The Office of the National Coordinator for
Health Information Technology

Health Information Technology Security Pilot

May 10, 2011

presented by

Dr. Roxanne B. Everetts

Under contract to ONC

Agenda

- Introductions
- Background
- Project Goal and Objectives
- Approach
- Impact

Introductions

- Office of the National Coordinator for Health IT
  - Deborah Lafky, MSIS, Ph.D., CISSP

    HIT Security Pilot Program Manager
    Program Officer: Security | Cybersecurity
    Office of the Chief Privacy Officer
    Office of the National Coordinator for Health IT
    Department of Health and Human Services
  - Roxanne B. Everetts, DM, CISSP, CISM, CBCP

    Information Assurance Research Fellow, LMI

    HIT Security Pilot Project Lead
- National Institute of Standards and Technology
  - Matthew Smith

    G2, Inc

Background

- Initiative from HIT Cyber Working Group
  - Examine practical methods for improving security of health IT
  - Reduce security burden on end user
- Providers and patients must be confident that the electronic health IT products and systems they use are secure
- Several barriers to successful adoption of end user security measures
  - Lack of usability
  - High complexity
  - Misinformation
  - User awareness

Project Goal and Objectives

- Goal:
  - Develop and pilot test one or more methods of end to end automated security in healthcare settings
    - Identify and test practical steps to improve the security of PHI
    - Remove a significant barrier to the success of EHR
    - Increase Electronic Health Record (EHR) adoption
- Objectives:
  - Remove security as a barrier to EHR adoption
  - Identify methods to improve security of EHR products
  - Examine impact of diversity of configurations in HIT ecosystem
  - Ensure that securing PHI be transparent to end users
  - Gather information about how EHR products can improve security posture
  - Leverage investment in EHR security research across agencies/departments

NIST and ONC Collaboration

- **Close collaboration with NIST**
  - NIST and ONC staff meet regularly
    - Ensure LMI and NIST are in sync as projects develop
  - NIST is conducting two projects for HHS on related topics
    - Automated HIPAA Security Rule toolkit
    - Developing secure HIT Ecosystem templates for use in testing

The Office of the National Coordinator for
Health Information Technology

NIST

Health IT
Security Content Automation

Matthew Smith, G2 Inc.

Under contract to NIST

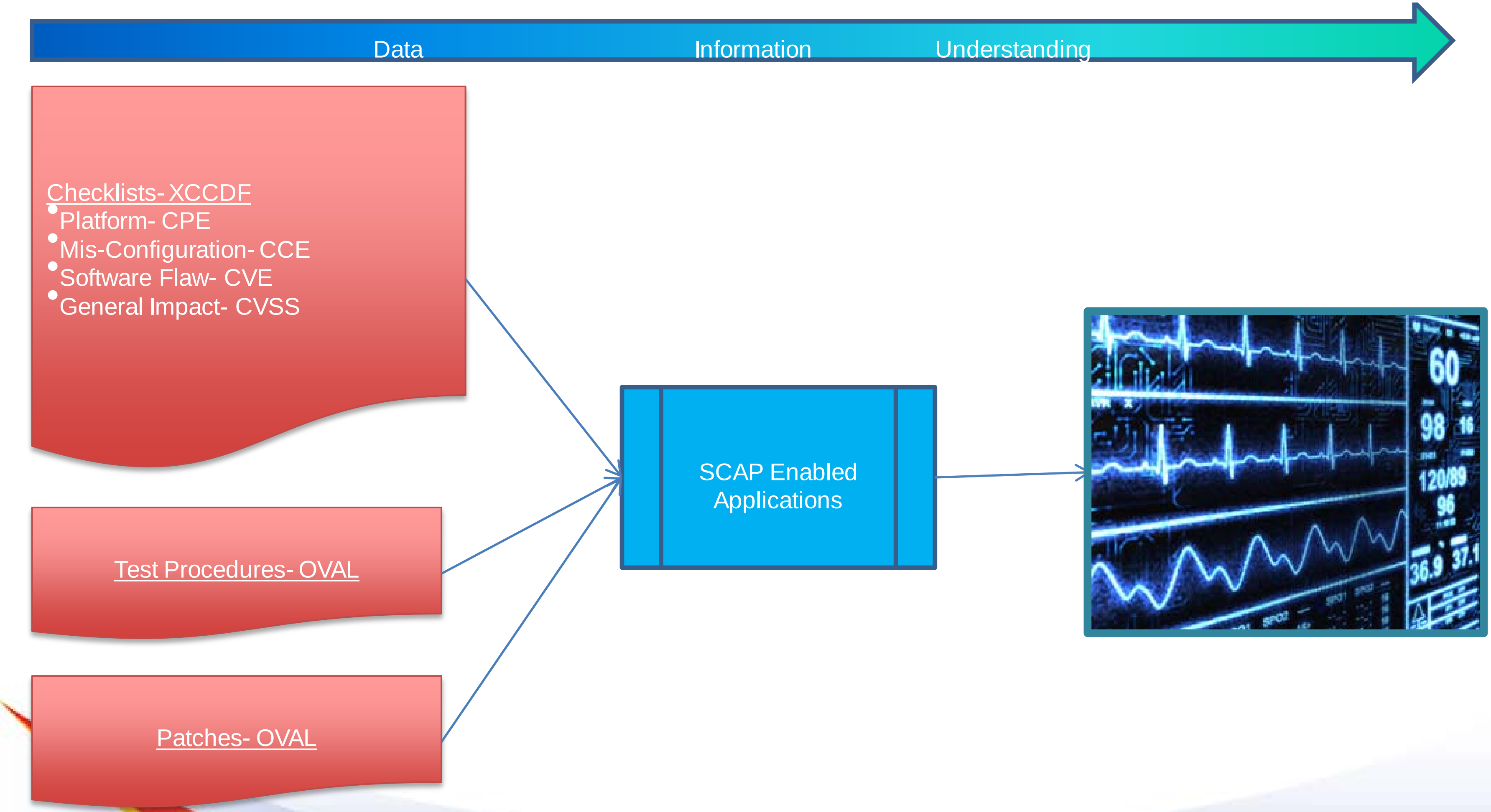
Context

- Working Groups
  - Important progress being made at multiple levels
    - Thanks to all the groups for their work
- Implementation
  - What needs to be accomplished?
    - Data Security
    - Compliance with Rules, Law
  - What technologies could we use to automate checking?
  - What types of processes and languages could we use?
  - SCAP

How does SCAP fit into Health IT?

- Enabling Data Security and Compliance Checking through:
  - Asking the computer questions
    - Scanners produce automated responses
  - Asking humans questions
    - HIPAA Security Rule Toolkit - NIST/Exeter Presentation on Wednesday Afternoon
  - Creating software profiles and virtual images of health care configurations
    - Recreation of the actual environment in lab setting
    - Quality Assurance
  - Dashboarding - How am I doing?

How SCAP Works



Data Information Understanding

Checklists- XCCDF

- Platform- CPE
- Mis-Configuration- CCE
- Software Flaw- CVE
- General Impact- CVSS

Test Procedures- OVAL

Patches- OVAL

SCAP Enabled Applications

Security Content Automation Protocol (SCAP)

Standardizing How We Communicate

NIST

MITRE	CVE cve.mitre.org	CVE	Common Vulnerabilities and Exposures	Standard nomenclature and dictionary of security related software flaws
MITRE	CCE™	CCE	Common Configuration Enumeration	Standard nomenclature and dictionary of software mis-configurations
MITRE	CPE™ common platform enumeration	CPE	Common Platform Enumeration	Standard nomenclature and dictionary for product naming
National Security Agency United States of America	XCCDF security benchmark automation	XCCDF	eXtensible Checklist Configuration Description Format	Standard XML for specifying checklists and for reporting results of checklist evaluation
MITRE	OVAL™ Open Vulnerability and Assessment Language	OVAL	Open Vulnerability and Assessment Language	Standard XML for test procedures
FIRST Improving Security Together Cisco, Qualys, Symantec, Carnegie Mellon University	cvss	CVSS	Common Vulnerability Scoring System	Standard for measuring the severity of vulnerabilities

Reference: NIST Special Publication 800-126

Current Project Deliverables

- Develop baseline HIPAA Security Rule (HSR) Security configuration checklists for common HIT platforms
  - Value: Enables quicker HSR compliance checking
- Create a virtual test environment to confirm checklists are operating correctly
  - Value: simulate medical environment to provide highest quality
- These deliverables will be used as input to larger test framework that our partners at NIST and LMI are building
  - Value: seamless integrated testing for the broader HIT space

Next steps

- Eliminate the overlap caused by multiple compliance rules asking the same security questions
  - Minimize time that you, the health professionals, are not caring for patients
  - Achieve compliance in a quicker fashion
- Leverage lessons learned from Defense and Intel spaces

Project Approach

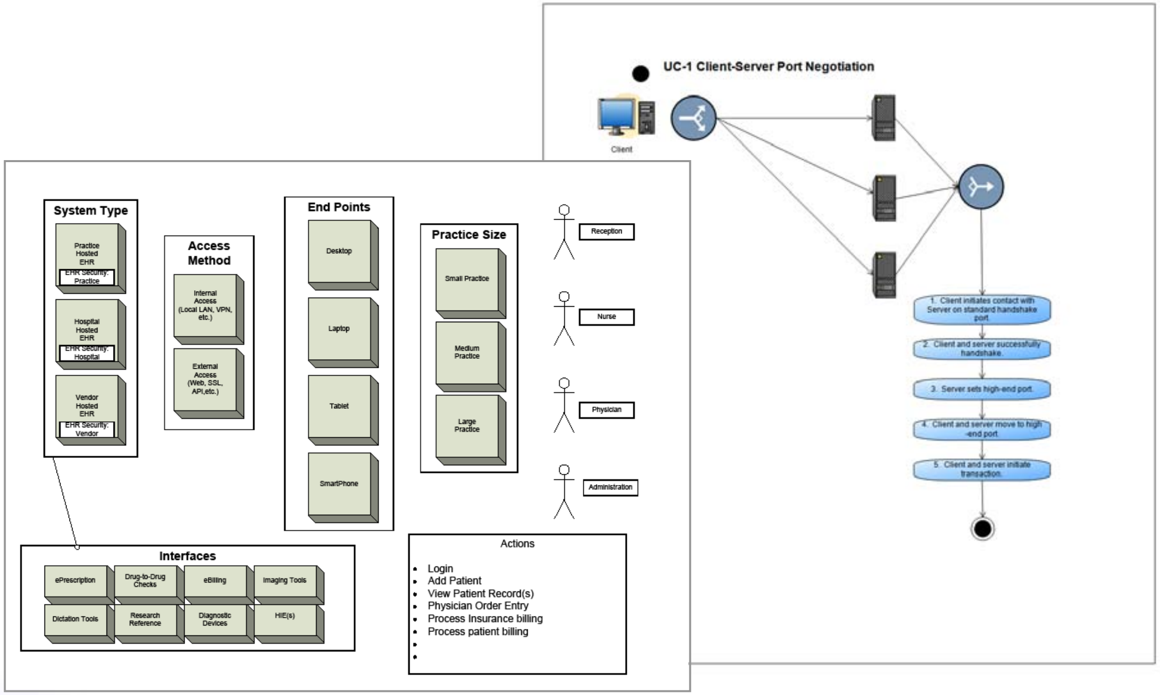
- Phase 1: Research and Establish Test Bed
- Phase 2: Test and Evaluation
- Phase 3: Reporting

Phase 1: Research and Establish Test Bed

- Identify emerging technologies and methods to protect healthcare information
  - Leverage research by ONC, as well as research by industry and technology partners
- Perform market survey
  - Identify EHRs (complete and module) as prospective technologies for test bed
  - Collaborate with HITRC

Phase 1: Research and Establish Test Bed —continued

- Develop and validate use cases that accurately reflect HIT ecosystem



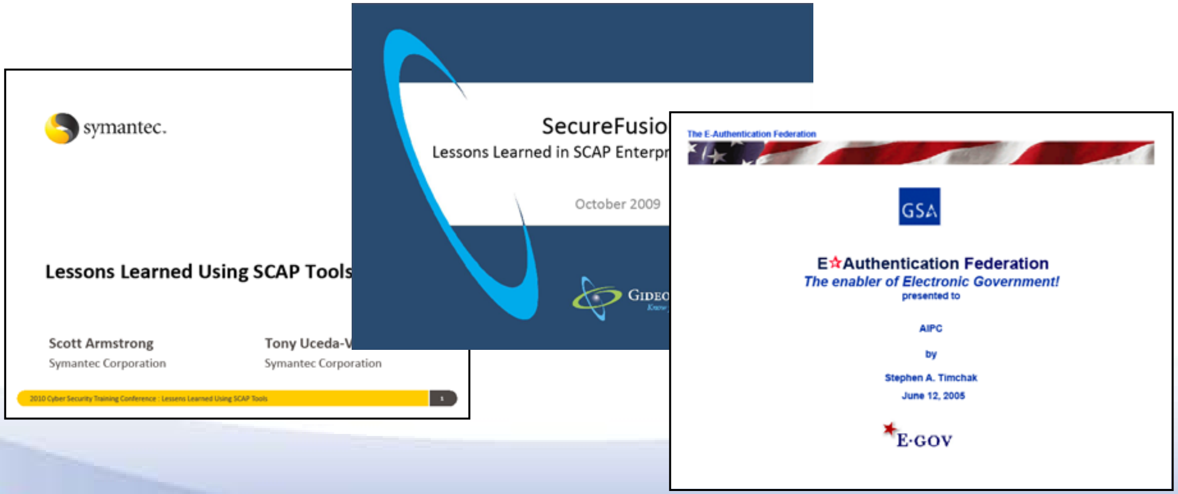
1. Client initiates contact with Server on standard handshake port.
2. Client and server successfully handshake.
3. Server sets high-end port.
4. Client and server move to high -end port.
5. Client and server initiate transaction.

Actions

- Login
- Add Patient
- View Patient Record(s)
- Physician Order Entry
- Process Insurance billing
- Process patient billing
-
-

Phase 1: Research and Establish Test Bed —continued

- Gather and analyze lessons learned from the other initiatives to identify information security tools for end users.
  - e.g., SCAP, E-Authentication, and ICAM initiatives



symantec.

Lessons Learned Using SCAP Tools

Scott Armstrong
Symantec Corporation

Tony Uceda-V
Symantec Corporation

2010 Cyber Security Training Conference : Lessons Learned Using SCAP Tools 1

SecureFusio
Lessons Learned in SCAP Enterpr

October 2009

GIDEO

The E-Authentication Federation

GSA

E☆Authentication Federation
The enabler of Electronic Government!
presented to

AIPC

by

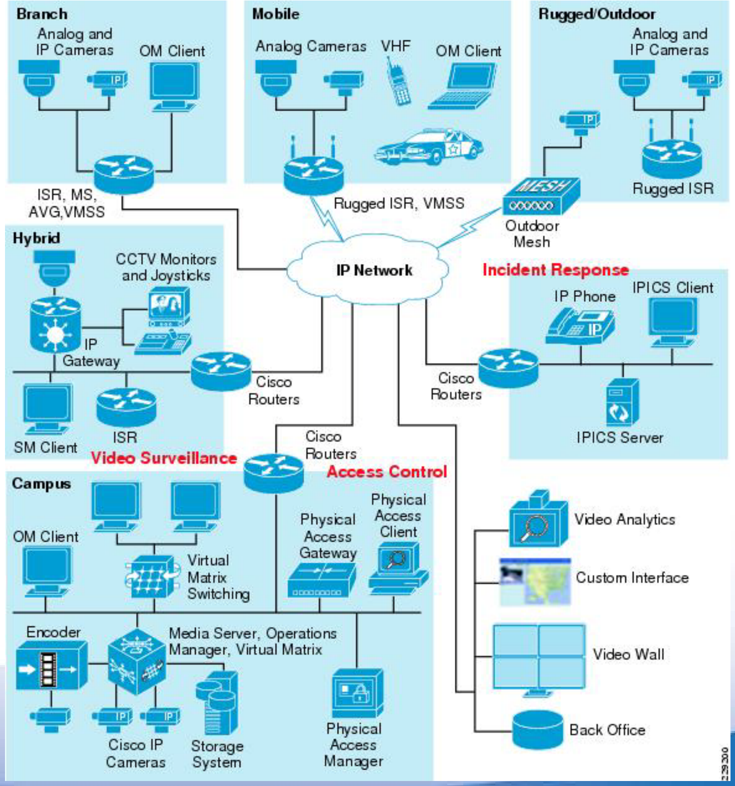
Stephen A. Timchak
June 12, 2005

E·GOV

Phase 1: Research and Establish Test Bed—continued

- Establish a scalable health IT test bed
  - Model a realistic representative HIT ecosystem
    - Multiple architectures
  - Provide for multiple different settings
    - including physician offices, hospital nursing stations, emergency departments, and others

- Develop and execute unbiased, comprehensive, and thorough proof-of-concept pilot tests



Phase 2: Test and Evaluation

- Work closely with subject matter experts, government and industry partners to confirm the approach and identify roles and responsibilities
  - ONC
  - NIST
  - OCR
  - HIT Cyber Working Group (NSS, VA, SSA, DoD, FCC)
- Coordination with test partners, such as vendors and RECs
- Establish test development teams to develop test data, test scripts, and expected results
- Prepare test materials (including the test plan)

Phase 2: Test and Evaluation—continued

- Use auto-validation tools to compare test cycle outputs
- Validate collected outputs against industry best practices
- Document the test environment configuration
- Assess compliance with tested requirements
- Verify and document results

Security Pilot Criteria

- Selection Criteria for prospective EHR Candidates
  - Must be an ONC Certified Complete EHR Solution
    - Eliminates need to validate solution functionality
  - Must be a primary care EHR
    - Reflects ONC focus
    - Reduces pool
  - Vendor size
    - Number of employee
    - Number of complete implementations
  - Software implementations
    - Reported by vendors and RECs
  - Geographic distribution of implementations
  - Costs

Major Challenges

- EHRs are evolving
  - Functional and technical vectors are often divergent
- EHRs implemented across a broad spectrum of technologies
  - Very old technologies are still in use
- Emerging federal guidance and statutory regulations and standards
  - ACO
  - CMS
- ONC Privacy and Security FACAs developing policy and standards
- Moving from “Meaningful Use” Stage 1 to Stage 2
  - As additional stages are implemented, need to ensure whatever standards established do not create conflict

Impact

- Improve quality of care and patient safety
- Facilitate EHR adoption
- Reduce security risk/burden on end users (medical professionals)
- Allow medical professionals to focus on patient care (and not IT security)
- Identify methods for EHR vendors to improve/simplify product security

For further information…

- ONC:
  - HHS ONC.Security@HHS.gov
- NIST:
  - kevin.stine@nist.gov