2006-01-24

MYSEA Multilevel Testbed and Cross Domain Solutions

Irvine, Cynthia

NAVAL
POSTGRADUATE
SCHOOL

MYSEA Multilevel Testbed and Cross Domain Solutions

January 2006

Cynthia Irvine
Naval Postgraduate School

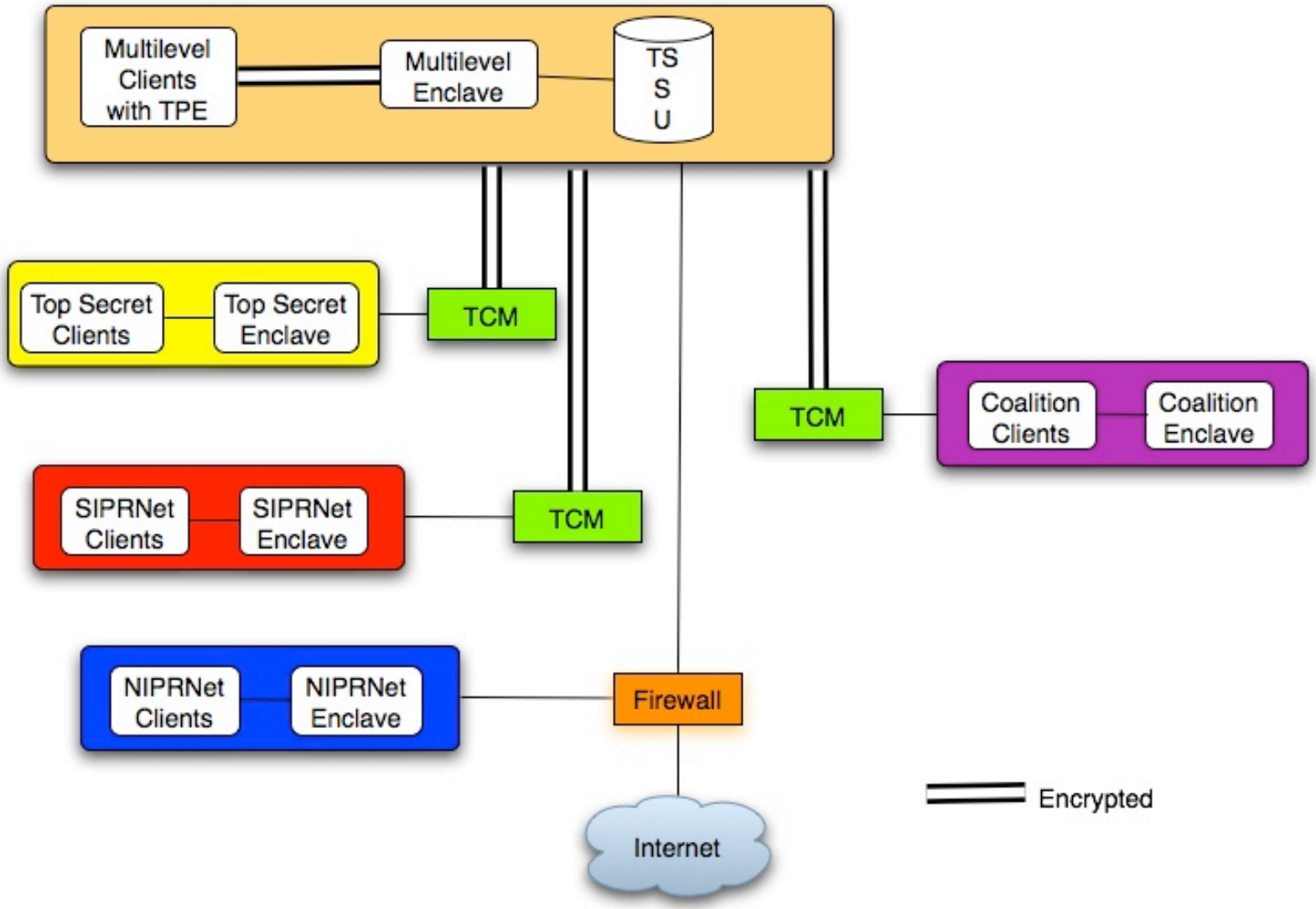
MYSEA Testbed Objectives

- Experimentation and Research Framework
  - High Assurance Solutions
  - Distributed Multilevel Functionality
  - Dynamic Security
  - Trusted Authentication
  - Open Architectures and Interfaces
- Currently Support:
  - MYSEA Research Project
  - Trusted Computing Exemplar Project
  - Dynamic Security Services Project
  - Basic GIG IA Architecture and Security Concepts
- Long Range Applicability
  - Additional GIG IA experiments
  - Other Complex Enterprise Networks

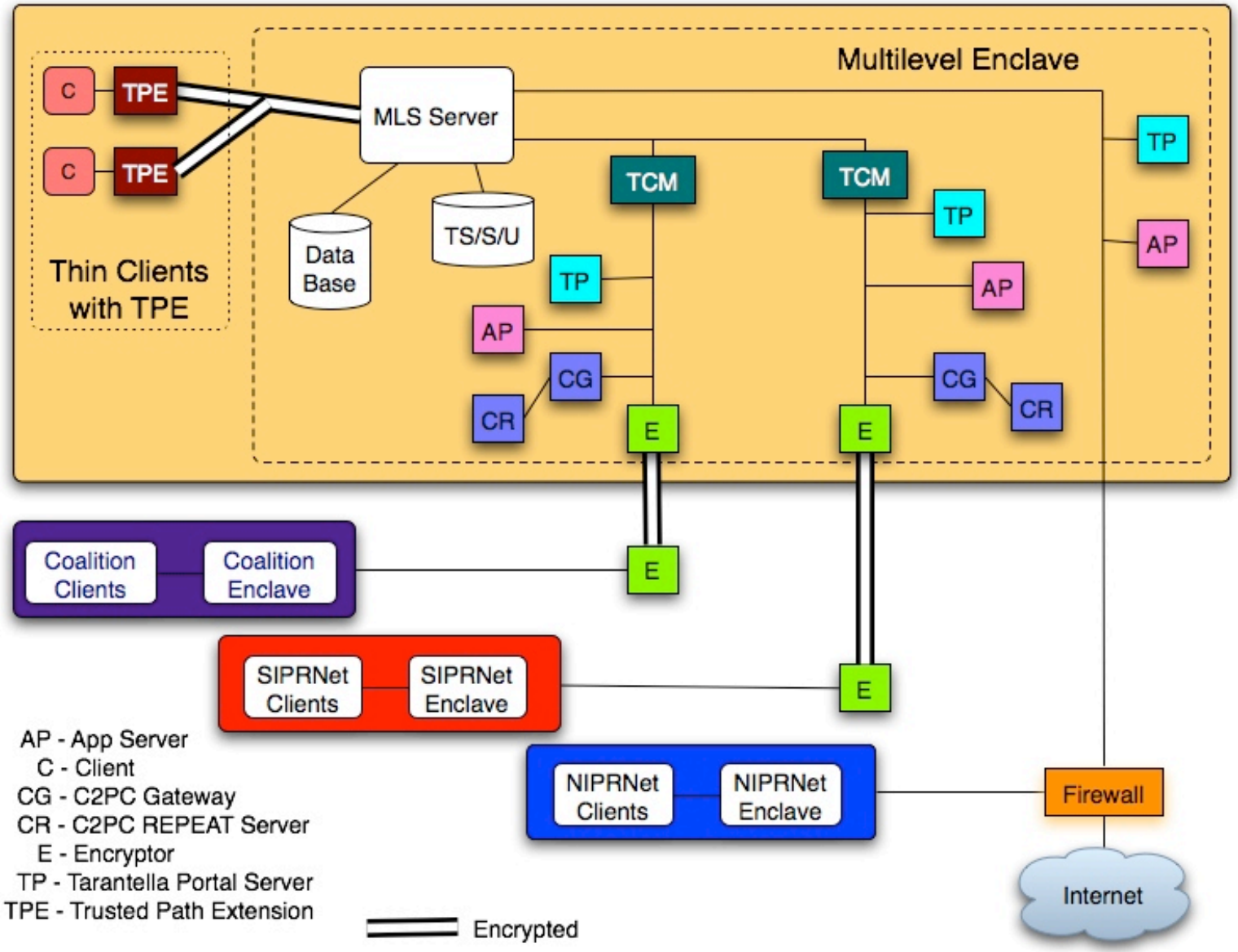
Near-Term Testbed Experiments

- Secure connections to classified networks
- Use COTS and legacy hardware and software components
- Use open standards
- Apply high assurance security technology to legacy elements
- Centralize security management
- Integrate high assurance multilevel security with existing sensitive networks
- Manage access to classified networks using high assurance trusted communication channel techniques
- Dynamic security services
- Open architectures to incorporate new technologies
- Use XML tags as security markings
- Secure single sign-on across multiple MLS servers
- Server cluster technologies

Testbed Architecture



Testbed Design



Demonstrated MYSEA Features

- Distributed Security Architecture
- Multilevel Policy Enforcement
- Unmodified Commercial Desktop Applications
- Trusted Path for Security-Critical Operations
- Reach-back to Single Level Networks
  - Aggregated Information Services
- Dynamic Policy Modulation of Security Services

Testbed Components Secure Server

- True Multilevel Security Policy Enforcement
  - Coherent View: Users at HIGH see Information at LOW
  - Label-based Policy Enforcement
    - Hierarchical and Categories
  - Support for Integrity-Based Separation
    - Isolate cyber-trash from reliable users and programs
  - Flexible Label Management
- Existing Commercial MLS Base
  - Digital Net XTS-400
  - Evaluated at Class B3 under TCSEC (aka “Orange Book”)
  - Currently Under Evaluation under Common Criteria
  - Support for Certification and Accreditation Goals

Server Network Enhancements

- Multilevel “inetd”
- Distributed High Assurance Authentication on MLS LAN
  - Trusted Path Services at Server
  - Distributed TCB to Client Locations
    - Trusted Path Extensions (TPE) at Clients
  - Controls TPE Activities
- Secure Session Services
  - Launch Applications at Corrected Session Level
- Dynamic Security Services
  - Policy Management Initiator
- Dedicated and Multiplexed Connections to Single Level Networks

Server Application Enhancements

- Ports of Popular Applications
  - All Made "Multilevel Aware"
  - HTTP: Apache-like Web Server
    - Base – standard Apache – minor modifications
    - WebDAV under development
  - SMTP: Sendmail
  - IMAP: University of Washington
  - NFS: User-level port
  - Secure Shell: OpenSSH (Single Level Only)
- Remote Client-Side Applications Support

High Assurance Trusted Path/Channel

- Trusted Path Extension Device
  - Ensure Communication with Trusted Server
  - Based on EAL7 Trusted Computing Exemplar (TCX) Separation Kernel
- Remote Security Operations
  - Log-on, Session Level Negotiation, etc.
- Server Supports Session Suspension and Resumption
- Trusted Channel Module
  - Ensure Proper Security Level Assigned To Information From Legacy Networks
- Dynamic Security Services Responders

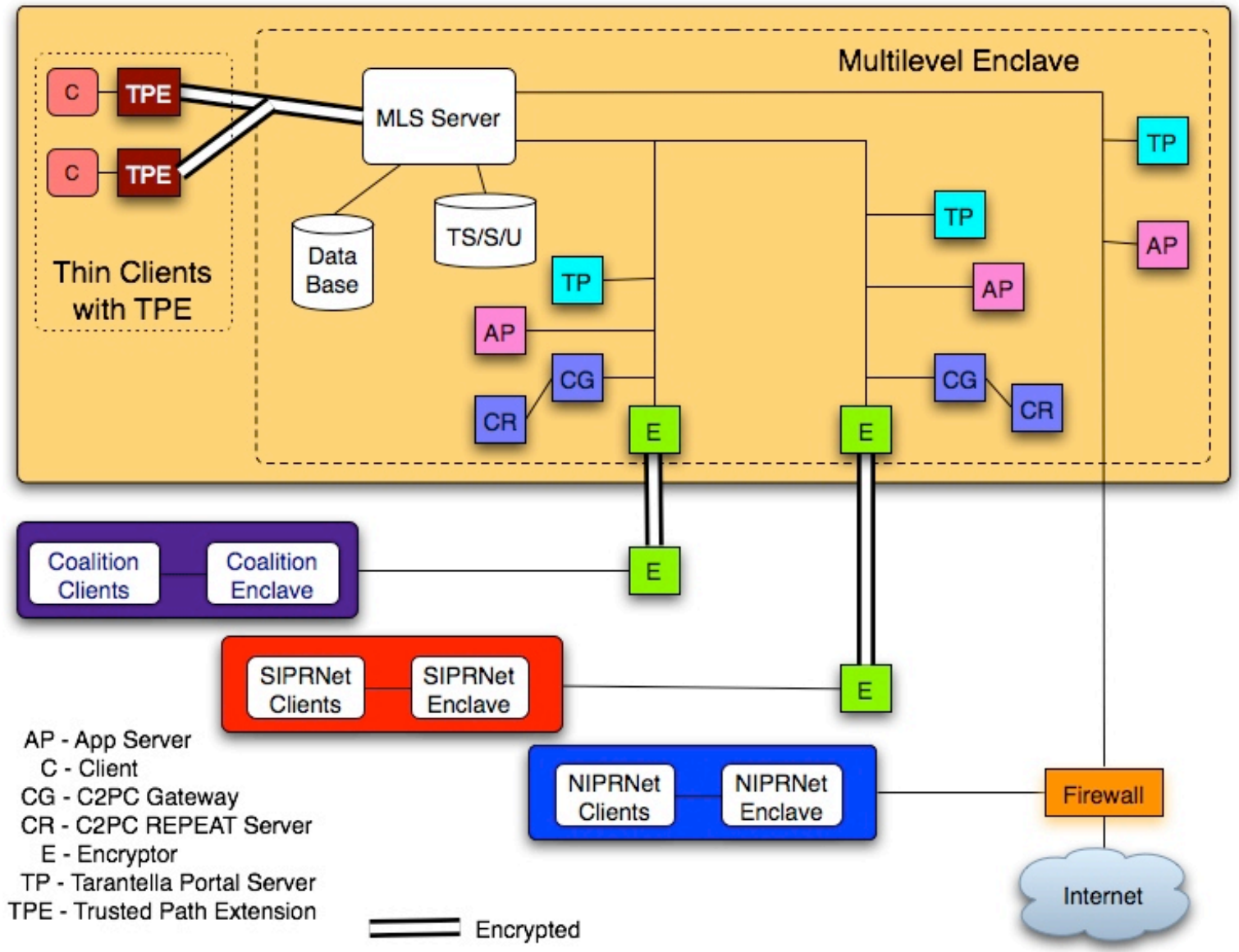
Commodity-Based Client

- Meet User Requirements
  - Web Browsing
  - Mail
  - Document Production
- Stateless To Address Object Reuse Requirements
  - Depot-level Configuration to Start Up in Useful State
  - Volatile Memory Only
  - Store State at Server at Appropriate Session Level
  - Working Prototypes:
    - Knoppix Linux
    - Windows XP Embedded

Web Portal Services

- Allow Reach-Back to Single Level Legacy Networks via Web Browser
- Part of MYSEA's Stateless Client Strategy
- Tarantella/enView product suite
  - Allow Clients to Access Web-based Applications On Different Platforms (Windows, Linux, Unix)
  - Present Integrated Portal View To Users
- Support GCCS
  - Command and Control Personal Computer System (C2PC)

Testbed Phase I



Phase I Configuration (1 of 2)

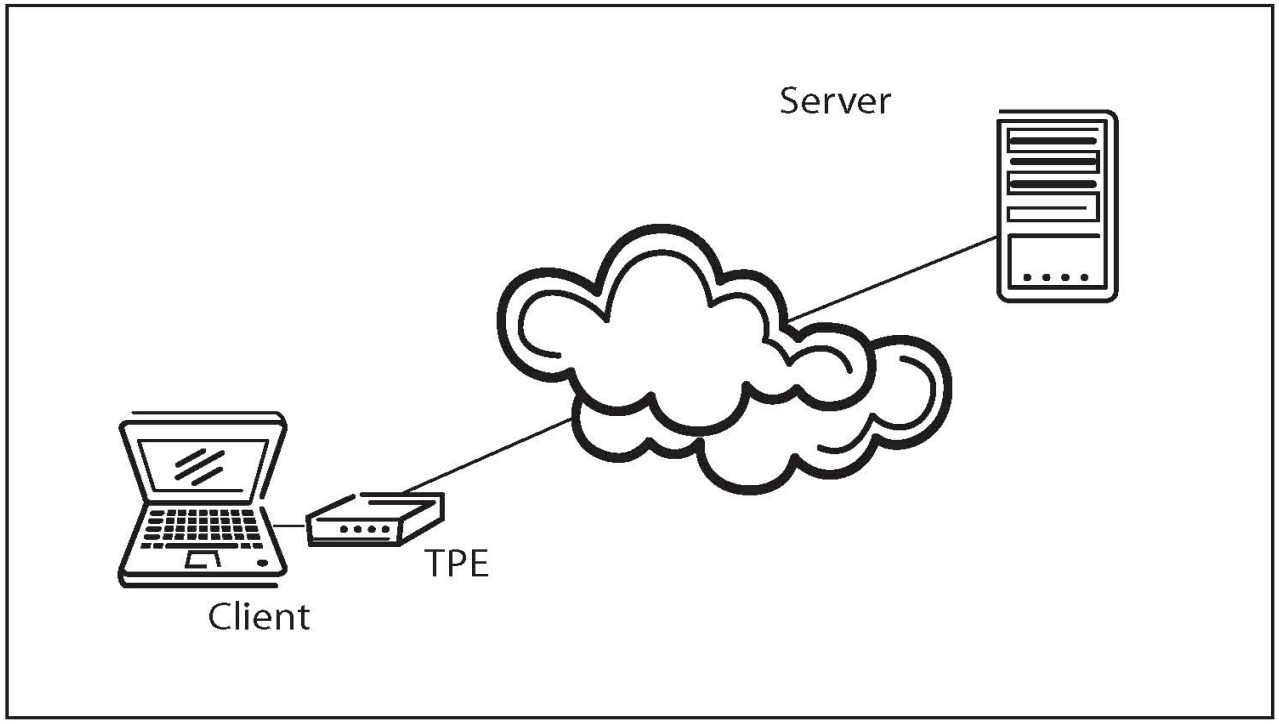
- Hardware: 35 components
  - MLS Server, Handheld TPEs, Desktops, Laptops, VPN Appliances, Network Switches, TACLANE Encryptors
- Operating Systems: Heterogeneous
  - Trusted OS: DigitalNet STOP
  - COTS OS: RedHat Linux, Microsoft Windows 2000 server, Microsoft Windows XP, Microsoft Windows XP Embedded, OpenBSD, Knoppix Linux and Familiar Project Linux

Phase I Configuration (2 of 2)

- Custom MYSEA Trusted Software
  - Trusted Path Service, Secure Session Management
- Linux Applications:
  - PostgreSQL, Apache web server, Edge Technologies enPortal, Tarantella Enterprise 3, imapd and sendmail
- Windows Applications:
  - Microsoft Terminal Services, Microsoft Office, Microsoft Project, Internet Explorer, C2PC Gateway, C2PC Client, REPEAT 2004–RepeatWinXR and Creative WebCam PROeX

Trusted Path Extension (TPE)

- Reference application for the TCX project
- Operational Environment - MYSEA MLS LAN
- Architecture will use separation
  - Untrusted and Trusted processes



TPE Form Factor

- PDA-like device
- Isolation from COTS processor
- Trusted Path functions control I/O to user
  - Device Screen
  - Device Keyboard
- Secure Attention Key design is simpler
- Encryption is on TPE
- Alternative: examine complex interactions between TPE and COTS system
  - Strong isolation is required for assurance

Questions and Contacts

Cynthia Irvine, Ph.D.
Center for Information Systems Security Studies and Research
Computer Science Department
Naval Postgraduate School, Monterey, CA 93943

irvine@nps.edu, 831 656-2461