REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

The public reporting burden for this 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 suggesstions 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 any oenalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
	Technical Report	-

4. TITLE AND SUBTITLE
Self-Protecting Security for Assured Information Sharing (2013 Progress Report)

5a. CONTRACT NUMBER
W911NF-12-1-0081

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
206022

6. AUTHORS
George Hsieh

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Norfolk State University
700 Park Avenue

Norfolk, VA 23504 -8060

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

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

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
60475-CS-REP.19

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

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
The main objective of this project is to research, design, and prototype the integrated, secure, embedded, and fine-grained security frameworks that can be used to provide self-protecting security for assured information sharing applications. These frameworks extend and use a variety of open standards, including eXensible Access Control Markup Language, XML Encryption, and XML Signature, in an integrated manner such that the access control policies, encrypted data, and digital signatures are all embedded and secured with the digital content to be protected. In addition, these security mechanisms are applied in a fine-grained manner such that different parts of

15. SUBJECT TERMS
Information security, self-protecting security, XML Security

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chung-Chu (George) Hsieh
UU	UU	UU	UU		19b. TELEPHONE NUMBER 757-823-8313

Report Title

Self-Protecting Security for Assured Information Sharing (2013 Progress Report)

ABSTRACT

The main objective of this project is to research, design, and prototype the integrated, secure, embedded, and fine-grained security frameworks that can be used to provide self-protecting security for assured information sharing applications. These frameworks extend and use a variety of open standards, including eXensible Access Control Markup Language, XML Encryption, and XML Signature, in an integrated manner such that the access control policies, encrypted data, and digital signatures are all embedded and secured with the digital content to be protected. In addition, these security mechanisms are applied in a fine-grained manner such that different parts of the digital content can be protected using different access control policies or encryption algorithms/keys.

We are extending our general-purpose self-protecting security framework, which can be used to protect digital content of any type or format, by adding support for data governance and publish-subscribe service. We are also extending our domain-specific framework for protecting electronic medical records by integrating advanced cryptographic schemes, such as attribute-based encryption and privacy-preserving keyword search capabilities, for patient-controlled and cloud-based personal health record applications.

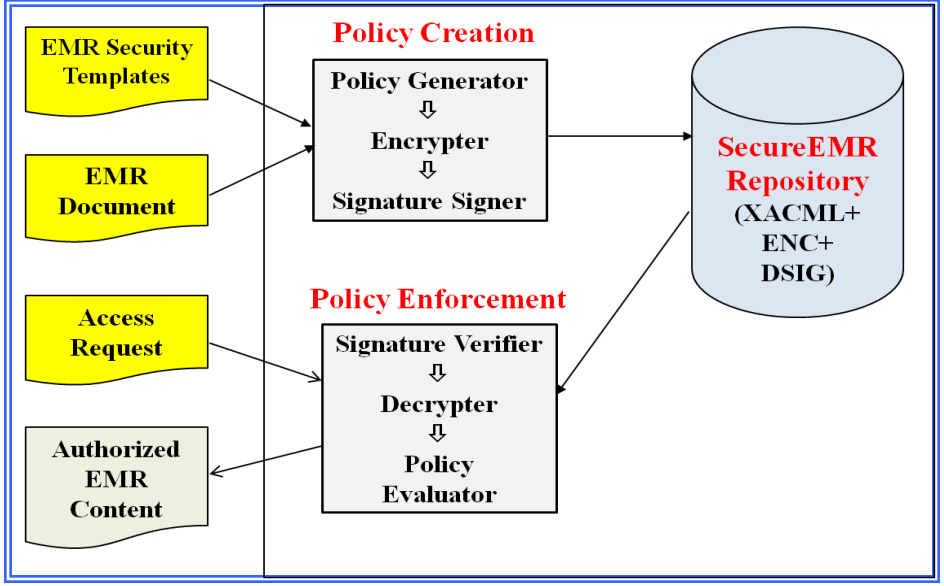
Self-Protecting Security Framework for Assured Information Sharing

George Hsieh, Norfolk State University
Tel. (757) 823-8313, E-Mail: ghsieh@nsu.edu

Objective:

Design and develop secure, integrated, embedded, and fine-grained security frameworks for Assured Information Sharing applications:

- ❑ Design a new domain-specific framework for protecting electronic medical records
- ❑ Extend frameworks to support secure data governance and publish-subscribe interaction
- ❑Incorporate new policy-driven security capabilities
- ❑Develop and enhance prototype software systems



Scientific/Technical Approach:

Extend and integrate XML based security standards to provide self-protecting security:

- ❑ Embedding - Content and security related information embedded in a single data object
- ❑ Fine-grained - Different parts of content can be protected with different rules, crypto keys, etc.
- ❑ Open standards - XACML for access control, XML Encryption for confidentiality, XML Signature for integrity

Enable lifetime protection no matter where data resides.

Accomplishments/Highlights (FY13):

- ❑ Completed Version 1 prototype software system for EMR self-protecting security framework
- ❑ Proposed a design for a cloud-based personal health record service using the security framework and advanced cryptographic schemes
- ❑ Published 5 peer-reviewed papers; supported 2 students; engaged 9 students in related research

Next Steps for Research:

- ❑ Continue with work on data governance and publish-subscribe
- ❑ Integrate advanced crypto schemes into prototype