

Final Report: Navy STTR – Information-Centric Security

Submitted by: TecSec® Incorporated
1953 Gallows Road
Suite 220
Vienna, VA 22182

George Mason University
American Management Systems

Phase I Contract Number: N00014-03-M-0342

Office of Naval Research STTR

Phase I Award Start Date: 01 JUL 2003

Phase I Award End Date: Apr 04

Proposal Title: Information-Centric Security

Data Item Number: 0001AC Final Report

Security Classification: None

Issuing Government Activity: Office of Naval Research

Submitted on: February 4, 2004

Principle Investigator: Dr. Wai Tsang / TecSec
(703) 744 8447
wait@tecsec.com

Corporate Official: Ms. Karen Burkardsmaier
(703) 744-8488
karenb@tecsec.com

Report Documentation Page		Form Approved OMB No. 0704-0188
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.		
1. REPORT DATE 06 FEB 2004	2. REPORT TYPE Final	3. DATES COVERED 01 Jul 2003 - 06 Feb 2004
4. TITLE AND SUBTITLE Information-Centric Security		5a. CONTRACT NUMBER N00014-03-M-0342
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Tsang, Wai; Scheidt, Ed; Burkardsmaier, Karen		5d. PROJECT NUMBER N00014-03-M-0342
		5e. TASK NUMBER 0001AC
		5f. WORK UNIT NUMBER TS_REP_0001AC
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) TecSec Incorporated 1953 Gallows Road Suite 220 Vienna, VA 22182		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Office of Naval Research Attn Dr. Ralph Wachter, ONR 311, Attn John Williams, ONR 364 800 North Quincy Street Arlington, VA 22217-5660		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 Under Phase I, the TecSec team focused on applying information centric security in a commercial medical and healthcare scenario. Use cases showed the utilization of a portable electronic device (PED) to assure information resident on the PED. However, the platform is not well protected as information is moved along from the host PED to its final destination. As governed by laws (i.e., Healthcare Information Portability and Accountability Act or HIPAA), medical information must be assured of its confidentiality, integrity and availability (CIA). Cryptography can be used for access control enforcement. It is further recognized that an efficient key management must be emplaced to accommodate the mobile operating environment where it is often represented by a dynamic, ad-hoc environment. In order to access the feasibility of such a security design, the Team assesses the feasibility of such a design alternative. In line with the certification and accreditation, a hardware implementation of asymmetric key management was examined. The use of a field programmable gate array (FPGA) was examined, benchmarked and validated. In order to capitalize on the fast moving commercial market, we evaluate the buy vs. make option and recommend that an initial design is to host the information centric security solution on a PED platform which is the HP/Compaq iPAQ h5500 Personal Digital Assistant (PDA). A Phase II 5-Page Plan, which focuses on the benefits for Future Naval Capabilities, was submitted on February 4, 2003.		

15. SUBJECT TERMS

Key management, Cryptography, Confidentiality, Integrity, Availability, CKM, Cryptographic Cores, PEDs and PDAs, FPGA, FPGA/ASIC Hybrid, Role Based Access Control, Insider Threat, Trust Model, HIPAA, Commercial and Naval Medical Use Cases (Medical Use Case: Military Medical Records; Medical Use Case: Point-of-Care Information Assurance)

16. SECURITY CLASSIFICATION OF:

a. REPORT

unclassified

b. ABSTRACT

unclassified

c. THIS PAGE

unclassified17. LIMITATION
OF ABSTRACT**SAR**18. NUMBER
OF PAGES**23**19a. NAME OF
RESPONSIBLE PERSON

Table of Contents

Introduction	3
Administrative Overview	3
Topic Review	4
Topic Issues and Problem Understanding	4
Topic Objectives	5
Shift of Focus	5
Goals of Objective	6
Team Composite	6
Summary of Results from the Phase I Effort	8
Performance criteria and design goals	8
Assessment of the Results	9
Medical/Healthcare Use Cases	10
The HIPAA context	10
The Health Insurance Portability and Accountability Act (HIPAA)	10
Medical Use Case 1: Point-of-Care Information Assurance	13
Medical Use Case 2: Military Medical Records	14
PEDs (Portable Electronic Devices)	16
Developing a Business Case for a Mobile Device such as a PDA	17
Information-Centric Cryptography and Key Management	19
Cryptographic Cores	19
Cryptography	20
Constructive Key Management (CKM) With Strong Authentication	21
Next Steps	22
Near term: Phase I option	22
Mid term: Phase II	22
Long term: Phase III/Commercialization Phase	22
Appendix A - Overview of the Trust Model	23

Introduction

This final report outlines the objectives and findings of Phase I of the Navy STTR N00014-03-M-0342 for Information-Centric Security. A companion 5-page document has been created to discuss the proposed plan for a Phase II effort.

ADMINISTRATIVE OVERVIEW

Non-Disclosure Agreements between the team members were executed. Further, an Intellectual Property Agreement (Cooperative Research and Development Agreement – CRADA) between TecSec and George Mason University was established and forwarded to Mr. John Williams of the Office of Naval Research. No new IP was developed as a result of Phase I research.

The first meeting with the original COTR, Mr. Frank Deckelman, was held in August of 2003.

Several technical interchange meetings between the team members took place during Phase I.

The first meeting with the new COTR, Dr. Ralph Wachter, took place on January 21, 2004. The focus of this meeting was to meet the new COTR and discuss Phase I as well as the plans for Phase II.

At the January 21 meeting, it was agreed upon that the TecSec team would continue building on the medical applications and business cases using Portable Electronic Devices (PEDs) and focus on how these applications would apply to Future Naval Capabilities – C4&ISR.

An additional research focus for Phase II would include Naval Sensor Protection with access control and confidentiality enforced through encryption.

Topic Review

The initial objective of this topic was to develop an information centric security prototype for demonstration in representative operational environments and prepare for NIAP and FIPS-140 certification for commercialization.

The scope for Phase I (as outlined in topic N03-T008 Information-Centric Security) was to review previous government sponsored research, perform original research to extend the concepts previously considered, propose a working model of an information centric security prototype, and investigate a combination client and server version based on ANSI Standard X9.69.

The scope for Phase II (as outlined in topic N03-T008 Information-Centric Security) was to develop a prototype that would achieve role based access control of information resident on a Local Area Network (LAN) within a protected environment that demonstrates separation of data within the automated information system, collect data concerning the performance and scalability of the prototype for sensitive but unclassified data, and investigate the feasibility of moving the prototype model into firmware.

One of the key research areas related to Information Centric Security is Knowledge Superiority and Assurance. The Future Naval Capabilities (FNC) process was designed to raise the focus from individual technology goals to the achievement of future capabilities for naval forces with inputs from the Commander in Chief's Command Capability Issues and from Headquarter Marine Corps' capabilities needs. In parallel, one of the President's priorities as espoused in the National Strategy to Secure Cyberspace is to reduce the malicious insiders in cyberspace who seek to exploit vulnerabilities.

TOPIC ISSUES AND PROBLEM UNDERSTANDING

Today, an insider threat from a person or persons working for an organization can range in degree of sophistication from novice to skilled to the most highly placed and experienced. The privileges of an insider can vary from a user possessing limited access to a user holding access to cross-organizational assets. The insider can be an individual on the job for many years, perhaps only recently departing and leaving malicious software code behind to do damage, or put in place for later use by another user. In any case, an 'Insider Threat' could consist of any number of plausible scenarios.

The Department of Defense (DoD) and the Intelligence Community (IC) are extremely selective in who is cleared for access to physical and logical assets. These users are granted various levels of permission after a stringent process of security checks and verification. Historically in the classified world, a combinatorial portfolio of physical identification and Authentication procedures are emplaced to assure and enforce physical security in addition to a number of procedures that are required for gaining logical access to assets of automated information systems.

Recent augmentations to overall security, such as portal and digital dashboards, are gaining traction within the IC and DoD communities under the concept of available ease of use for authorized users. Today's systems are aggregating large volumes of information in broad enclaves using local area networks (LANs) and commercial-off-the-shelf (COTS) products and workstations. Once accreditation takes place, the designated insider can have a broad reign over access to data, being able to retrieve, disseminate, and in some cases even modify classified data across the most secure IC and DoD networks comprising Coalition Wide Area Network (CoWAN), Secret Internet Protocol Router Network

(SIPRNET), Joint Worldwide Intelligence Communications System (JWICS), Intelink, StoneGhost, and so forth.

The result of an insider misusing their access privileges and the misuse of such global information sets, as well as the evidence of known past hostile intrusions, continues to represent a visible tip of a much larger iceberg of uncertainty concerning the overall Authentication status of government information access, such as document control.

When some accredited and authorized insiders to the enclave of protected government secrets violate the rules and circumvent the policy set in place, we, the country, are faced with the most serious of security problems. As networks continue to grow and interconnect and move into more and more open, wireless modes of operation, unattended steps to correction of the Insider Threat and Document Control will only serve to exacerbate the ongoing problem. Defense against an insider who tries to abuse their computing privileges is one of the most critical security problems facing the Information Assurance (IA) segment because an insider can catastrophically damage the automated information systems (i.e., networks and computer systems).

Handling of data and information must be similar to the handling of corresponding paper documents. If the insider has a right to access and the overseer of that data designates that the insider has a need to access, the security tools must effect a separation of data so that only that data designated for need to access is available.

The topic of the insider access has as much relevance to the medical services as future naval services. The insider can be a medical administrator, hospital staff, or a physician. The security tools developed for the Navy can have direct applicability for medical services applications. The blurring of computing capabilities with mobility is necessary for Navy applications and for the medical services.

The insider threat is being emphasized now. The physical security barriers and encryption tools for Authentication have been demonstrated as effective shields for the outside threat. New developments in encryption frameworks can enhance these traditional Authentication tools to further an Authorization capability. Role based access control and data separation access can be elements of Authorization. A third piece for the new security tools is the Trusted Platform. The operational environment needs to compliment the global nature of Authentication and the local nature of Authorization.

TOPIC OBJECTIVES

The original objectives were included in the Phase I proposal and were as follows:

- Task 1: Review previous government sponsored research
- Task 2: Working model of an information centric security design
- Task 3: Common Criteria EAL and FIPS 140-2 Certification
- Task 4: Key Management Enhancement with RBAC
- Task 5: Investigate the feasibility of an extended ANSI X9.69 to a hybrid client/server system

These objectives have been shifted to focus on a common solution for Navy and medical services.

SHIFT OF FOCUS

The first meeting with the original COTR, Mr. Frank Deckelman, was held in August of 2003. During the course of this meeting the original objectives shifted to focus on securing medical information and data employing PDAs for both military and commercial environments.

The objectives for Phase I that evolved out of discussions with the COTR at August meeting included the following elements:

- Evaluation of potential medical use cases
- Qualify Customers (healthcare providers, e.g. physicians, medical administrators, hospital staff, nurses, etc)
- Provide Use Cases
- Build up business case to support an Authorization capability enforced through encryption
- Role Based Access Control enforced through a Constructive Key Management encryption framework using a mobile or PDA platform
- Prototype and demonstrate in Phase II
- Assess committing part of the CKM combiner architecture to firmware
- Assess PDAs, Wireless Devices for an encryption capability platform
- Certification and system architectural criteria would be further extended into Phase II. Other related computing technologies such as VOIP and multiple domain applications, where encryption can be a value added technology, could be extended into another activity phase.

GOALS OF OBJECTIVE

The Phase I goal is to establish that encryption has a business case for Navy and the Medical services in mobile environments and that the resultant solution can address the insider threat.

The Phase II goal is to prototype a mobile environment using a portable electronic device (PED) such as a PDA with an encryption framework that can address the insider threat.

Additional goals include:

- To provide solutions that not only benefit the Navy but that can provide generic security solutions for the Department of Defense (DoD), Northern Alliance Treaty Organization (NATO), Department of Homeland Security (DHS), Southern Command (SOCOM), Joint Forces Command (JFCOM), the Intelligence Community, other Federal sectors as well as the commercial sector.
- To result in a commercial solution to keep the costs down
- To use market solutions that can be enhanced and that would result in quicker time-to-market
- To get new security related capabilities into the hands of users faster

TEAM COMPOSITE

The TecSec team for Phase I was composed of TecSec, George Mason University (GMU), and American Management Systems (AMS). The team composite reflects TecSec's desire to leverage the wholly integrated team concept to extract the best features of each team member. TecSec possesses the core competence and knowledge about ANSI X9.69 and the key management scheme, Constructive Key Management® (CKM®). GMU, with its renowned Center for Secure Information Systems (CSIS), is poised to add to the advancement of technologies to tighten and strengthen the new CKM functionality.

TecSec is bringing in AMS to explore and expand CKM deployments and applications. AMS is a global business and information consulting firm and a recognized expert in Application Security, National Information Security Strategy, Information Operations, Information Assurance and Large-Scale Systems Development & Integration. TecSec believes that this team can bring forth a viable advanced concept design with enough real world realism that it will be adopted and deployed in many different sectors.

Summary of Results from the Phase I Effort

Under Phase I, the TecSec team focused on applying information centric security in a commercial medical and healthcare scenario. Use cases showed the utilization of a portable electronic device (PED) to assure information resident on the PED. However, the platform is not well protected as information is moved along from the host PED to its final destination. As governed by laws (i.e., Healthcare Information Portability and Accountability Act or HIPAA), medical information must be assured of its confidentiality, integrity and availability (CIA). Cryptography can be used for access control enforcement. It is further recognized that an efficient key management must be emplaced to accommodate the mobile operating environment where it is often represented by a dynamic, ad-hoc environment. In order to access the feasibility of such a security design, the Team assesses the feasibility of such a design alternative. In line with the certification and accreditation, a hardware implementation of asymmetric key management was examined. The use of a field programmable gate array (FPGA) was examined, benchmarked and validated. In order to capitalize on the fast moving commercial market, we evaluate the buy vs. make option and recommend that an initial design is to host the information centric security solution on a PED platform which is the HP/Compaq iPAQ h5550 Personal Digital Assistant (PDA).

PERFORMANCE CRITERIA AND DESIGN GOALS

The team approach is to ensure that the proposed innovation minimally impact the existing infrastructure. The message rings loud and clear from our team members who have spent years in the arena. Fully recognizing that there are disparate hardware and systems in terms of capabilities and functionalities, the solution will have to be designed to address the major portion of the equipment out there. With our team members' unique background, we propose the following parametric metrics as benchmarks in designing our information-centric security solution:

- Standards compliance—We will comply with published standards that are published and validated by national standards bodies and associations.
- Interoperability and scalability—Given that systems are so widespread, it is necessary to have a fieldable security solution capable of accommodating a large number of users across disparate disciplines (medical and healthcare as well as distributed sensor networks).
- Highly available and secure solution—The solution needs to ensure cyber security, and is capable of being evaluated and certified by the National Information Assurance Program (NIAP) under the Common Criteria (ISO 15777) and the Federal Information Processing System (FIPS) of National Institute of Science and Technology (NIST)
- Ease of use and retrofitable—Some infrastructure providers may not be amenable to a major fork-lift solutions, the solution should be retrofitted.
- Cost effectiveness—We are acutely aware of the role that economy plays in the eventual adoption of the solution. The Total Cost of Ownership (TCO) and Return of Investment (ROI) will be rationalized and justified.

ASSESSMENT OF THE RESULTS

The following sections provide an overview of the assessment of the results included in the following sections:

- Medical/Healthcare Use Cases
 - HIPAA as a driver
 - Use Cases
- PEDs (Portable Electronic Devices)
 - PDAs
 - FPGA Assessment
 - Rationale for Selection of the HP/Compaq iPaq h5550
- Cryptography
 - Cryptographic Cores
 - Key Management
 - CKM

Medical/Healthcare Use Cases

This section provides an overview of HIPAA and the HIPAA context as well as two specific use cases for protecting medical information on PDAs.

THE HIPAA CONTEXT

HIPAA is one of the major drivers for security in healthcare today.

The use of electronic mechanisms to store and transmit information is quickly becoming the standard across healthcare organizations. Paper records and forms are being replaced by electronic forms and applications, which use intranets (internal to organizations), extranets (between organizations) and the Internet (multiple organizations) as the mechanisms to transmit information.

The use of electronic mechanisms offers an organization much potential for cost savings through improved efficiency and enhanced quality of healthcare due to more accurate and timely information that is accessed by healthcare professionals. The Internet offers a unique opportunity for healthcare organizations to transmit electronic information such as patient information, electronic medical records, enrollment verifications and claims. In addition, electronic information in storage can be more easily accessed than paper information.

The use of electronic mechanisms can contribute to an organization's competitive advantages through streamlined business processes and improved quality of healthcare services to patients. The challenges for the organization are the ability to use electronic mechanisms in a secure manner and to protect patient information.

THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

HIPAA Privacy and Security Regulations cover the following requirements for the protection of patient information:

- Healthcare plans must obtain consent from patients about the release of medical information;
- Patients have the right to see their records and to request corrections;
- Health Plans and Providers must have administrative systems in place to protect health information;
- Information systems must protect data in transit and data at rest; and
- Access to data is based on a user's "need-to-know".

Sensitive Patient Identifiable Information (PII) and Protected Health Information (PIH) stored on and transmitted using handheld devices must also adhere to HIPAA rules and regulations.

Administrative Simplification will only drive costs out of health care delivery if privacy and security are addressed. An average of 26 cents of each health care dollar is spent on administrative overhead. Standard transactions reduce this figure. Electronic Data Interchange (EDI) allows partners to exchange information and transact business in a fast and cost-effective way. Code Sets include data elements used to uniformly document the reasons why patients are seen and what is done to them during their health care encounters (procedures). Identifiers are numbers used in the administration of healthcare to identify healthcare providers, health plans, employers, and individuals (patients).

The HIPAA Privacy Rule (effective 14 April 2003) necessitates mapping the data flows for Protected Health Information (PHI). The HIPAA Security Rule (effective 21 April 2005) implements application-layer controls for protection of data flows.

Security requirements are implied in the Privacy Rule. HIPAA requires “Chain-of-Trust Partner Agreements” between business partners. The Integrity and Confidentiality of transmitted data must be protected. Technical Controls include:

- Authentication
- Authorization
- Access Control
- Encryption
- Audit trail

In developing use cases to support HIPAA our base scenario assumes that provider personnel are issued a PDA. The main question to be posed when using a PDA in conjunction with medical information is: “*Who* knew *What* and *When*?” Parsing this question helps clarify the “Chain-of-Trust” issue which requires the information/medical data to be protected both at rest and in transit, and establishes the need for CKM.

When asking “*Who*?” the PDA must identify the provider by unique identification (UID). The PDA must also authenticate the provider by:

- Biometric (e.g. finger, voice)
- Real-time Shared Secret
- Password

When asking “*What*?” an additional question that needs to be posed is: “Which security objective carries more weight in a given use case, Integrity or Confidentiality?” HIPAA has elevated Privacy concerns and the need for data confidentiality. Patient care quality and malpractice issues necessitate the preservation of data integrity.

What data requires Integrity protection? The PDA must support the cryptographic protection of data integrity for the following data sources:

- Electronic Patient Records (EPRs)
- Laboratory Data
- Pharmacological
- Radiological Systems
- Other Specialized Clinical Systems

What data requires Confidentiality protection? The PDA must cryptographically enforce access controls on Protected Health Information (PHI) that can be used to establish individual patient identity. The PDA must also cryptographically enforce Role Based Access Controls by business functions within the provider domain. These business functions include:

- Patient Assess Services (Enrollment)
- Patient Financial Services (Billing)
- Health Information Management (Third Parties)

The third part of the main question in the HIPAA context is “*When?*” When has the particular data object been accessed? The PDA must support audit logging of cryptographic service events and the audit log file may be cryptographically protected.

MEDICAL USE CASE 1: POINT-OF-CARE INFORMATION ASSURANCE

The primary actor in this use case is a physician treating patients in a clinical setting. The goal is to enable physicians to utilize a single device to handle all data capture and retrieval needs securely in a clinical setting. Data integrity, confidentiality and non-repudiation are of primary importance from an information assurance perspective.

The system will consist of an HP/Compaq iPAQ Pocket PC loaded with medical software packages (records, diagnostics, prescriptions, etc.) and general-purpose personal productivity software (email, word processing, etc.). Security hardware and software will also be installed to improve system trustworthiness.

The success end condition consists of patients being diagnosed, treated, records being updated and charges being recorded. Access to information is appropriately controlled; changes to records are prohibited except for specified circumstances; digital signatures are bound to data objects; and audit trails are preserved.

The failed end condition would be that the security hardware and software fail to protect data integrity, confidentiality or enable user actions to be repudiated. A second failed end condition would be that the security system interferes with the clinical system.

The main success scenario describes the steps that are taken from trigger event to goal completion when everything works without failure. It also describes any required cleanup that is done after the goal has been reached. The steps are listed below:

Step	Actor	Action Description
1	Physician	Logs into the iPAQ handheld computer.
2	Security System	The security system executes Identification, Authentication, Authorization, and Access Control protocols. Audit functionality is working.
3	Physician	Patient comes in for treatment.
4	Physician	Accesses patient's generic, unspecified Electronic Medical Records (EMR).
5	Security System	Data elements available to the Physician role are decrypted.
6	Physician	Dictates notes to the iPAQ.
7	iPAQ	iPAQ updates the EMR.
8	Security System	Encrypts information the stored EMR data.

MEDICAL USE CASE 2: MILITARY MEDICAL RECORDS

As in the previous use case, the primary actor is a physician treating patients in a clinical setting. The Military Medical Records (MMR) case differs from the more general Point-of-Care use case in that a subset of records may contain sensitive information of national security interest (Prisoner-of-War treatment, military-related toxic exposures, weapons effects, etc.). Such sensitive information may be shared on a need-to-know basis with persons not affiliated with normal healthcare delivery operations.

The goal is to enable physicians to utilize a single device to handle all data capture and retrieval needs securely in a clinical setting. Data integrity, confidentiality and non-repudiation are of primary importance from an information assurance perspective.

The system will consist of an HP/Compaq iPAQ Pocket PC loaded with medical software packages (records, diagnostics, prescriptions, etc.) and general-purpose personal productivity software (email, word processing, etc.). Security hardware and software will also be installed to improve system trustworthiness.

The success end conditions consists of patients being diagnosed, treated, records being updated and charges being recorded. Access to information is appropriately controlled; changes to records are prohibited except for under specified circumstances; digital signatures are bound to data objects; and audit trails are preserved.

The failed end condition would occur if the security hardware and software failed to protect data integrity, confidentiality or enabled user actions to be repudiated. A second end condition would be that the security system interferes with the clinical system.

The main success scenario describes the steps that are taken from trigger event to goal completion when everything works without failure. It also describes any required cleanup that is done after the goal has been reached. The steps are listed below:

Step	Actor	Action Description
1	Physician	Logs into the iPAQ hand held computer.
2	Security System	The security system executes Identification, Authentication, Authorization, and Access Control protocols. Audit functionality is working.
3	Physician	Patient comes in for treatment.
4	Physician	Accesses patient's generic (unspecified) Electronic Health Records (EHR)
5	Security System	Data elements available to the Physician role are decrypted.
6	Physician	Dictates notes to the iPAQ.
7	iPAQ	iPAQ updates the EHR.

8 Security System Encrypts information the stored EHR data

This is a listing of how each step in the main success scenario can be extended. The extensions are followed until either the main success scenario is rejoined or the failed end condition is met. The step refers to the step that is extended in the main success scenario and has a letter associated with it (i.e., if step 3 changes the extension step is 3a).

Step	Condition	Action Description
1a.	Intelligence Analyst logs into system	Login proceeds as normal.
4a.	Intelligence Analyst accesses data record	Cryptographically-enforced Role Based Access Control (RBAC) limits data access to defined objects or data elements.

If a variation can occur in how a step is performed it will be listed here.

Step	Variable	Possible Variations
4a.	Physician accesses additional data	Access to a Department of Defense (DoD) CHCS II clinical data repository or a Department of Veterans Affairs (VA) VistA health data repository.
4b.	Physician accesses additional data	Access to detailed laboratory data from a military "Laboratory Data Sharing and Interoperability (LDSI)" compliant data service.

PEDs (Portable Electronic Devices)

Capabilities of portable electronic devices (PEDs) cover a wide spectrum. These portable and mobile platforms can be a two-way pager, a personal digital assistant (PDA), and a personal computer laptop. Our information-centric security solution involves cryptography with a key management system needed to be hosted on the PED platform. One of our assessments is to evaluate the feasibility of our solution on potential PED candidates, but we have also included PED platform constraints as outlined below:

- Limited processing power
- Limited memory
- Limited bandwidth
- Limited battery life
- Limited user interface

Below are tables that depict the timings for RSA, DSA and El-Gamal, and ECC operations on various PED platforms¹. It is noted that these PEDs represent the low and mid ranges in the PED group:

- RIM (Research-in-Motion) Pager
Intel 386, 10 MHz, 2 MB of flash memory, 304 KB RAM
1 AA battery + lithium cell
- PalmPilot PDA
Motorola 68000 “Dragonball”, 16 MHz,
2-4 MB RAM
2 AA battery + NiCad cell
- PC laptop
Pentium II, 400 MHz

Assumptions (Languages and Libraries)

- Language: C
- Libraries: Open PGP reference implementation
- Open SSL
- Code size: ~370 kB

RSA in Constrained Wireless Devices

	1024-bit modulus			2048-bit modulus		
	Pager	Pilot	Pentium II	Pager	Pilot	Pentium II
RSA key generation	580,405	1,705,442	2,740.87	—	—	26,442.04
RSA encrypt ($e = 3$)	533	1,023	2.70	1,586	3,431	7.26
RSA encrypt ($e = 17$)	683	1,349	3.23	2,075	4,551	9.09
RSA encrypt ($e = 2^{16} + 1$)	1,241	2,670	5.34	4,142	8,996	16.57
RSA decrypt	15,901	36,284	67.32	112,091	292,041	440.78
RSA signing	15,889	36,130	66.56	111,956	288,236	440.69
RSA verifying ($e = 3$)	301	729	1.23	1,087	2,392	4.20
RSA verifying ($e = 17$)	445	1,058	1.76	1,585	3,510	6.10
RSA verifying ($e = 2^{16} + 1$)	1,008	2,374	3.86	3,608	7,973	13.45

Table 7: Timings (in milliseconds) for 1024-bit and 2048-bit RSA operations on various platforms.

¹ M. Brown, D. Cheung, D. Hankerson, J. Hernandez, M. Kirkup, and A. Menezes, “PGP in Constrained Wireless Devices,” Proc. 9th USENIX Security Symposium, Denver, CO, Aug. 2000, http://www.usenix.org/publications/library/proceedings/sec2000/full_papers/brown/brown.pdf

DSA and El-Gamal in Constrained Wireless Devices

	512-bit modulus			768-bit modulus			1024-bit modulus		
	Pager	Pilot	PII	Pager	Pilot	PII	Pager	Pilot	PII
ElGamal key gen	—	—	51,704	—	—	219,820	—	—	1,200,157
ElGamal encrypt	7,341	17,338	19.13	16,078	34,904	35.91	26,588	73,978	67.78
ElGamal decrypt	8,704	19,060	22.55	26,958	56,708	59.53	57,248	148,059	144.73
DSA key gen	—	—	3,431	—	—	14,735	—	—	54,674
DSA signing	2,955	6,329	7.53	6,031	11,875	15.55	9,529	25,525	24.28
DSA verifying	5,531	12,389	14.31	11,594	24,277	26.13	18,566	52,286	47.23

Table 8: Timings (in milliseconds) for DL operations on various platforms.

Elliptic Curve Cryptosystems in Constrained Wireless Devices

	Koblitz curve over $F_{2^{163}}$			Random curve over $F_{2^{163}}$		
	RIM pager	PalmPilot	Pentium II	RIM pager	PalmPilot	Pentium II
Key generation	751	1,334	1.47	1,085	1,891	2.12
ECAES encrypt	1,759	2,928	4.37	3,132	5,458	6.67
ECAES decrypt	1,065	1,610	2.85	2,114	3,564	4.69
ECDSA signing	1,011	1,793	2.11	1,335	2,230	2.64
ECDSA verifying	1,826	3,263	4.09	3,243	5,370	6.46

Table 3: Timings (in milliseconds) for ECC operations over $F_{2^{163}}$ on various platforms.

	Koblitz curve over $F_{2^{233}}$			Random curve over $F_{2^{233}}$		
	RIM pager	PalmPilot	Pentium II	RIM pager	PalmPilot	Pentium II
Key generation	1,552	2,573	3.11	2,478	3,948	4.58
ECAES encrypt	3,475	5,563	7.83	6,914	11,373	13.99
ECAES decrypt	2,000	2,969	4.85	4,593	7,551	9.55
ECDSA signing	1,910	3,080	4.03	3,066	4,407	5.52
ECDSA verifying	3,701	5,878	7.87	7,321	11,964	14.08

Table 4: Timings (in milliseconds) for ECC operations over $F_{2^{233}}$ on various platforms.

DEVELOPING A BUSINESS CASE FOR A MOBILE DEVICE SUCH AS A PDA

In assessing various wireless PED devices, the following criteria for the platform were taken into account:

- Mobile and tetherless (some form of wireless appliqué)
- Small Size, Weight and Power (SWAP) (the medical personnel can carry it with them)
- Reasonable Cost
- Identification and authentication (biometric-enabled)

Based on these and other criteria, the HP iPAQ Pocket PC h5550² was found to be the most suitable candidate.

The HP iPAQ Pocket PC h5550 has a processing speed of 400 MHz, 64 MB of RAM with 48 MB of Flash. In addition, it includes a wireless package (GSM, GPRS) and a biometric capability. Additional features of the HP iPAQ Pocket PC h5550 include:

- Microsoft® Windows® Mobile™ 2003 software
- Integrated Wireless LAN 802.11b
- Integrated Bluetooth™
- Integrated Biometric Fingerprint Reader
- Removable/Rechargeable Battery



² Source: <http://h10010.www1.hp.com/wwpc/us/en/en/WF05a/215348-64929-215381-314903-f44-322916.html>

- Integrated Secure Digital slot
- Intel® XScale processor
- Increased memory
- Advanced Power Management

Information-Centric Cryptography and Key Management

The TecSec team in Phase I has investigated the following:

- The feasible utility of a hardware cryptographic platform such as Field Programmable Gate Array (FPGA)
- Key management and the use of cryptography in assuring confidentiality, integrity, and availability (CIA) in the commercial healthcare and medical arena

CRYPTOGRAPHIC CORES

The GMU team, led by Dr. Kris Gaj, has been very active in research and development regarding the efficient implementations of cryptographic transformations using FPGA technology since 1998 [reference to major GMU publications]. During this period, a comprehensive library of hardware cryptographic cores targeted at the major families of FPGA devices has been developed. This library covers several major classes of cryptographic transformations, including:

- Secret-key ciphers (Advanced Encryption Standards (AES), Triple DES, Serpent, Twofish, RC6, and Mars) for bulk data encryption
- Cryptographic hash functions (SHA-1 and SHA-512) and Message Authentication Codes (HMAC) for message authentication
- Public-key ciphers (two major groups of Elliptic Curve Cryptosystems), for key distribution and non-repudiation based on digital signatures

Each of the secret-key ciphers included in our library has been implemented using four different architectures suitable for different classes of applications and environments, including:

- Compact architecture for wireless communication and portable devices
- Iterative architecture for low-cost hardware accelerators for individual workstations and servers
- Inner-round pipelined architecture for the gigabit-rate security gateways for Internet Protocol Security (IPSec) and Secure Socket Layer (SSL)
- Fully pipelined architecture, suitable for cryptographic accelerators for satellite communications, high-speed terrestrial computer networks and high-volume secure storage

These architectures offer various trade-offs among speed, area, and power consumption. The distinctive features of our cryptographic modules include:

- Support for multiple key sizes and modes of operation
- Very high encryption in decryption throughputs (in excess of 16 gigabits per second (Gbps) for AES)
- Efficient use of circuit area (the best throughput to area ratio reported in the literature for all five final AES candidates)
- Universal and simple external interface

The GMU implementations of cryptographic transformations for encryption and message authentication support most recent federal standards approved by NIST in 2002. For example, our implementation of HMAC and SHA-512, offers security exceeding by many orders of magnitude the security of old standards, such as Chain Block cipher (CBC)-MAC and SHA-1. In GMU implementations, these more

secure algorithms are also significantly faster (up to 1 Gbps using current generation of FPGAs) than the old standards, which are in common use today.

Our implementations of public key transformations include compact and fast implementations of two families of Elliptic Curve Cryptosystems (over $GF(2^n)$ in polynomial basis and optimal normal basis). Because of the small area and power consumption, these implementations are particularly suitable for key exchange and signature generation in wireless networks and portable devices.

CRYPTOGRAPHY

Progress in the heuristic methods of designing computationally secure cryptographic algorithms, such as secret-key ciphers, led to the design of a large group of algorithms with the estimated level of security considered as sufficient for both military and the most demanding commercial applications. When security itself is no longer a factor that clearly favors one algorithm over the other, efficiency in software and hardware becomes a major indication of the quality of an algorithm. The importance of this requirement was clearly demonstrated during the recent contest for the Advanced Encryption Standard (AES), when ranking of the algorithms by cryptographic community and NIST was based, to a large extent, on implementation efficiency and flexibility.

The growing demand for security in both military and commercial applications, combined with the need for interoperability often requires that the same cryptographic transformation is to be implemented on a large variety of platforms, covering a broad spectrum from low-cost 8-bit microprocessors to high-performance custom Application-Specific Integrated Circuits (ASICs). Designing a cryptographic transformation that behaves uniformly well across all these platforms is an extremely challenging task that is still an open research problem. Additionally, because of the long lifetime of cryptographic algorithms and standards it is difficult to predict the detailed characteristics of future software and hardware platforms on which a given cryptoalgorithm is going to be implemented.

Two primary parameters describing the efficiency of the cryptographic device are throughput and latency. Throughput determines the amount of data encrypted in a unit of time. Latency determines time necessary to complete encryption of a single block of data. In applications where the large amounts of data are encrypted or decrypted, throughput determines the total encryption/decryption time, and thus is the best measure of the system speed. Latency becomes important in applications where the response time of the system is of primary concern.

Hardware implementations of cryptography can significantly improve both throughput and latency compared to software implementations. This speed-up can be accomplished primarily by making full use of parallel processing and pipelining, and by operating on arbitrary size words. In particular, a significant increase in the speed of cryptographic transformations can be achieved in hardware by using pipelining. It was shown that the throughput of AES candidates can increase by up to two orders of magnitude by applying mixed inner- and outer-round pipelining, and can reach throughputs in the order of 15 Gbps using commercially available FPGA devices. Nevertheless, several conditions must be fulfilled to take advantage of such significant speed-ups. All atomic operations must be decomposable into a sequence of simpler operations, to be implemented using combinational units separated by pipeline registers. The area required by each atomic operation must be small enough, so that multiple repetitions of the same operation are possible within the limits imposed by the integrated circuit area. Additionally, an internal structure of the cryptographic transformation cannot include feedback loops preventing pipelining. For example, standard feedback modes of block ciphers, such as Cipher Block Chaining (CBC), Cipher Feedback (CFB) and Output Feedback (OFB), prevent using pipelining during encryption, because the next block of data cannot be processed before the previous block is fully encrypted.

CONSTRUCTIVE KEY MANAGEMENT (CKM) WITH STRONG AUTHENTICATION

It is essential for system operators to recognize that while cryptography is an important component of protecting their system, it is only one tool from a much larger set. Cryptography is only effective if it is deployed as part of a comprehensive set of security policies, and when it is combined with adequate attention to physical security.

Key management is a critical component of the solution set needed for system integration and operation. Key management schemes must be capable of controlling the distribution, use and update of cryptographic keys.

Constructive Key Management (CKM), which is specified in ANSI X9.69, systemizes key creation, implementing dual control or split knowledge by using key components to construct the final working key. This working key may be used in several ways including a session key, for a store-and-forward application such as e-mail, and for file encryption applications such as archiving, or protecting file information until accessed by a user. Other applications are possible.

The practice of split knowledge key creation has been used mainly to transport key parts into systems where master keys were used to protect keys in storage, and to recover the working keys for a current application. With this methodology, a working key will be created as needed for a specific encryption process, and re-created when needed to decrypt the object. Depending on the application, the key may be saved or destroyed after each use. The working key is never transmitted; the application program only knows it when it is in use.

Certainly, any solution based on secret-key cryptography has an advantage in terms of implementation efficiency. On the other hand, they may not be resistant to a special node compromise, and may lack in terms of multiple flexibility criteria, including scalability.

An approach to provide security in a distributed, decentralized system often involves services that can perform non-repudiation with a high degree of confidence. Typically, this prescribes a Public Key Infrastructure (PKI), which effects authentication, identity, non-repudiation, privacy and confidentiality. Many systems have deployed PKI as an architectural component to extend an existing directory so that the entities in the directory have public and private key attributes as well as certificates. In a large-scale deployment, many have preferred the use of role-based access control technology.

The role of PKI is for authentication, whereas CKM fills the role of authorization. Both will be working on the trusted platform, which in this case is the PDA.

Next Steps

The next steps for a Phase II effort are outlined in more detail in the Phase II 5-page report and include the following elements:

NEAR TERM: PHASE I OPTION

We recommend that the STTR Phase I option be exercised for the following expressed reasons. The TecSec team has established medical and healthcare use cases for potential medical and healthcare customers include the Veterans Administration, Centers for of Medicaid and Medical Services, Military Health Services, and others. We would like to further definitize and validate the requirements and try to establish a customer base for Phase II co-sponsorship. We propose that the STTR Phase I results be briefed to these customers to alert them of the utilities of an information-centric security solution that provides role based access control using an efficient key management scheme on a widely adopted PED platform by the medical personnel.

The Phase I option will involve the generation of a test and demonstration plan on the medical and healthcare use cases. It is also proposed that the purchase of the PDA devices (i.e., HP iPAQ h5550) be made for initial assessment and evaluation.

In order to avail the information-centric security solution with key management for protecting data at rest and in transit in a plethora of applications, this might involve the segregation and hosting of the solution on a module which is then connected to the hosted PED platform. An area of research will include the preliminary assessment and evaluation of design alternatives to tradeoff the embedded versus modular design.

MID TERM: PHASE II

Under Phase II, we would aim for the following objectives:

- The implementation of the asymmetric information-centric security solution in the selected PDA to avail information assurance in the areas of confidentiality, integrity and availability. This design could be integrated into other mobile platforms.
- Recognizing that the mobile environment often is wireless and tetherless, the design could include a modular instantiation of the embedded design as discussed above. This would require an air interface in connecting the then stand-alone encryption module to the host platform.
- The validation of the trust model to provide different levels of trust architectures between domains. Key sharing would involve parameters on what to share, how to share, and when to share
- Demonstrate through the prototype hardware implementation that the design could be applied to Navy and commercial medical services.

Our goal is to make our solution portable across multiple platforms and operating systems. Any medium cost PDA with a predefined interface and communication capabilities may be adapted for use in our system. Our software and hardware token will work efficiently with any PDA platform fulfilling some well defined minimum requirements, such as clock speed, memory size, interface type, and communication module.

LONG TERM: PHASE III/COMMERCIALIZATION PHASE

Our objective is to implement and deploy widely and pervasively.

Appendix A - Overview of the Trust Model

The trust model describes the basic security relationships between the domains in an ad-hoc networked environment. At the domain level we use a model with one domain as a reference. We view all other domains in relation to this single domain. This allows us to describe the trust relations between any domain and all other domains in an ad-hoc networked environment.

We only distinguish between three different basic trust levels:

Untrusted Domain

Untrusted domains are by definition all networked domains that the reference domain has no security relations with and that it has not (yet) been able to identify and/or verify the identity of. For example, any new domain that a user belongs to is an untrusted domain from the perspective of all the other domains to which the user belongs.

Second Party Domain

A second party domain has an owner different to that of the reference domain. Second party domain identities can be verified, i.e., authenticated. It is also possible to make a secure key exchange with a second party domain. A second party domain might be trusted for some actions while still be untrusted for other actions. The fine grain level of trust given to a particular second party domain is determined by the security policy of the reference domain and is part of the service level trust model.

First Party Domain

A first party domain has the same owner as the reference domain. Furthermore, all first party domains are able to identify all other first party domains and distinguish a first party domain from a second party domain or untrusted domain. It is possible to make a secure authenticated key exchange with a first party domain without any manual user interaction.

Domain Initialization

A prerequisite for secure communication and authentication of domains is a common security association. A security association can either be a shared secret or shared public key root key(s). The creation of a security association, i.e., generation or transfer of key(s), we call "domain initialization". The cryptographic initialization is a procedure of equipping the domain with a secret value of a cryptographic parameter. This procedure, where the initial secret cryptographic parameters are set in the domain, is the most sensitive part of the communication.