolated network, it is an ideal environment in which a true baseline performance of OpenVPN can be measured and evaluated.

Figure 5 shows the test bed configured for the evaluation of the OpenVPN product. The test bed was formed by the addition of two more networked computers (*colonial and patriot*) to the test bed that was used for the experimentation of the TLS protocol (figure 1). The first computer was connected to the subnet controlled by the host named *beaver*, and the second computer was connected to the subnet controlled by the host named *terrapin.* The two hosts established a VPN in which all the evaluation activities were performed.

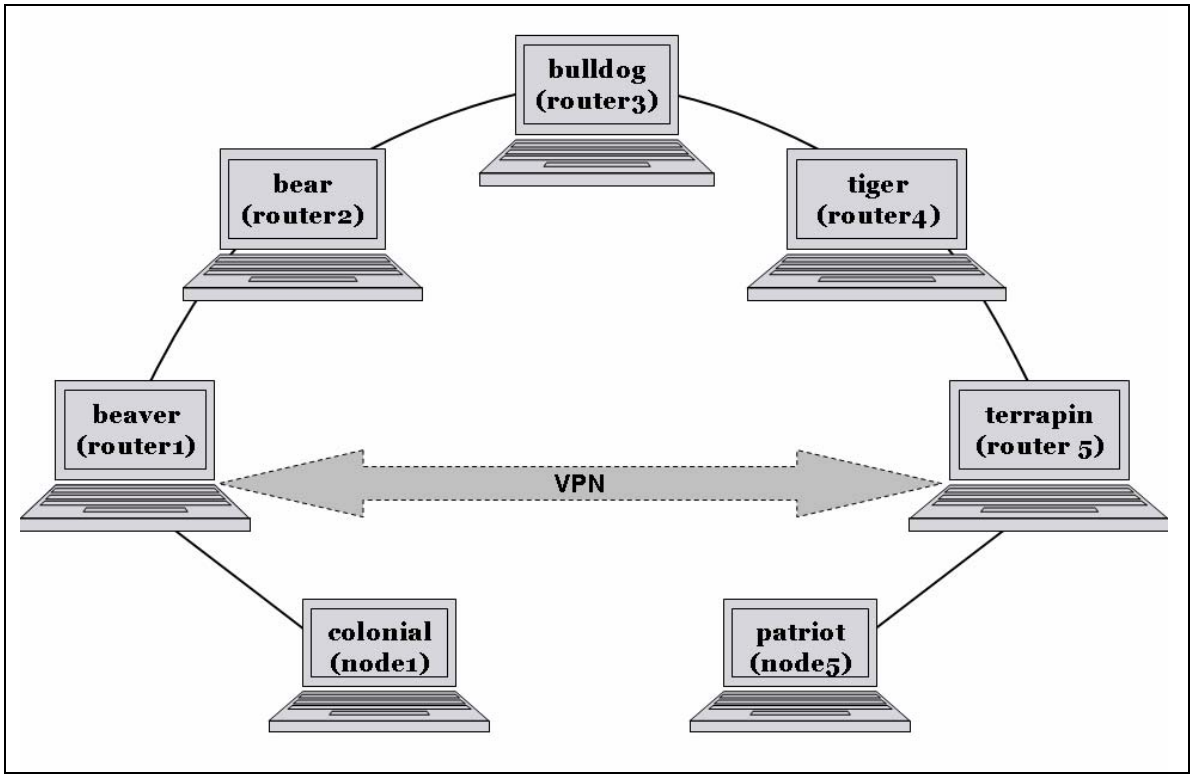

Figure 5. The configuration of the test bed for evaluating a VPN.

The gigabit network test bed consisted of five routers and four gigabit network hops. Each router, a Dell laptop, was configured with two gigabit network interfaces and operated in Linux operating systems. These routers were connected together to link a six-gigabit local area network (LAN) together in a daisy chain. The *colonial* (node1) computer was connected to the far left of the LAN, and the *patriot* (node5) computer was connected to the far right. The *beaver* (router1) router and *terrapin* (router5) router were installed and configured with OpenVPN to enable them to communicate with each other securely through the VPN link.

Table 2 summarizes the evaluation of the open source OpenVPN version 2.0.7 based on security properties and network performance in the gigabit network test bed.

Table 2. OpenVPN evaluation results.

Properties	Features	Results	Remarks
Security	Confidentiality	Yes	AES, BF, DES3, CAST5
	Data Integrity	Yes	HMAC
	Authentication	Yes	Password, certificate of Authority
	Non-Repudiation	Yes	Certificate of Authority
	Anti-Replay	Yes	
Network Performance (compared to non-VPN)	Overhead in transferring 1MB	0.16 MB	95.96%; based NFS copy
	Bandwidth in the transmission-control protocol (TCP)	86.8 Mbps	(37.55%); based on iperf
	Bandwidth in the user-datagram protocol (UDP)	124.5 Mbps	(15.31%); based on iperf
	Latency	2.504 ms	31.10%; based on ping
	Jitter	0.03275 ms	11.02%

The measurement of bandwidth performance (of non-VPN or VPN) in Transmission Control Protocol/User Datagram Protocol (TCP/UDP) based on *iperf* (an open-source network-performance measurement tool) depends on a few characteristics of LAN such as link speed (1 Gbps for this application), maximum transfer unit (MTU), and TCP/UDP socket send/receive buffer. These characteristics can vary, depending on the default setting of operating systems and manufacturers of network interfaces. Besides these default settings, OpenVPN also sets the default for TCP/UDP socket send/receive buffer to 64 KB through VPN link. When these network characteristics are tuned, the network bandwidth measurement through *iperf* can be higher and approach the link speed. For the purpose of this evaluation, we used only the lowest attainable bandwidth in non-VPN and VPN case based on all the defaults of hardware and software.

Having analyzed the results of this evaluation, we noticed that OpenVPN provides all the necessary security features for the building of a secure distributed computing of ERA. The reduction of network performance of networks with VPN compared to non-VPN network case was moderately reasonable in exchanging for the network security in transmission. The network overhead in using OpenVPN appeared to be almost 96% compared to non-VPN case, but this increase in network overhead can be minimized if we tune the MTU and TCP/UDP socket buffer.

Further investigation is needed to configure and tune OpenVPN to maximize the network performance for the building of an operational secure distributed environment for processing sensitive ERA.

3. Barriers and Resolutions

These three tasks were more complex than we initially realized. Two areas presented real challenges:

- Since ARL is a military agency and NARA is a civilian agency, there were concerns in the areas of policy and procedures with installing a system that would capture data at NARA and transfer them to ARL for analysis. The solution was to install a mini-version of ARL's IDS at NARA. This system would remain at NARA, and ARL will train NARA in the use of and analysis of data that are maintained in the system.
- The other challenge was the fact that an actual secure portal was unavailable for experimentation purposes. This obstacle precluded the conduct of empirical studies of IA products on an actual secure portal of NARA. Overcoming this obstacle required ARL to build a test bed environment and a secure web server. The test bed was a four-hop gigabit network of notebook computers running the Red Hat Linux operating system, which is the same operating system being deployed at an actual portal of NARA, which ARL could not access during the performance period. All computer software programs and scripts developed and run in this test bed will run in the actual environment with minor adjustment or modification.

4. Conclusions and Recommendations

The measured throughput, performance measurements, and projected estimations of performance reported in this document are system specific to the test bed environment in which the studies were conducted. They should not be used as a replacement for an actual experimentation with an authentic portal of sensitive ERA with the same computer code and measurement techniques. Therefore, the measurement will be relatively straightforward and thus is expected to be more expeditious.

ARL finally was able to successfully build an isolated multi-hop, gigabit network test bed locally for conducting empirical evaluation and experiments. Cryptographic protocols, algorithms, and tools potentially capable of providing basic information assurance services were empirically studied. Initial experimental results suggest that

- The TLS protocol will be the only protocol to be deployed in every actual secure portal or web server that has sensitive electronic records archives

- Mutual authentication between the server and its clients will be enabled via cryptographic certificates, which can be created and managed locally if the user pool is small.
- The size of an archive will be set to at least 10 megabytes.
- The following cipher suites, listed in the order of their preference, will be used in the secure transfer of ERA over a public network:
    - TLS_DHE_DSS_WITH_AES_256_CBC_SHA
    - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
    - TLS_RSA_WITH_AES_256_CBC_SHA
- A VPN will be established whenever remote access to an ERA network is required.

To meet the distributed ERA-processing research needs of NARA for persistent preservation of authentic electronic records archives, the following technical endeavors are recommended:

- Transfer advanced intrusion detection technologies to NARA.
- Continue conducting empirical research, test, and evaluation of advanced cryptographic algorithms and protocols for example, elliptic curve cryptography (ECC).
- Further empirically experiment with secure communications technologies and products that employ cryptographic tunneling protocols (e.g., VPNs).
- Provide reasonable assurances for authentic archives in processing by assessing the potential risks associated with the use of advanced ERA-processing tools and techniques.
- Increase the flexibility and capability of the test bed by implementing advanced emulation and virtual network technologies to create various network configurations.
- Investigate potentially enabling distributed computing technologies that can be used to build advanced distributed environments for collaboratively processing ERA.

5. References

1. Dierks, T.; Allen C. "The TLS Protocol Version 1.0" RFC 2246, January 1999, http://www.ietf.org/rfc/rfc2246.txt.

2. Coarfa, Christian; Druschel, Peter; Wallach, Dan S. Performance Analysis of TLS Web Servers, *Network and Distributed System Security Symposium Conference Proceedings*: San Diego, California, 6–8 February 2002. URL: http://www.isoc.org/isoc/conferences/ndss/02/proceedings/papers/coarfa.pdf (accessed 11 October 2006)

3. Apostolopoulos, G.; Peris, V.; Saha, D. Transport Layer Security: How much does it really cost? *INFOCOM'99, Conference on Computer Communications, Eighteenth Annual joint conference of the IEEE Computer and Communications Societies* 21–25 March 1999. http://citeseer.ist.psu.edu/apostolopoulos99transport.html

4. He, Xubin. A Performance Analysis of Secure HTTP Protocol, *Storage Technology and Architecture Research (STAR) Lab Technical Report*, Tennessee Technological University, March 2003 http://iweb.tntech.edu/hexb/publications/https-STAR-03122003.pdf

5. Bergman, Michael K. The Deep Web: Surfacing Hidden Value, *The Journal of Electronic Publishing, University of Michigan Press*, Aug 01, Vol 7, Issue 1, ISSN 1080–2711 http://www.press.umich.edu/jep/07-01/bergman.html

6. Nguyen, B. *Issuing Cryptographic Certificates Using OpenSSL*; ARL-MR-655; the U.S. Army Research Laboratory (ARL): Adelphi, Maryland, December 2006.

7. "Advanced Encryption Standard", Federal Information Processing Standards (FIPS) 197, National Institute of Standards and Technology (NIST), November 2001. URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

8 "Data Encryption Standard", FIPS 46-3, NIST, October 1999. URL: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

9 Khanvilkar, S.; Khokhar, A. Experimental evaluations of open-source Linux-based VPN solutions. *Proceedings of the 13th International Conference on Computer Communications and Networks (ICCCN)*, 11–13 Oct. 2004, pp, 181–186.

INTENTIONALLY LEFT BLANK.

Distribution List

ADMNSTR
DEFNS TECHL INFO CTR
ATTN DTIC-OCP (ELECTRONIC COPY)
8725 JOHN J KINGMAN RD STE 0944
FT BELVOIR VA 22060-6218

DARPA
ATTN IXO S WELBY
3701 N FAIRFAX DR
ARLINGTON VA 22203-1714

OFC OF THE SECY OF DEFNS
ATTN ODDRE (R&AT)
THE PENTAGON
WASHINGTON DC 20301-3080

US ARMY TRADOC
BATTLE LAB INTEGRATION & TECHL DIRCTRT
ATTN ATCD-B
10 WHISTLER LANE
FT MONROE VA 23651-5850

SMC/GPA
2420 VELA WAY STE 1866
EL SEGUNDO CA 90245-4659

COMMANDING GENERAL
US ARMY AVN & MIS CMND
ATTN AMSAM-RD W C MCCORKLE
REDSTONE ARSENAL AL 35898-5000

US ARMY INFO SYS ENGRG CMND
ATTN AMSEL-IE-TD F JENIA
FT HUACHUCA AZ 85613-5300

US ARMY RSRCH LAB
ATTN AMSRD-ARL-CI-OK-TP TECHL LIB T LANDFRIED (2 COPIES)
BLDG 4600
ABERDEEN PROVING GROUND MD 21005-5066

NATL ARCHIVES & RECORDS ADMIN
ELECT RECORDS ARCHIVES PROG MGMT OFC
ATTN R CHADDUCK (5 COPIES)
8601 ADELPHI RD
COLLEGE PARK MD 20740-6001

US GOVERNMENT PRINT OFF
DEPOSITORY RECEIVING SECTION
ATTN MAIL STOP IDAD J TATE
732 NORTH CAPITOL ST., NW
WASHINGTON DC 20402

US ARMY RSRCH LAB
ATTN AMSRD-ARL-CI-HN J COLE (2 COPIES)
ABERDEEN PROVING GROUND MD 21005

DIRECTOR
US ARMY RSRCH LAB
ATTN AMSRD-ARL-RO-EV W D BACH
PO BOX 12211
RESEARCH TRIANGLE PARK NC 27709

US ARMY RSRCH LAB
ATTN AMSRD-ARL-CI-CN B LUU
(2 COPIES)
ATTN AMSRD-ARL-CI-CN B NGUYEN
(2 COPIES)
ATTN AMSRD-ARL-CI-CN G RACINE
(2 COPIES)
ATTN AMSRD-ARL-CI-OK-T TECHL
PUB (2 COPIES)
ATTN AMSRD-ARL-CI-OK-TL TECHL
LIB (2 COPIES)
ATTN AMSRD-ARL-D J M MILLER
ATTN IMNE-ALC-IMS MAIL &
RECORDS MGMT
ADELPHI MD 20783-1197