Meeting Cyber Security Challenges

Presented to
Naval Postgraduate School
Cyber Summit
29 October 2009

Cynthia Irvine, PhD, Professor
Naval Postgraduate School

UNCLASSIFIED
Overview

• Challenges in Cyber Security
• Important NPS capabilities
• Selected research activities
Cyberspace

- Internet is today’s core – many interdependencies

Information, software, virtual communities

Cyberspace physical infrastructure

Critical infrastructure dependent upon information technology
Networks upon Networks

- Cyberspace: hierarchies of virtual and cyber-physical networks
  - Range from tiny to large
- Many smart, small devices
  - Highly interconnected
- Hybrid systems pervasive
  - Sensor and control

Enormous Complexity
Cyber Security Grand Challenges

- Extensible Trustworthy Systems
- Cyber Identity
- Resilient Survivable Systems
- Information Provenance
- Measurement of Security
- Countering Insiders
- Ergonomic Security – Usability
- Balance security and privacy
- Better Methods to Construct & Assess Secure Systems
- Economic Security – reuse and composition
- Human Capacity
Cyber Security Grand Challenges

Extensible Trustworthy Systems

Single flaw can topple entire system.

Building blocks for which we have high confidence are needed.
Cyber Security Grand Challenges

Cyber Identity: Who and what am I talking to?
Cyber Security Grand Challenges

Resilient Survivable Systems

• Systems must
  – Degrade gracefully
  – Maintain security under attack
  – Recover securely from fall-back mode
  – In worst case: fail secure
Cyber Security Grand Challenges

Information Provenance

Real

Fake
Measurement of Security

• We need to be able to quantify security
  – Technically, to enable system construction
  – So that decision makers can weigh risks
Cyber Security Grand Challenges

Countering Insiders
Cyber Security Grand Challenges

- Ergonomic Security – Usability

Cyber security hygiene must be understandable and easy to use.
Cyber Security Grand Challenges

Balance security and privacy

These are sometimes conflicting objectives
Can information be authentic yet anonymous?
Cyber Security Grand Challenges

Better Methods to Construct & Assess Secure Systems

Current tools for constructing secure systems are often inadequate and difficult to use.
Cyber Security Grand Challenges

Economic Security

Reuse and composition of components

Do we have to boil the ocean yet again each time we build a secure system?
Cyber Security Grand Challenges

Human Capacity

• The need for talent at all levels is critical

• Education must be a high priority

• Our competitiveness in a globalized economy depends on it.
Huge Benefits / Huge Risks

• Cyber security is enabling technology.
  – Allows activities otherwise unthinkable

• Risks include
  – Physical failures
  – Technological failures
  – Misuse
    • Crime: extortion, theft
    • Disruption, usurpation
    • Propaganda, disinformation

Many risks today – adversaries have the upper hand
Need to change the balance
Overview

• Challenges in Cyber Security

• Important NPS capabilities
  – CISR
  – Educational Programs

• Selected research activities
In the NPS Computer Science Department,

we do it.

... AND WE HAVE BEEN DOING IT WELL FOR A LONG TIME (1978)
Things we’ve been doing well

- **Security Science**
  - Theoretical formalisms
  - Models
  - Protocol analysis
- **Constructive Security**
  - Highly trustworthy systems
  - Multilevel security
  - Hardware security
- **Security Engineering**
  - Tools and application
- **Security Analytics**
  - Forensics
  - Data mining
  - Vulnerability analysis
- **Security Applications**
  - Intrusion detection
  - Identity management
- **Security Education**
  - Courses & Curricula
  - Certificates
  - Games & Outreach
Center for Information Systems Security Studies and Research

- CISR established in 1996
- Began national security education outreach in 1997
- Center of Academic Excellence
  - NSA and DHS joint award
  - Information Assurance Education
  - Information Assurance Research
- Scholarship Programs
  - IASP in cyber security for military officers
  - Inaugural participant NSF Scholarship for Service
    - 60 graduates to date – civilian members of Federal workforce
    - Monarch – to encourage women and underrepresented groups
- Synergistic research and education
  - Large research group with critical mass for hard problems

Irvine, 29 October 2009
NPS Cyber Security Summit
Educational Programs

- MS and PhD degrees
- All MS students take introduction to computer security
- Security track in CS Department
  - 4 required courses
  - 4 electives
  - Thesis research

- Certificate Programs
  - Identity Management Certificate
    - 4 courses
    - “Hybrid” format
      - Participants work at their regular jobs while taking classes
  - Information Systems Security Engineering Certificate
    - Currently teaching to students at NSA
Courses: Elementary to Advanced

• Introduction to Computer Security
• Secure Management of Systems*
• Network Security* ✓
• Secure Systems Principles* ✓
• Security Policies Models and Formal Methods*
• Cyber Ethics and Policies
• Network Vulnerability Analysis and Risk Mitigation ✓
• Biometrics

CS Core

§ CS Core
* Security Track Required
✓ Information Systems Security Engineering Certificate
 ○ Identity Management Certificate (joint with two IS courses)

• Identity Management Infrastructure
• Protocol Analysis
• Introduction to Information System Security Engineering ✓
• Applied Information System Security Engineering ✓
• Secure Systems Lifecycle
• Wireless Security
• Advanced Vulnerability Analysis
• Forensics
• Data Fusion
• Certification and Accreditation
• Advanced topics

Irvine, 29 October 2009

NPS Cyber Security Summit
Overview

• Challenges in Cyber Security
• Important NPS capabilities
• Selected research activities
  – Trusted Computing Exemplar
  – Trustworthy Architectures
  – Multilevel Security
  – Cyber Security Game
  – Hardware Security
Trusted Computing Exemplar Project
Address Subversion - Limit Opportunity

• **Need lifecycle assurance**
  – High assurance
  – Protection via rigorous security engineering
    • No unspecified functionality
    • Use of formal verification techniques
  – When Applied in MLS Context:
    • Bound information flow
      – Prevents Trojan Horse damage
    • Uses formal models
      – Supports implementation assessment
TCX Integrated Activities

• Rapid High Assurance Development Framework
  – Configuration Management, Engineering Process, …
  – Semantic programming-based documentation system
• Develop High Assurance Security Concepts
  – Separation Kernel - EAL7
    • Many student research projects
  – High Assurance Application
    • Authentication Device for MLS Trusted Path
• Evaluate Components for High Assurance
  – Developing EAL6+ Separation Kernel Protection Profile
    • ST will be EAL7
• Disseminate Results via Open Methodology
TCX Benefits

• Evaluable Reference Implementation
• Components with *a priori* Assurance Against System Subversion
• Public Availability of High Assurance Development Framework
• Transfer to Next Generation
  – New Experts in Security Development
  – High Assurance Knowledge and Capabilities
Trustworthy Architectures

emergency access to critical data
• Most of the time Joe is an ordinary guy
• During emergencies, he is allowed to access critical information
• Extraordinary information cannot be leaked to the internet
• When emergency ends, collected information sent to emergency management
• Device is purged of emergency information, reset for next emergency
Key Concepts

• Based on Least Privilege Separation Kernel
  – Ensures separation of normal and emergency information
  – Permits emergency activities to access selected “normal” data

• Extraordinary access mediated by high assurance enforcement mechanism
  – Gives cooperating organizations confidence that shared information is protected

• Trusted path mechanism
  – Receives initial emergency signal
  – Insures that only authorized first responders have access to emergency information

• Provides ergonomic security

Irvine, 29 October 2009
NPS Cyber Security Summit
Multilevel Security
Networks that cannot share

• National policies information protection must be enforced
  – Separate networks for each classification level
    • Internet / NIPRNET / SIPRNET / JWICS
  – Some communities require mandatory separation of compartments
  – Coalitions result in additional networks

Problem: No coherent view of classified information

• Requirements
  – Secure - enforce national policies
  – Usable - support applications that make users productive
  – Scalable - extensible beyond small laboratory experiments
Our Solution: MYSEA

• The Monterey Security Architecture (MYSEA)

A high assurance client-server system that allows authenticated users executing popular commercial applications to securely access data and services at different classification levels simultaneously

• High assurance multilevel LAN/WAN architecture
  – Many commodity components
    • Commercial off-the shelf workstations, OS and applications
    • Legacy single-level networks
  – Reduce system footprint – one PC, many classification levels
  – Strategic high assurance components
    • Policy decision and enforcement

• Prototype implementation and integrated MLS testbed
MYSEA Security Features

- Technical elements
  - Familiar user work environment
  - Integration of MLS LAN with classified networks
  - Centralized security management
  - Dynamic security policies and services
  - True multilevel access to data
  - Single sign-on within the MLS LAN
  - Server replication supports scalability
  - High assurance trusted path

SUMMARY
MYSEA gives users coherent view of information at different classifications levels
CyberCIEGE

a cyber security game
Player = Information Security Decision Maker

ATTACKERS
Top Secret Formula
Critical Data

$$

Goal

Asset $$

Computer

Goal

Network

VPNs
Firewalls
Antivirus
Link encryptors
PKI
Authentication servers
Access control lists
Cross domain solutions
Card readers
Biometric scanners
Procedural security

User

User

Goal

Asset $ 

Computer

Goal

Asset $$$$ 

Computer

Vandals

Trojan horse
Trap door
Insiders
Virus / worms / Bots
Wiretaps
Denial of service

Irvine, 29 October 2009
NPS Cyber Security Summit
Who Uses CyberCIEGE?

Requests by the numbers:
- Navy: 60
- Army: 103
- Air Force: 104
- Marines: 20
- US Government: 139
- University: 245
- Community College: 45
- High School: 18
- Other: 85

Irvine, 29 October 2009
NPS Cyber Security Summit
3Dsec

Security in Hardware
3DSec: Trustworthy System Security through 3D Integrated Hardware

Goal: Build trustworthy systems using commercial hardware components

Problem: Integrating specialized security mechanisms is too costly for hardware vendors

Idea: Augment commodity hardware after fabrication with a separate layer of security circuitry

Anticipated Benefits:
Configurable, protected, low-cost hardware security controls that can override activity in the commodity hardware

Privacy Applications:
Detect and intercept the execution of malicious code
Prevent the microprocessor internals from being exploited to leak crypto keys
Tag and Track private information as it flows through a processor
Summary

• Challenges in Cyber Security
• Important NPS capabilities
• Selected research activities

NPS resources in CISR and the Department of Computer Science are among best in the world for the study and advancement of Cyber Security.
Cynthia E. Irvine, PhD
Director, Center for Information Systems Security Studies and Research
Department of Computer Science
Naval Postgraduate School
Monterey, California

irvine@nps.edu