

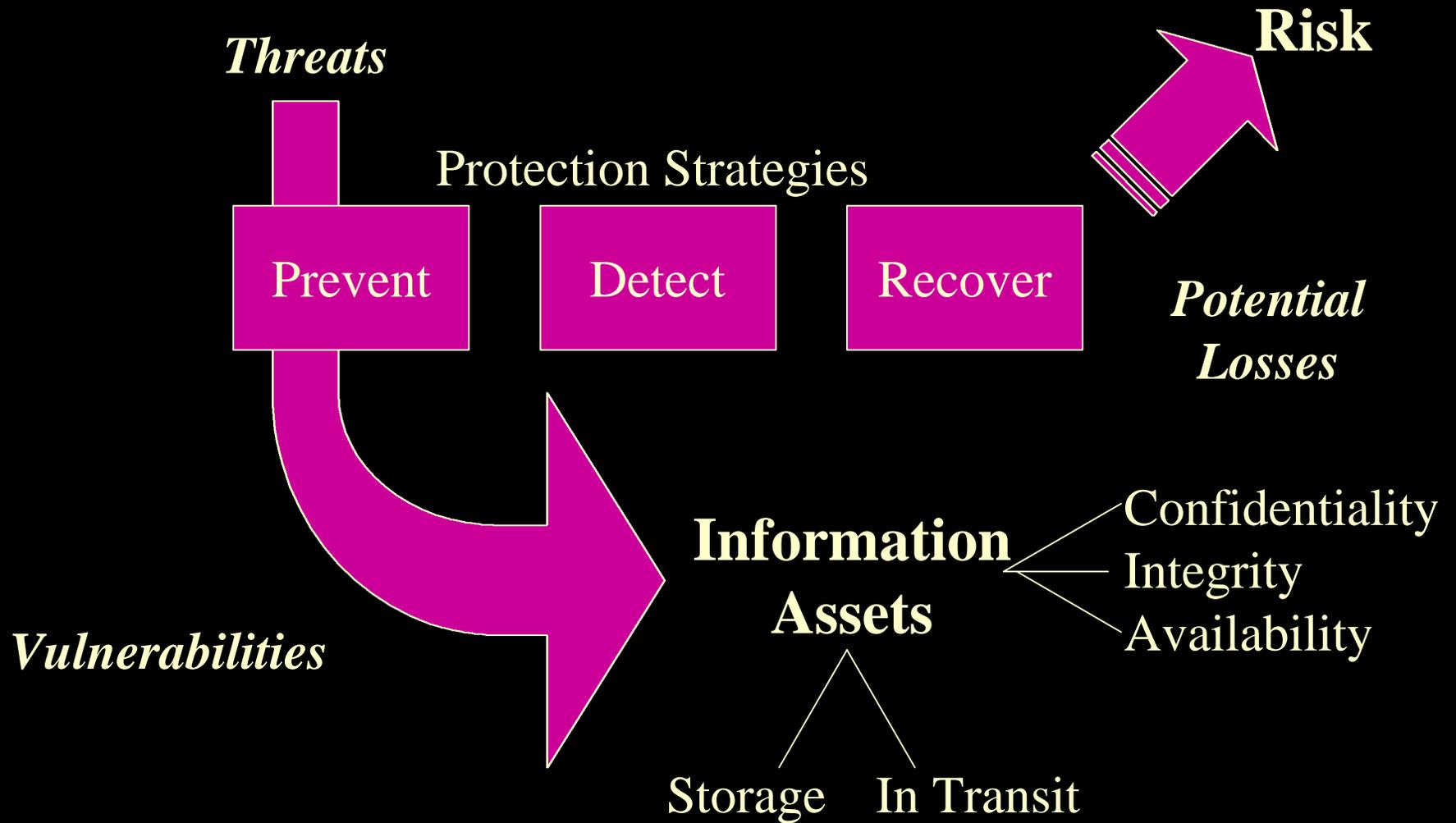
# Information Security in a Wireless World

Dennis D. Steinauer  
Computer Security Division  
Information Technology Laboratory  
National Institute of Standards and Technology  
Gaithersburg, MD

# Information Security in a Wireless World

- Basic Security Strategy
- Emerging Technologies
- Critical Information Infrastructure Elements
- Emerging Security Needs

# The Lingo



# Security Services

- Confidentiality
- Integrity
- Authentication
- Access Control
- Non-Repudiation

# Emerging Technologies

All new information technologies that have impact on critical national infrastructures will have security needs -- which must be addressed from the start.

- Wireless communications
- Intelligent/mobile agents
- Embedded & ubiquitous computing
- Component-based systems
- Next ???

# Critical National Infrastructures

- Banking
- Transportation
- Oil & Gas Distribution
- Electric Power Distribution
- Emergency & Protective Services
- Information & Communications
- Government Services

# Critical *Information* Infrastructure Elements

- Internet Backbone
- Internet Domain Name Service
- Public Key Infrastructure(s)
- Underlying Communications Technology

# Emerging Security Needs

- Formal security criteria
- Advanced testing methodologies
- High confidence, high availability systems
- Advanced authentication
- Advanced, high-speed cryptography
- Complex system composition/analysis
- Configurable/maintainable systems
- Intrusion Detection
- Audit & threat monitoring

# Critical Infrastructure Protection

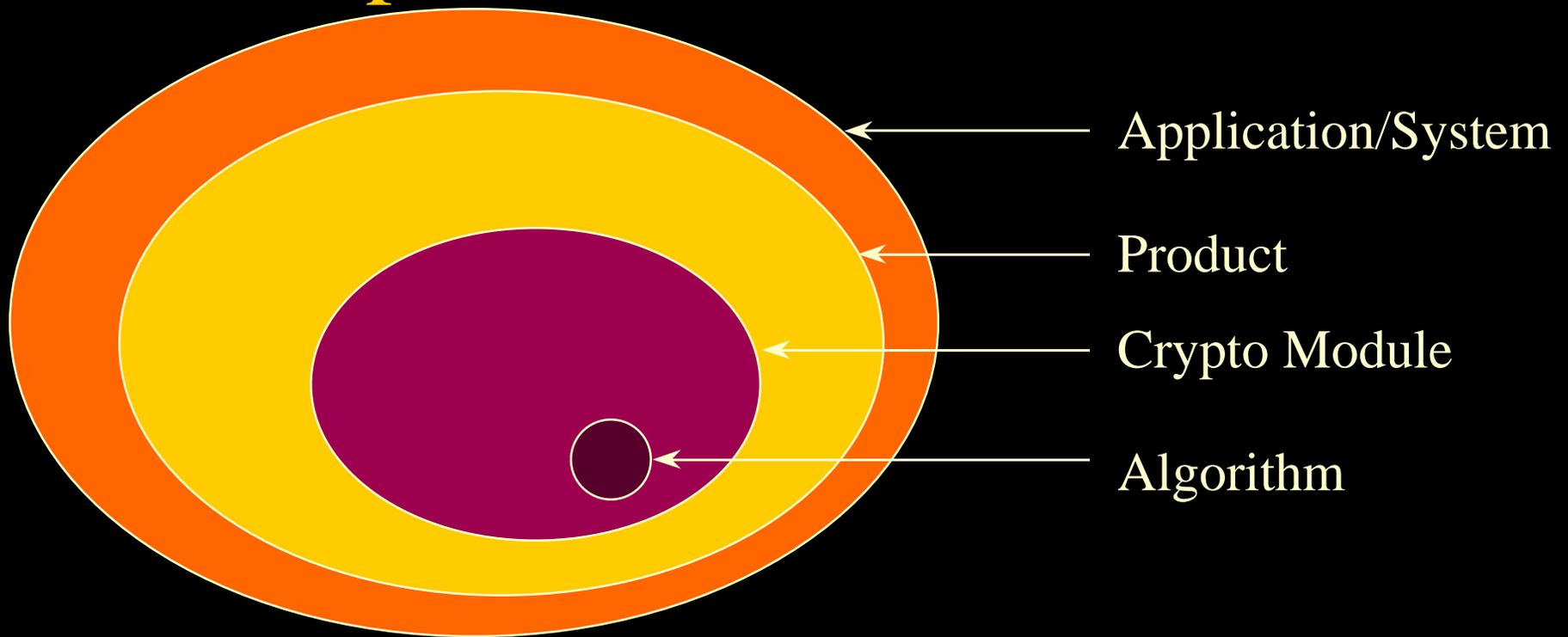
## Focus Areas

- Security Technology
- Systems Survivability
- High Assurance Systems
- Application of Domain-Specific Expertise
- Security for Federal Systems

# Security Technology

- Advanced Cryptography
- Public Key Infrastructure
- Common Criteria (CC)
- National Information Assurance Partnership (NIAP)

# Specification-Based T/E



Level	Example	Specification
Application/System	Air Traffic Control	CC, GSSP, ...
Product	Firewall , OS	Common Criteria (CC)
Security Module	Crypto Module	FIPS 140-1
Algorithm	DES	FIPS 46-2

# System Survivability

- Extend *intrusion detection & response technology* to large-scale, high criticality systems & networks
- Metrics, test methods, & remote testing techniques for *assessing system survivability*
- *Best practices* for designing and deploying survivable systems
- Security framework for “security” *mobile agents*

# High Assurance Systems

- Legacy system evaluation
- High assurance security engineering
  - Transfer system engineering technology from NASA, NRC, FAA safety critical systems
  - Develop new technical methods & approaches
  - Automated testing techniques
  - Professional certification
  - Fault tolerance/redundancy

# Security for Domain-Specific Operational Support Systems

- Manufacturing supervisory control & data acquisition (SCADA) systems (MEL)
- Cybernetic building management systems (BFRL)

# Security for Federal Systems

## *“Lead by Example”*

- Identify, apply “Best Practices”
  - Training & awareness guides
- Develop standards, reference implementations, & security and interoperability testbeds
  - Criteria, tests, & accreditation requirements for system security administrators
- Agency Assistance
  - Protecting their critical infrastructures
  - Using advanced security technology

# Security Technology for Critical Infrastructure Systems

- Applying existing technology
- Extending domain expertise
- Building *security* infrastructures
- High assurance systems engineering
- Meeting emerging needs
- Government-Industry partnership

# **NIST Computer Security Program: From Algorithms to Critical Infrastructures**

- Basic Technologies
- Program Strategy
- IT Security Standards
- Program Structure
- Program Elements

# Basic Information Security Technologies

- Cryptography
  - Privacy encryption
  - Digital Signatures
- Authentication
- Access Control
- High Assurance Systems Engineering
- Test and Evaluation
- Audit, Threat Monitoring, Intrusion Detection

# NIST Security Program Strategy

- Collaboration with Industry
  - Work with industry to develop specifications and conformance tests for **secure, trustworthy, interoperable** products and systems
- Primary Focus on Specification-Based Testing
  - Validate conformance of commercial products to FIPS
  - Common Criteria
  - National Information Assurance Partnership
- Act as “honest broker”
- Technology Transfer
- Balance **Computer Security Act, PDD63**, and “Traditional” NIST/ITL Roles

# NIST IT Security Standards

— a record of partnership with Industry

- Data Encryption (DES) - FIPS 46-2, ANSI
- Message Authentication (MAC) - ANSI, FIPS 113
- Cryptographic Module Security Requirements - FIPS 140
- Key Management - ANSI X9.17, FIPS 171
- Digital Signature and Hash (DSA/SHA) - FIPS 186, 180-1
- Entity Authentication (FIPS 196) - IETF
- Cryptographic API's (Draft FIPS) - X/OPEN
- Posix - FIPS, IEEE, ISO
- Minimum Interoperability Specification for PKI Components (MISPC) - NIST SP, IETF

# NIST Computer Security Program

Customers



Industry

Federal  
Government

Health Care

Environment

Manufact.

Elec.Comm.

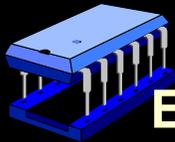
Gov't Svcs

Education

Libraries

National/Critical Information Infrastructure

## Program Focus Areas



### Enabling Technology

- Cryptographic Technology and Applications
- Key Recovery
- Secure Internet Protocols



### Enabling Infrastructure

- Public Key Infrastructure
- Criteria and Assurance
- Internetworking Security
- Security Management

# Cryptographic Technology and Applications

- Commercial Cryptographic Standards
  - Advanced Encryption Standard (AES)
  - FIPS to allow RSA & EC technology
  - Conformance Tests for ANSI RSA & ECDSA
- Crypto-Module Validation Program (FIPS 140-1)
- ANSI Random Number Generation (co-editor)

# Key Recovery

- Technical Support for Emergency Access Working Group by Testing Key Recovery Pilots
- Secretariat and Liaison for Commercial Data Recovery Technical Advisory Committee; and Participation as Gov't Technical Representative
- Establish Key Recovery Root CA
- Develop Pilot Email Key Recovery System

# Public Key Infrastructure

- Tests and Assertions for Minimum Interoperability Specification for PKI Components (MISPC)
- Develop MISPC Reference Implementation
- Implementation of a root CA Testbed for government pilots
- Develop Security Requirements for CA components

# Internetworking Security

- IPv6 Reference Implementation and Test Bed
- Role Based Access Control
- Federal Government Computer Incident Response Center (FedCIRC)

# Security Management and Support

- National Information System Security Conference
- Computer System Security and Privacy Advisory Board
- Federal Computer Security Program Managers Forum
- Agency Assistance & Collaboration

# Criteria and Assurance

- Specification-Based Testing & Evaluation (T/E)
- Common Criteria (CC)
- Common Criteria Testing Program (CCTP)
- National Information Assurance Partnership (NIAP)

# Advanced Network Technology

- IPsec
- IP testbed
- Mobile agents
- Virtual Private Networks
- “Adaptive” Networks

# High Assurance Development Tools

- Current Work
  - Role Based Access Control (RBAC)]
  - Software Analysis Tools (Slicer, etc.)
- Planned/Potential Work
  - Advanced Analysis Tools, Toolkit
  - Automated Testing
  - Error/Failure Database
  - Formal Methods

# For Additional Information

- NIST Computer Security Resource Center
  - <http://csrc.nist.gov>
- President's Commission on Critical Infrastructure Protection
  - <http://www.pccip.gov>
- Internet Engineering Task Force
  - <http://www.ietf.org>