The Naval Postgraduate School
Multilevel Secure Local Area Network
Project

Presented to WISAC
26 September 2000

Dr. Cynthia Irvine, Director
Center for INFOSEC Studies and Research
Code CS/1c, Computer Science Department
Naval Postgraduate School, Monterey, California, USA
http://cisr.nps.navy.mil/
(831) 656 2461  irvine@cs.nps.navy.mil

Topics to be Covered

• Motivation
• NPS MLS LAN Architecture
• Protocols
• Trusted Services
• Application Services
• Future Work
**Motivation: Security**

- Policy
  - Mandatory and discretionary access control
  - Object Reuse
  - Identification and Authentication
  - Audit
- Support needed integrity policies
- Concurrent access to multiple secrecy levels
- Connectivity to shared resources
- System Architecture
- Assurance of security policy enforcement

**Motivation: Productivity**

- Single desktop system.
- User-friendly interface.
- Support for popular application protocols.
  - E-Mail, File Services, Directory Services, etc.
- Latest commercial application software.
- Up-to-date popular PC operating systems.
- Commercial PCs.
- Simple TCB interface.
- Low cost solution.
Why Worry About COTS-Only Solutions?

- Subject
  - Address space and execution point
  - Rules adjudicate access to system-controlled resources
- Discretionary Access Controls
  - Permit subjects to modify access permissions
- COTS Software
  - Untrustworthy
  - May modify permissions unexpectedly
    - Result: Security Policy Violation

DAC-Only COTS System Vulnerability: Data-Driven Attack

Data-Driven Attack inserts Trojan Horse. Good user unaware of "behind-the-scenes" system corruption and exfiltration of sensitive information.
Oil and Water?

- Disadvantages of Most Secure Products
  - Lack of Useful Application Suites
  - Expensive
  - Inflexible
  - Difficult to Administer

- Disadvantages of Most COTS Products
  - Lack of Mandatory Policy Enforcement
  - Little Assurance of Correctness
  - Unevaluated

MLS LAN Architecture
NPS MLS LAN: High Assurance Server Base

- Evaluated Product
  - Wang XTS-300, TCSEC Class B3
  - Uses Government Investment in Assurance
  - Locus of policy and accountability enforcement

- Enhancements Required
  - Server Support
  - LAN-based Trusted Path
  - Multilevel Ethernet

- Architectural Analyses, Requirements and Tests by
  - Cpt Jason Hackerson
  - LT Steven Balmer

NPS MLS LAN: Client Workstations

- COTS Hardware Platforms
- COTS Operating Systems
- COTS Office Productivity Software
  - Runs session level “as usual” at PC
    - Attachment of local files
    - Security protocols
    - View of mail constrained by TCB
- Read-only disks for software
- Read-Write disks purged
NPS MLS LAN: TCB Extension (TCBE)

- Secure Boot at PC Workstation
- Assurance of Trusted Communications
  - Trusted Path services
    - Secure Attention Key
    - Reliable Capture and Display for User Interface
  - Session support
  - Modular cryptographic support
- Prevent Unauthorized Storage at PC
  - Inter-Session Purge Prevents
    - Trojan Horses stored between sessions
    - Sensitive information leakage

TCBE Requires Hardware Support

- Non Bypassable
  - Constrains Untrusted Workstation
- Self-Protecting
  - Secure Initial State
- Always Invoked
- Protects keys, passwords, etc.
TCB Extension in Context

Desired TCB Extension Features

- PCI Bus and NIC interfaces
- HD Controller for OS delivery/Control
- State-of-the-art Cryptographic capabilities
- Keyboard/Display for SAK and I&A
- BIOS Control for High integrity Bootstrap
- TCBE Analysis and Experimentation
  - LT Cihan Agacayak
  - LT Bora Turan
MLS LAN Protocols

Protocol Requirements and Specification

- Requirements & Specifications by LtCol JD Wilson
- Protocol for Secure Attention Key Delivery
  - Platform identification
  - Trusted Path Initialization
- Trusted Interaction Channel
  - Supports trusted path operations
- Protected Communications Channel
  - Protects session
  - IPSec and IKE considerations
Ethernet Trusted Services

- Initial Work by LT Scott Heller and LT Susan Bryer Joyner
  - Ethernet Secure Attention Key Services
  - Preliminary Identification and Authentication
  - Multilevel Ethernet Support
  - Single Level Session Server
- Many Enhancements by David Shifflett
  - Complete Identification and Authentication
  - Dynamic Instance Creation from Client
    - Full DAC support
    - Performance Improvements

MLS LAN: Multilevel Ethernet Services

- Connection Services
  - **TCB Extension Server**
    - Simultaneous trusted path connections for client TCBEs
    - Protocol for LAN-based trusted path
    - Framework to use trusted path for user I & A and session level negotiation.
  - **Protected Session Server**
    - Single level connection for client applications.
    - Framework for encryption services: Trusted path and application sessions
- Enhancements to XTS-300 TCB were required
Application Services

- Servers on High Assurance Base
- COTS clients on PCs
- Services
  - IMAP
  - SMTP
  - HTTP

IMAP Mail Delivery Agent (MDA) Server

- Internet Mail Access Protocol (IMAP)
  - Free software available from University of Washington
- Advantages Over Post Office Protocol (POP)
  - Mail left on server
    - Can be used by purged or thin clients
    - Stored mail controlled by server policy
- Port to Server by Major Brad Eads
- Capabilities expanded to read down
  - Required some modification of IMAP internals
- Full set of standard IMAP e-mail manipulation commands
IMAP Server to Client

- Tests with Mail User Agent Clients
  - Use of IMAP Messages of Mail Status by Clients
    - Better Human-Computer Interface
- Clients tested
  - Pine - good results
  - Lotus
  - Netscape Messenger
  - Postal (Java Client) - good results
  - Microsoft Outlook
- Work Completed by LT Theresa Everette
  - Also upgraded IMAP Server to latest release: IMAP4rev1

IMAP Administrative Tools

- Problem: Per Access Class Mail Folder Creation
  - At least one folder must exist
- Challenge: Minimize IMAP Modifications
- Choices:
  - Deflection Directories
  - User-Name/Access-Class
  - Access-Class/User-Name
- Administrator tool developed
- Completed by LT Richard Rossetti
SMTP Server

- Need Mechanism to Move Mail Within LAN
  - Existing XTS mail has limited capability
- Mechanism must support Mail and Attachments
- Need Mechanism to Move Mail Beyond LAN
  - Note: Communications Services also Required
- Simple Mail Transfer Protocol
  - Moves mail from one address to another
  - Provides mail transfer agent (MTA) instances in XTS-300

Port of Sendmail to Server

- Sendmail most popular SMTP server
  - UNIX-based
  - Supports sophisticated mail environments
- Port Completed by LT Emma Brown
  - Untrusted Sendmail instances
  - Newest version
  - Supports Mail and Attachments
  - Mail from clients using COTS MTA client software
    - Netscape Messenger
    - Microsoft Outlook
What About the Web?

- Modern Systems Need Web Services
  - Interface to Databases
- Hypertext Transfer Protocol (HTTP)
- Chose Apache Version 1.3 Server for Apache-Based Port
  - Most widely used server - over 60% of all servers
  - Porting kits available for numerous Unix platforms

Apache-Based Web Server

- HTTP/1.1 (RFC2616) compliant
- implements the latest protocols
- configurable and extensible with 3rd-party modules
- Use Apache module API to customize
- full source code and unrestricted license
- most versions of Unix
- active development
Apache-Based Port to High Assurance Server

- Port Completed by Evelyn Bersack
  - Graduation Date: December 2000
- Major Challenges
  - Modification of software generation ("make") files
    - Platform file system
  - Configuration
- Single Level Web Server Instances
- Currently in Testing Phase

Benefits of Our Approach

- Use Evaluated High Assurance TCB
- Leverage Existing Hardware and Software
- Understood Technology for Network Interfaces
- COTS Components
- Builds on Known Science and Engineering
- Highly Secure Multilevel System
- Office LAN Compatibility
- COTS Applications
- New COTS PC Applications easily Integrated
- Designed for Family of High Assurance Services
Future Work

- Read/Deleted Mail in Multilevel Environment
  - Modification to TCB File System
- Implementation of LAN Protection Protocols
- Implementation of TCBE Services
- Support of External Communications Services
- Support of Web-based applications

---

Seeing is Believing

Demonstration at
NPS CISR Open House

WHEN:  Tuesday, 26 September 2000
1730 to 1830
WHERE:  NPS Campus
        Building - Spanagel
        Room - 506