Building More Secure Systems for the Critical Infrastructure

The Role of IT Security Standards, Metrics, and Assessment Programs

Dr. Ron Ross

Today's Climate

- Rapidly changing information technologies and compressed technology life cycles
- Growing complexity of IT products and systems
- Increasing connectivity among systems
- Dependence on commercial off-the-shelf IT products and systems
- Need for greater assurance in critical information infrastructures (both public and private sector)

Today's Challenge

- Consumers have access to an increasing number of security-enhanced IT products with different capabilities and limitations
- Consumers must decide which products provide an appropriate degree of protection for their information systems
- *Impact: Choice of products affects the security of systems in the critical information infrastructure*

The Fundamentals

Building more secure systems depends on the use of---

- Well defined IT security requirements and security specifications

  - describing what types of security features we want…

- Quality security metrics and appropriate testing, evaluation, and assessment procedures

  - providing assurance we received what we asked for…

What Is Needed?

- Producers of IT products need to have a better understanding of consumer's information security requirements
- Consumers of IT products, systems, and networks need to have better ways to:
  - ✓ specify desired security features and assurances
  - ✓ assess the security claims made by producers

The International Standard

Common Criteria-ISO/IEC 15408

What the standard is –

- Common structure and language for expressing product/system IT security requirements
- Catalog of standardized IT security requirement components and packages

How the standard is used –

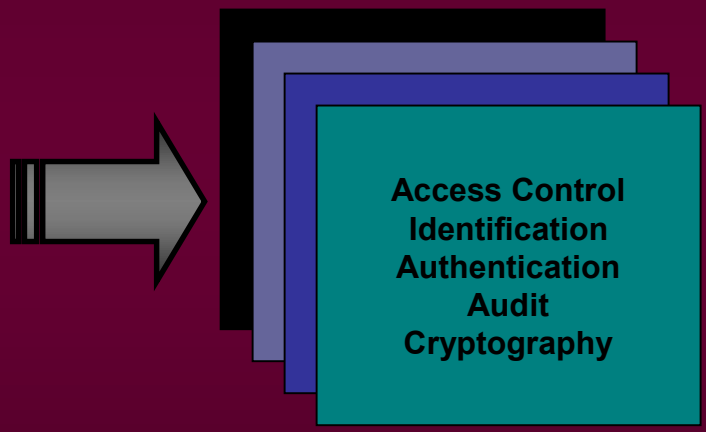
- Develop IT security requirements and specifications for products and systems
- Evaluate products and systems against known and understood IT security requirements

Defining Requirements

ISO/IEC Standard 15408

A flexible, robust catalogue of standardized IT security requirements (features and assurances)

Protection Profiles



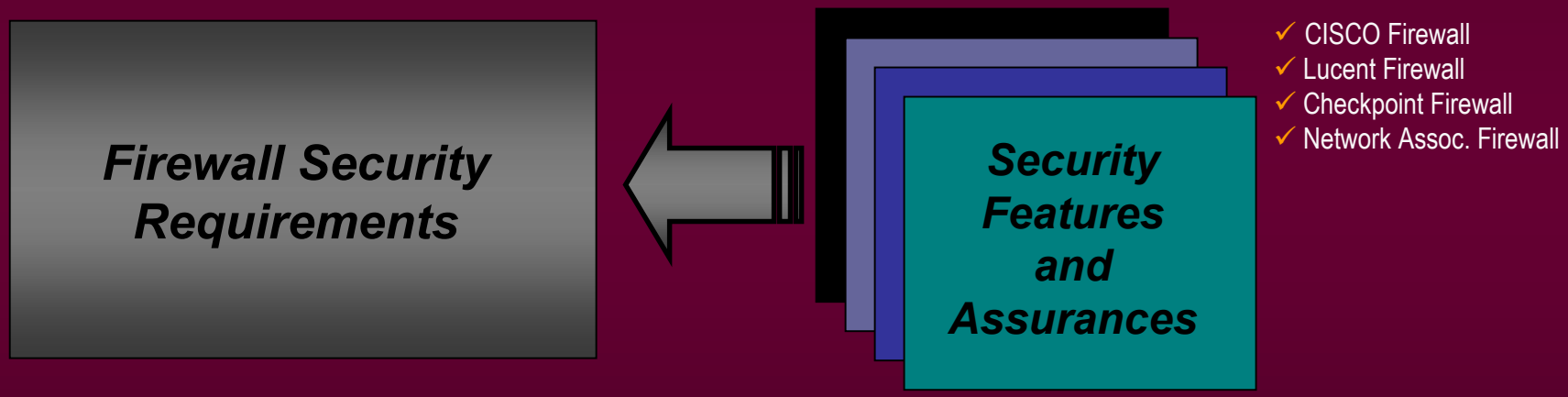
- ✓ Operating Systems
- ✓ Database Systems
- ✓ Firewalls
- ✓ Smart Cards
- ✓ Applications
- ✓ Biometrics
- ✓ Routers
- ✓ VPNs

Consumer-driven security requirements in specific information technology areas

Industry Responds

Protection Profile

Security Targets

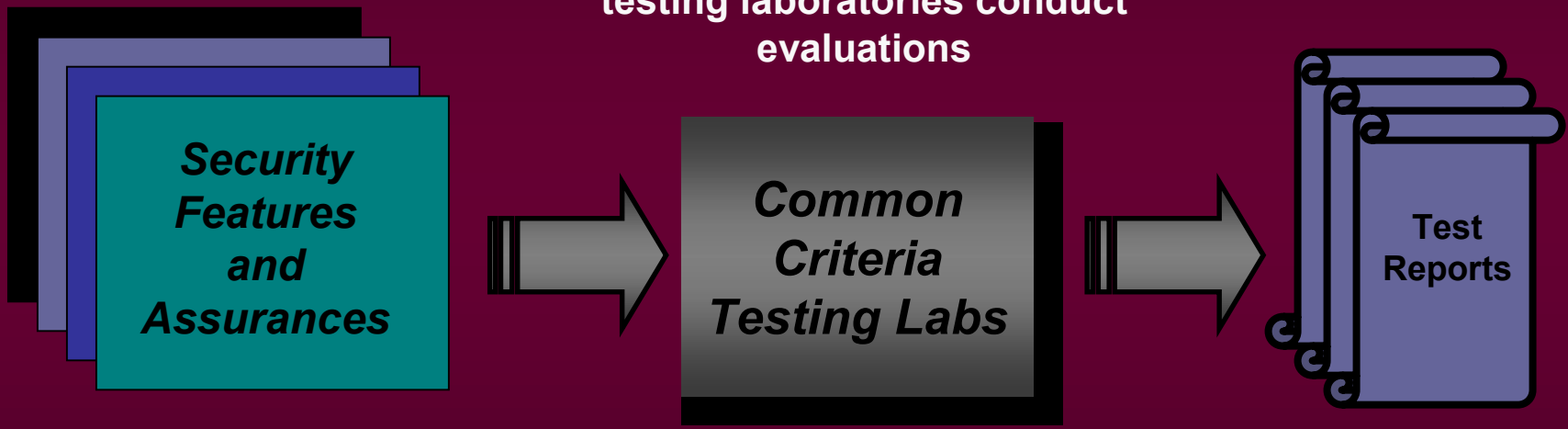


Consumer statement of IT security requirements to industry in a specific information technology area

Vendor statements of security claims for their IT products

Demonstrating Conformance

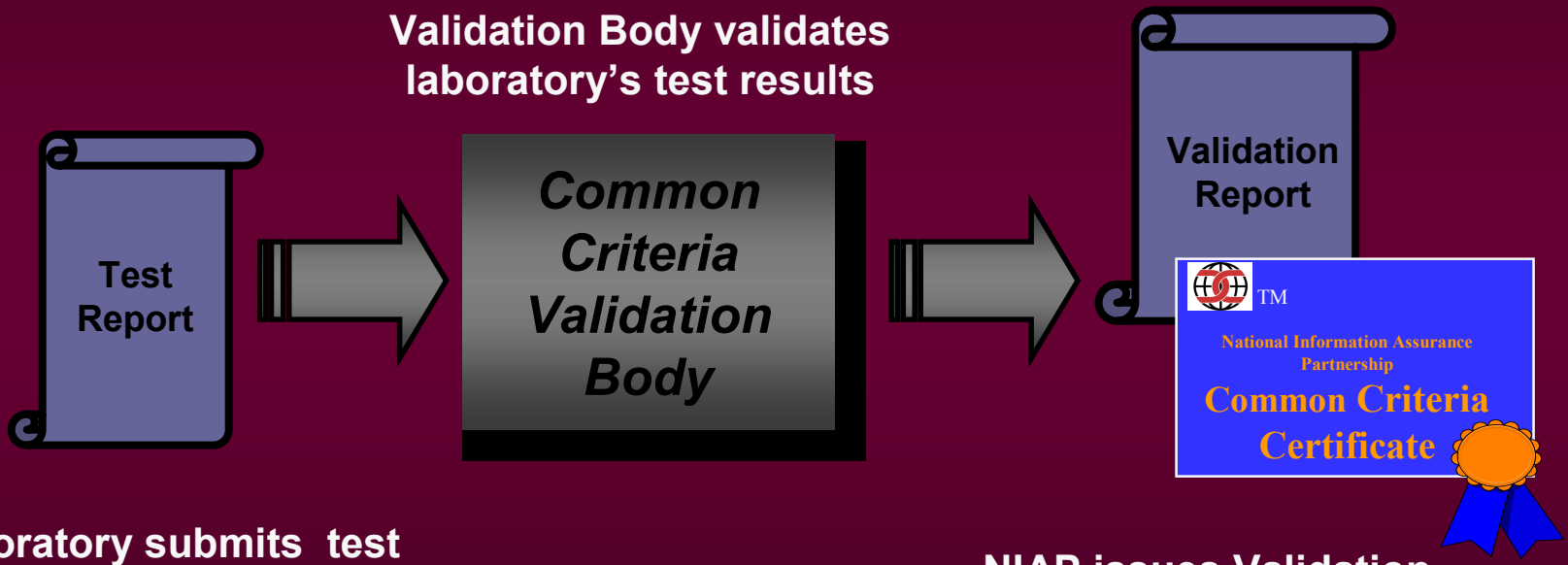
Private sector, accredited security testing laboratories conduct evaluations



Vendors bring IT products to independent, impartial testing facilities for security evaluation

Test results submitted to NIAP for post-evaluation validation

Validating Test Results



Laboratory submits test report to Validation Body

NIAP issues Validation Report and Common Criteria Certificate

Mutual Recognition Arrangement

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

- Provides recognition of U.S. issued Common Criteria certificates by 14 nations:

  Australia, Canada, Finland, France, Germany, Greece, Israel, Italy, New Zealand, Norway, Spain, Sweden, The Netherlands, United Kingdom
- Eliminates need for costly security evaluations in more than one country
- Offers excellent global market opportunities for U.S. IT industry

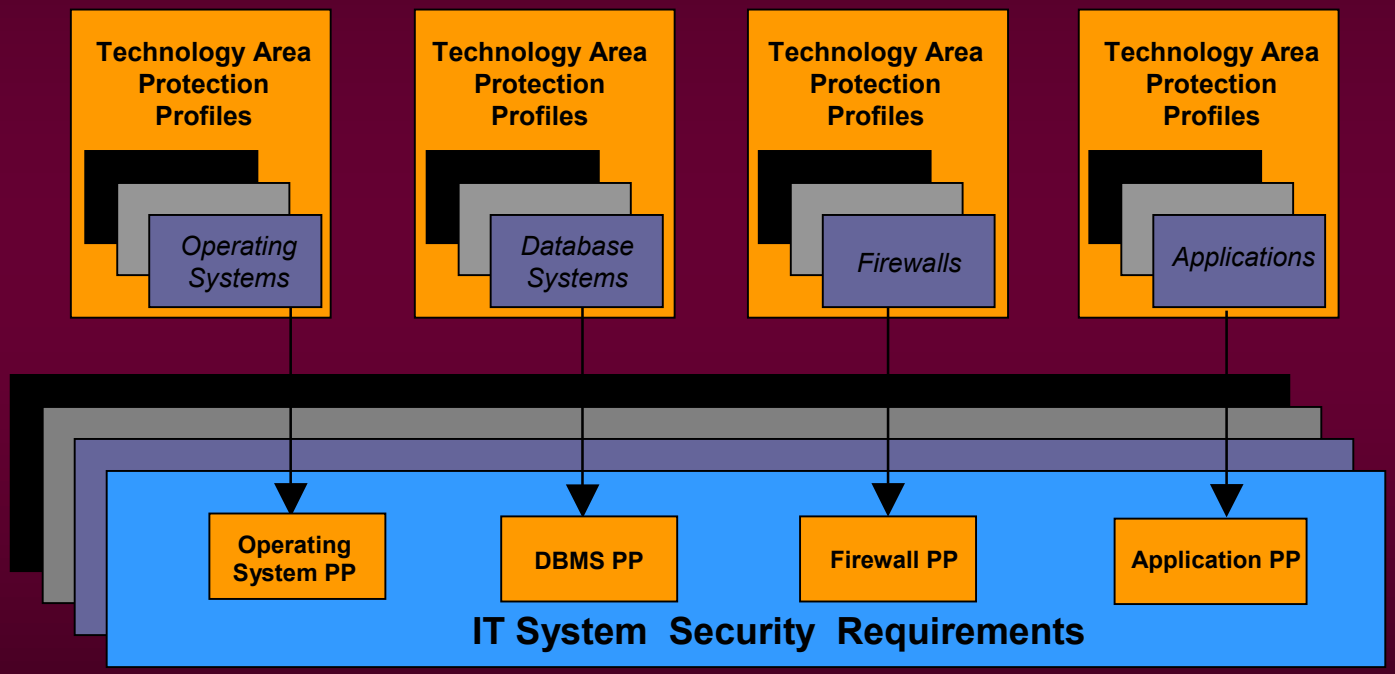
Extending Assurance to Systems

Building more secure systems requires --

- Well defined system-level IT security requirements and security specifications
- Well designed component IT products
- Sound systems security engineering practices
- Competent systems security engineers
- Appropriate metrics for product/system assessment
- Comprehensive system life cycle management

Role of Protection Profiles

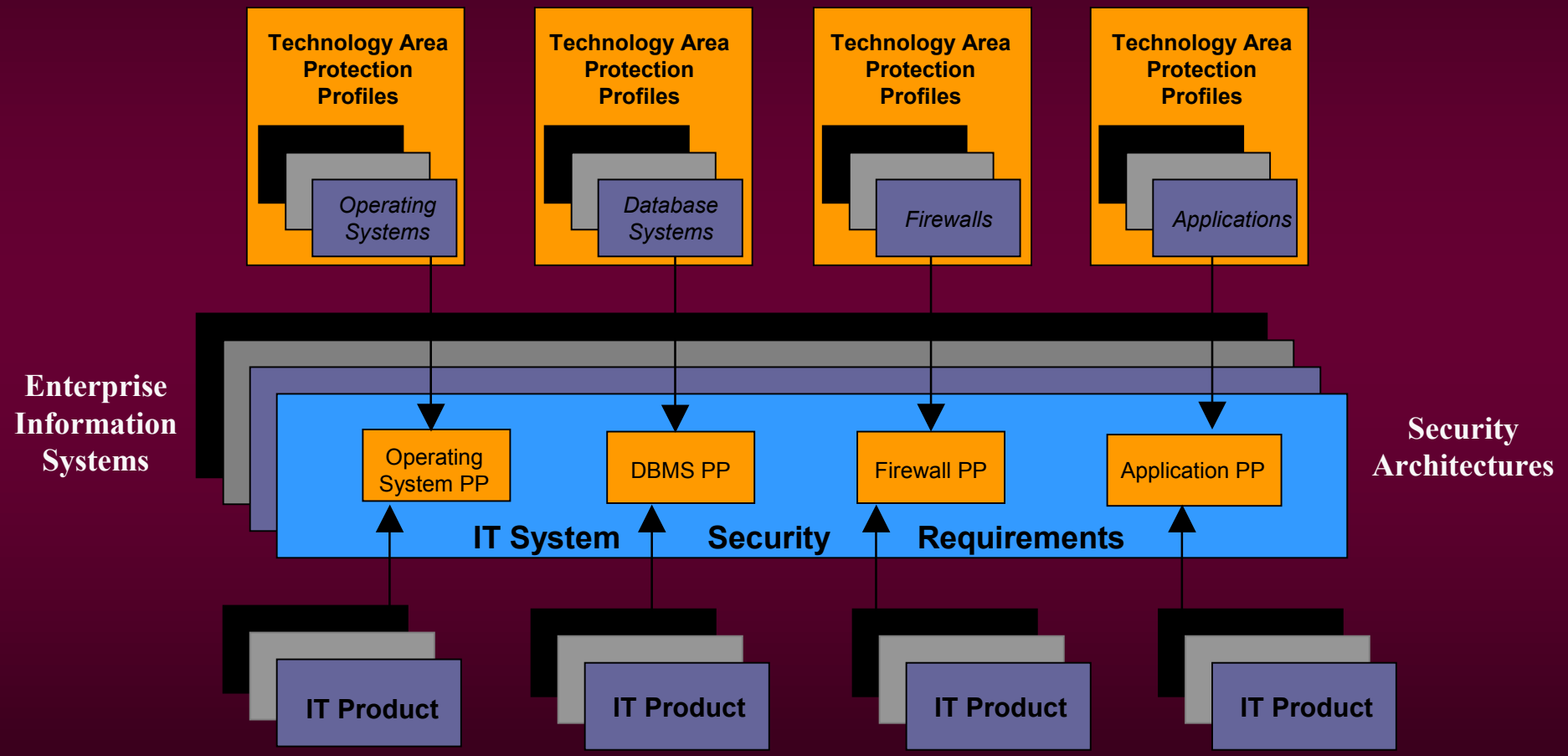
Generalized, Consumer Driven Security Requirements



Enterprise Information Systems

Role of Protection Profiles

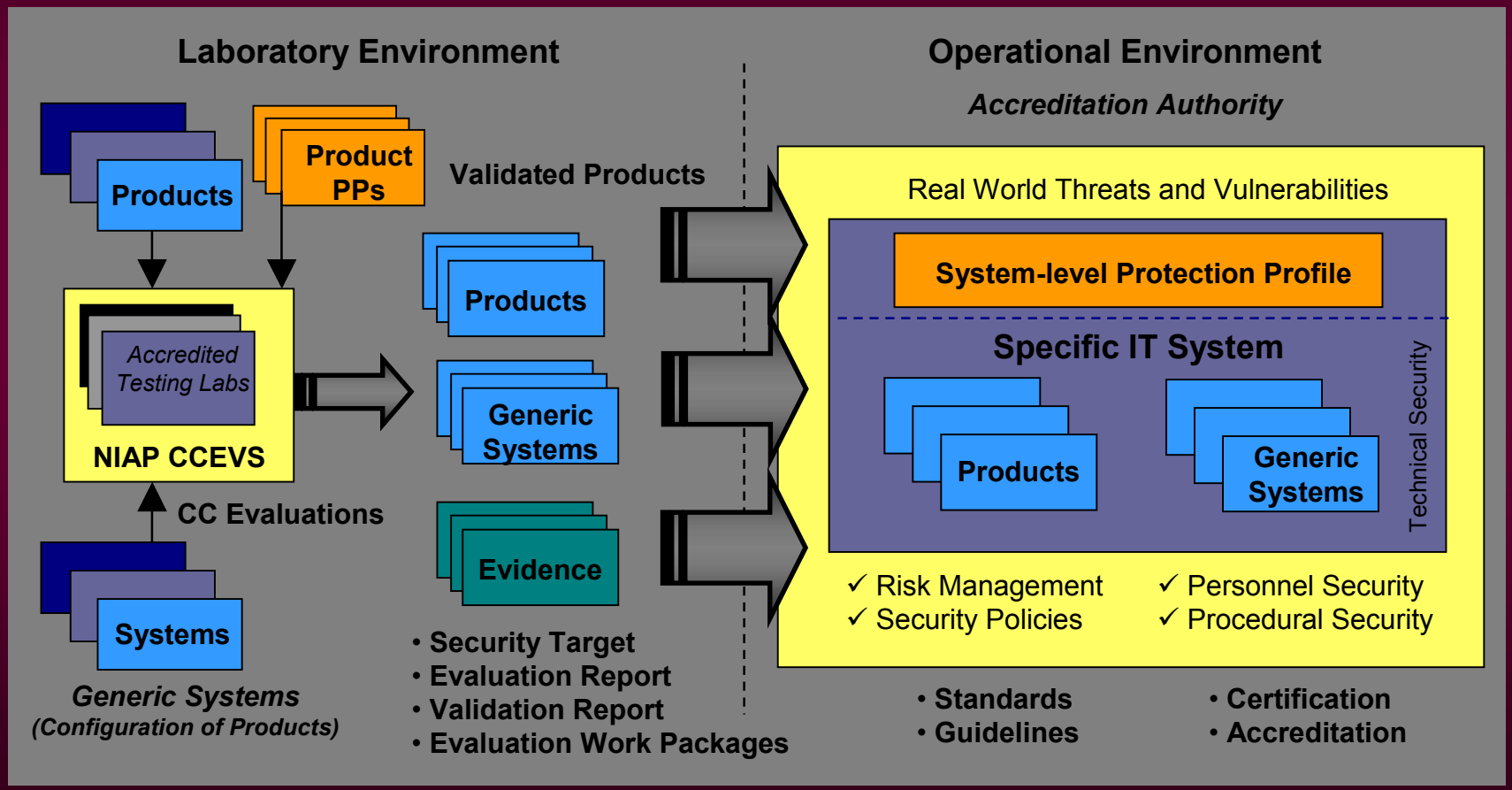
Generalized, Consumer Driven Security Requirements



Variety of Vendor Driven IT Products

A Comprehensive Approach

Linking Critical Assessment Activities



National Information Assurance Partnership®

NIAP Testing Advantages

- Specification of security features and assurances based on an international standard
- Evaluation methodology based on an international standard---leading to comparability of test results
- Security testing laboratory expertise assessed by recognized national bodies; quality technical oversight provided by government experts
- Testing results recognized by many nations
- Reduced testing costs to sponsors of evaluations

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Director
Dr. Ron S. Ross
NIST-ITL
301.975.5390
rross@nist.gov

Deputy Director
Terry Losonsky
NSA-V1
301.975.4060
tmloson@missi.ncsc.mil

Senior Advisor
Dr. Stuart Katzke
NIST-ITL
301.975.4768
skatzke@nist.gov

Chief Scientist
R. Kris Britton
NSA-V1
410.854.4384
britton@radium.ncsc.mil

Email: niap-info@nist.gov
World Wide Web: http://niap.nist.gov