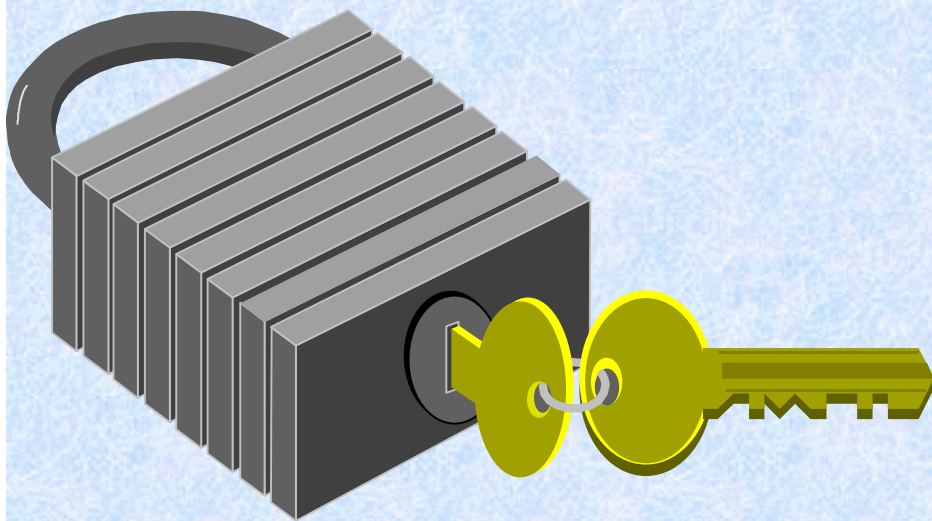


Security Compliance: Making the Proper Decisions

L. Arnold Johnson

National Information Assurance Partnership
National Institute of Standards and Technology



Short Answer to Moderators Questions

- **Advice Now:** Use IT hardware/software/network/plan security tools to detect & block further damage
- **Advice Before:** Perform IT system security accreditation/certification/validation analysis
- **Standards of Care:** Demonstrate adherence to International/National/Industry IT security Standards/Practices/Policies through recognized Accreditation/Certification/Validation sources
- **HIPAA Effect:** Need to show documented, traceable evidence of HIPAA compliance through requirements definition, analysis, technology selection, product & system evaluation/validation by recognized sources

The Healthcare Security Dilemma

How can the healthcare community satisfactorily demonstrate that its information technology systems are in compliance with policy (HIPAA, HCFA, etc.)?



The Dilemma is multifaceted.

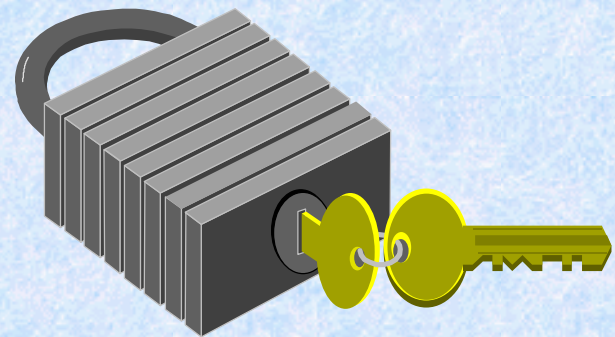
How do we:

- capture needs and concerns in implementable policy?
- translate policy into technology?
- confirm technology complies with policy ?

Security Requirements

Compliance with what???

- Healthcare IT security architecture(s)
 - operational environment
 - functional needs
 - security objectives
- Policy
 - public law
 - federal, state, local, organizational policy
 - standards
 - regulations
 - *et al*



Basic Healthcare IT Security Problem

- Lack of a common language to bridge the communication gap among HC security policy makers, standards organizations, consumers and developers
- Lack of a common structure for expressing HC security requirements and assurance
- Lack of accredited labs & recognized sources for
 - evaluating the security properties of HC products
 - validating product & system compliance

Is there an industry-recognized methodology or mechanism to bring some coherence to this problem ?

The ***Common Criteria***

a promising, and accepted, solution

- International Standard (**ISO/IEC 15408**)
- Practical way to specify and measure IT security
 - capture users' functional and assurance requirements
 - translate policy into product/system specifications
 - guide product/system development
 - evaluate products/systems
- Flexible and adaptable to healthcare needs

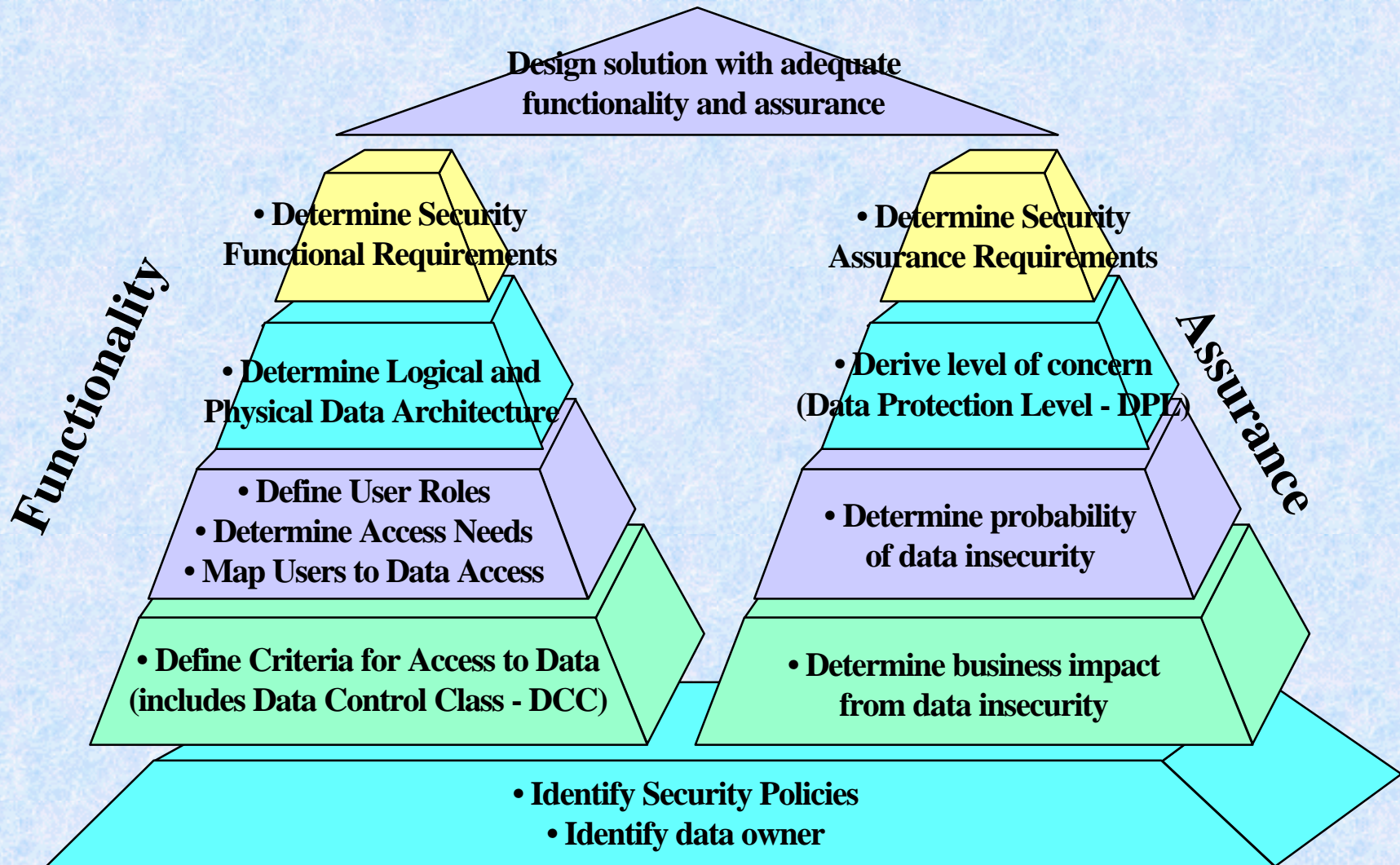
Standard for Defining Security Requirements

- **Common Criteria** (CC), a.k.a. ISO/IEC International Standard 15408, provides a framework for defining security requirements (both features and assurances) in IT products
- **CC Protection Profiles** (PP) describe generalized security requirements for a class of IT products (from consumers perspective), e.g., banking, healthcare
- **CC Security Targets** (ST) describe specific security claims by producers of IT products

Kinds of Requirements

- Functional Requirements
 - **for defining security behavior**
 - **implemented requirements become security functions**
- Assurance Requirements
 - **for establishing confidence in security functions**
 - **correctness of implementation**
 - **effectiveness in satisfying objectives**

Defining Security Requirements



Protection Profiles

Moving Toward Compliance

- Consumers specify generalized requirements in PP(s)
 - Implementation-independent
 - States security problem to be solved
 - Specifies functional and assurance requirements
 - Can be adopted, tailored or developed for healthcare
- Developers/vendors build specific products to satisfy PP(s)
 - To satisfy customer demand
 - For competitive advantage
 - To define market expectations

Protection Profiles (generic) & Security Targets (specific)

Consumer

Protection Profile contents

- Introduction
- TOE Description
- Security Environment
 - Assumptions
 - Threats
 - Organizational Security Policies
- Security Objectives
- Security Requirements
 - Functional Req'ts
 - Assurance Req'ts
- Rationale

Developer/Vendor

Security Target contents

- Introduction
- TOE Description
- Security Environment
 - Assumptions
 - Threats
 - Organizational Security Policies
- Security Objectives
- Security Requirements
 - Functional Req'ts
 - Assurance Req'ts
- *TOE Summary Specification*
- *PP Claims*
- Rationale

Benefits of using the Common Criteria

- A common language for specifying security functional & assurance requirements
- A comprehensive catalogue of security requirements that
 - can be mixed/matched, extended & refined
 - can specify a product or class of products/systems

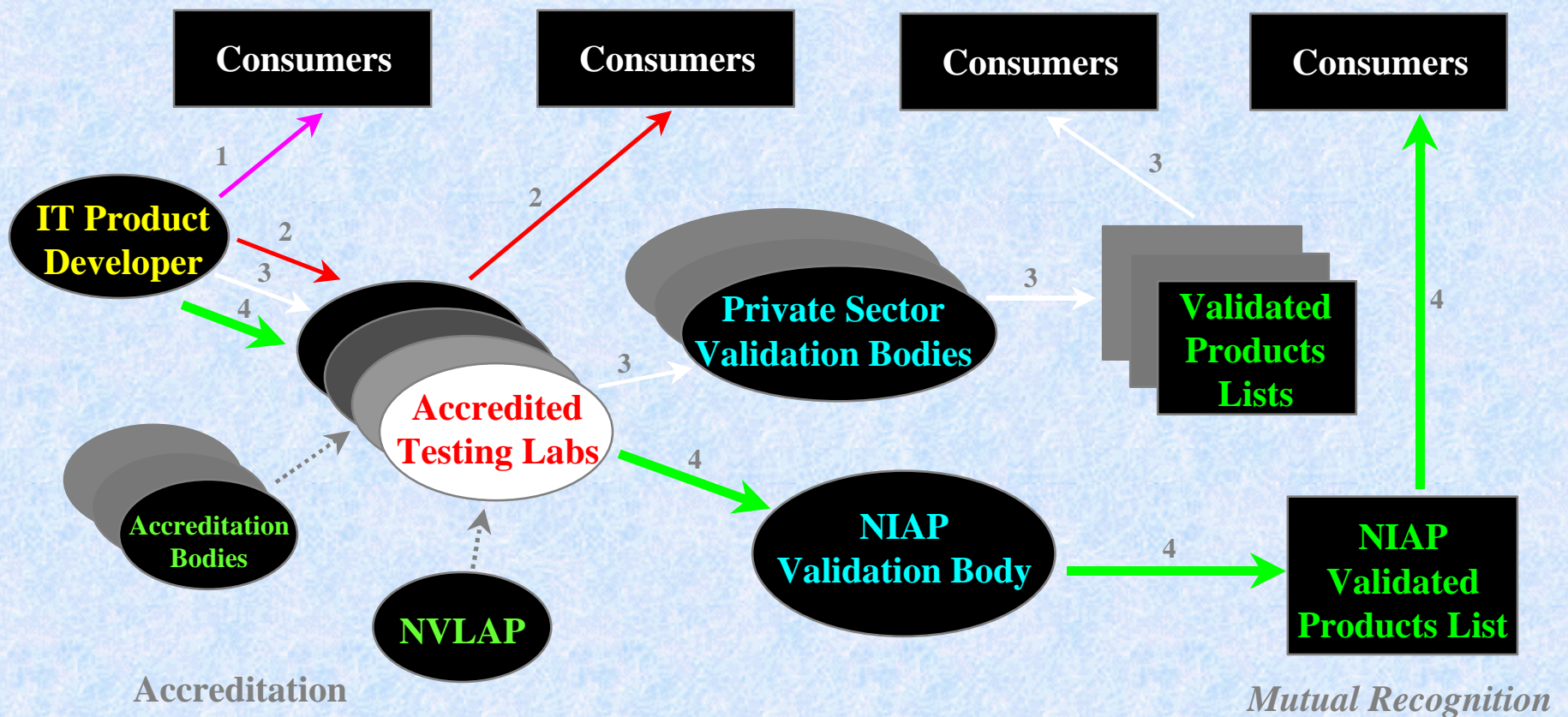
Benefits of using Protection Profiles

- Standard framework for capturing
 - government & social policies & regulations
 - enterprise specific policies & objectives
- Standard structure for articulating security functional & assurance requirements of solutions (products) that
 - **address specific HC security policies**
 - **meet specified HC security objectives**
 - **address specified HC risks/threats**
- Basis for verifying that products comply

Common Criteria Evaluation/Validation Scheme (CCEVS)

- Internationally recognized program
 - that accredits commercial security evaluation labs
 - to use approved test methods e.g., CEM standard
 - to evaluate products claiming compliance to CC-based security requirements traceable to security policies
 - provides independent validation of commercial labs' evaluations
 - awards certificates to validated products

Demonstrating Compliance



Activity 1: Developer self declaration of conformity.

Activity 2: Conformance demonstrated by 3rd party evaluation only.

Activity 3: Conformance demonstrated by 3rd party evaluation and private sector validation.

Activity 4: Conformance demonstrated by 3rd party evaluation and U.S. Government validation.

Benefits of using CCEVS

- Increases consumer confidence about purchased products
 - **verifies products built right, do what's expected, comply with policies**
- Lowers user expenses
 - shortens acquisition cycles
 - **outsourced security testing minimizes acceptance testing**
 - **fosters “build/buy/use anywhere” strategy**
 - increases vendor competitiveness
 - decrease liability costs
 - **legal: can provide “due diligence” & “best practices” evidence**
 - **insurance: potential to lower premiums**

Mutual Recognition Arrangement

NIAP, in conjunction with the U.S. State Department, negotiated a Common Criteria Recognition Arrangement that:

- Provides recognition of U.S. issued Common Criteria certificates by 13 nations:
Australia, Canada, Finland, France, Germany, Greece, Israel, Italy, New Zealand, Norway, Spain, The Netherlands, United Kingdom
- Minimizes need for costly security evaluations in more than one country
- Offers excellent global market opportunities for U.S. IT industry

Common Criteria Information

For more introductory info about the CC:

NIST-ITL Bulletin (11/98), get it at:
http://csrc.nist.gov/cc/info/cc_bulletin.htm

To obtain a copy of the *CC: An Introduction* and *CC User Guide* brochures

<http://csrc.nist.gov/cc/info/infolist.htm>

To get sample Protection Profiles:

<http://csrc.nist.gov/cc/pp/pplist.htm>

<http://www.iatf.net>

<http://niap.nist.gov/cc-scheme/PPRegistry.html>

For further information on the CCEVS and Validated Products

<http://niap.nist.gov/cc-scheme>

<http://niap.nist.gov/cc-scheme/ValidatedProducts.html>

**Have these concepts actually
been used in healthcare ?**

The Forum on Privacy and Security in Healthcare

Sponsored by industry and the
National Information Assurance
Partnership (NIAP)

General Focus of the Forum

Seek industry adoption of a common method to establish compliance with applicable security-related standard/laws/policies.

Strawman target for Demonstration

Construct CC PP(s) that will articulate system requirements to capture HIPAA regulatory requirements

Demonstrate how PPs and the supporting NIAP testing infrastructure can provide traceable Healthcare Security Information Systems requirements from policies through to product/system compliance

Status of NIAP Common Criteria Healthcare Examples

- **HC Methodology** “*Draft Development of a Methodology & Reference Architecture for Construction of Security Protection Profiles for Healthcare Information Systems*”
[Scheduled Revision 12/01]
- **HCFA based** “*Draft Security Functional Package for Systems Transmitting Sensitive HCFA Data (STS-HCFA)*”
[Scheduled Revision 10/01]
- **HIPAA based** “*Draft Functional Profile for Healthcare Provider Intranet with Limited Internet Exposure*”
[Scheduled Revision 11/01]
- **HC Application Protection Profile - HIPAA based**
“*Patient Point-of-Care Admission, Discharge & Transfer*”
[Scheduled Revision 10/01]

The Forum on Privacy and Security in Healthcare (FPSH)

- Incorporated as non-profit charitable organization
- Liaison established with
 - Smart Card Security Users Group,
 - AFEHCT/WEDI Project, CPRI-HOST,
 - HIPAA Summit Project, etc.
- Liaison discussions with Nat'l Assoc. of Chain Drug Stores (NACDS) and Electronic Healthcare Network Accreditation Commission (EHNAC)
- FPSH website (<http://healthcaresecurity.org>)

**How can the industry
[healthcare org,
vendors/developers and
certifying organizations] take
part in developing a set of
solutions?**

Send contact info and queries to:
info@healthcaresecurity.org

For More Information

- Forum on Privacy and Security in Healthcare
- <http://www.healthcaresecurity.org>
- *The Healthcare Security Dilemma:
Demonstrating Compliance* (white paper)
<http://www.arca.com>
- NIAP Website <http://niap.nist.gov>
- NIAP interim Protection Profile Registry
<http://csrc.nist.gov/cc/pp/pplist.htm>

Summary

- ISO/IEC 15408 *Common Criteria for IT Security Evaluation* and NIAP IT product/system evaluation and validation infrastructure an approach for “due diligence” in HC IT security
- NIAP providing sample protection profiles for selected HC environments as proof of concept for healthcare
- Demonstrating CC/PP paradigm tool for providing traceable and documented evidence of implementation of high level healthcare policy (i.e., HIPAA & HCFA) to product compliance

Contact Information

For further information contact:

L. Arnold Johnson

National Institute of Standards and Technology

Information Technology Laboratory

100 Bureau Dr. Building 820 (NIST North) Stop 8930

Gaithersburg, MD 20899

email: arnold.johnson@nist.gov

web: <http://niap.nist.gov>

phone: (301) 975-3247

fax: (301) 948-0275