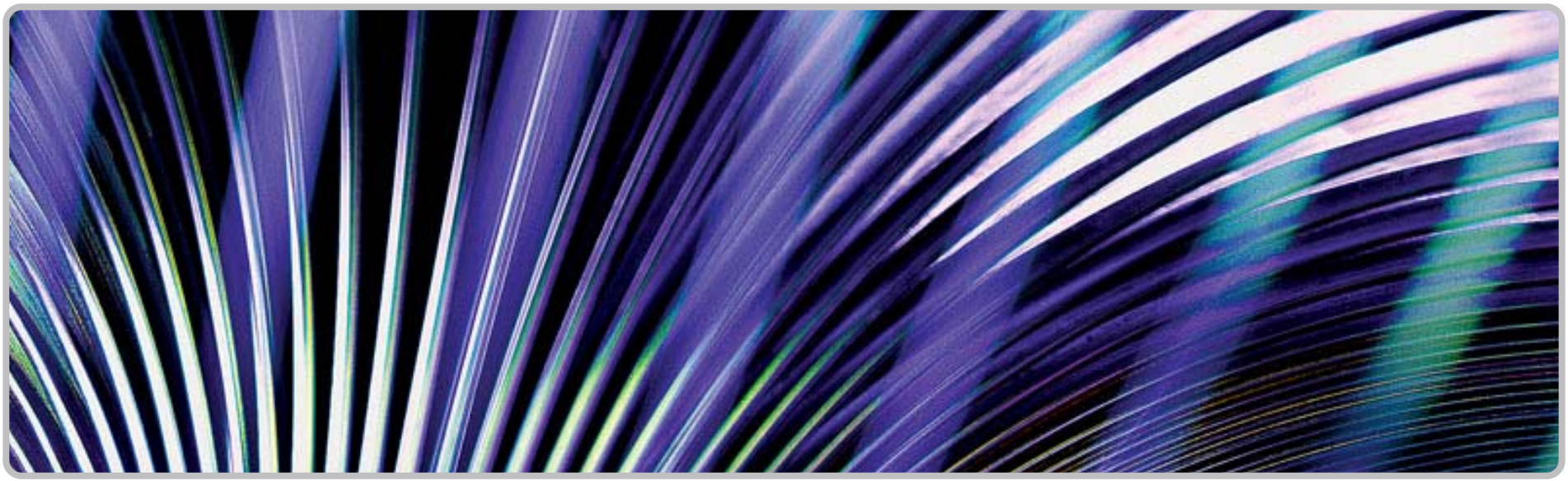


TRUSTED
COMPUTER SOLUTIONS

Trusted Computer Solutions
2350 Corporate Park Drive, Suite 500
Herndon, VA 20171

V: 703.318.7134
F: 703.318.5041
www.TrustedCS.com

SELinux Symposium Case Study

US Coast Guard
NetTop2 - Thin Client Implementation

March 15, 2007

Overview

- USCG Mission Statement
- Implementation of NetTop2 – Thin Client (NT2 –TC)
- Security Features
- C&A Status
- USCG Next Steps
- Lessons Learned

USCG System Mission and Impact Statement

- **Mission:** Coast Guard Intelligence analysts collect, produce, and disseminate foreign intelligence and counterintelligence to support warfighters in a timely manner.
- **Operational Requirement:** The Coast Guard is tasked to provide vital National Security mission-critical data to agencies such as the Commandant and Secretary of Homeland Security, the Federal Bureau of Investigation, and the Central Intelligence Agency. NetTop2 Thin Client will enable this mission-critical data to be disseminated in a timeframe that benefits US personnel who need this information while in harms way.
- **Mission Impact:** Lack of a cross domain solution like NetTop2 will result in vital intelligence products being pulled together manually–a time-consuming process. Where minutes can be crucial, this manual process leads to obsolete data being used by warfighters providing security of international waters and America's coasts, ports, and inland waterways. The result of which could be exposure of our warfighters and the citizens they defend to terrorist activities.

Current US Coast Guard Problem
Information Access and Transfer

Courtesy of NSA

Consolidation Approach
Information Access and Transfer

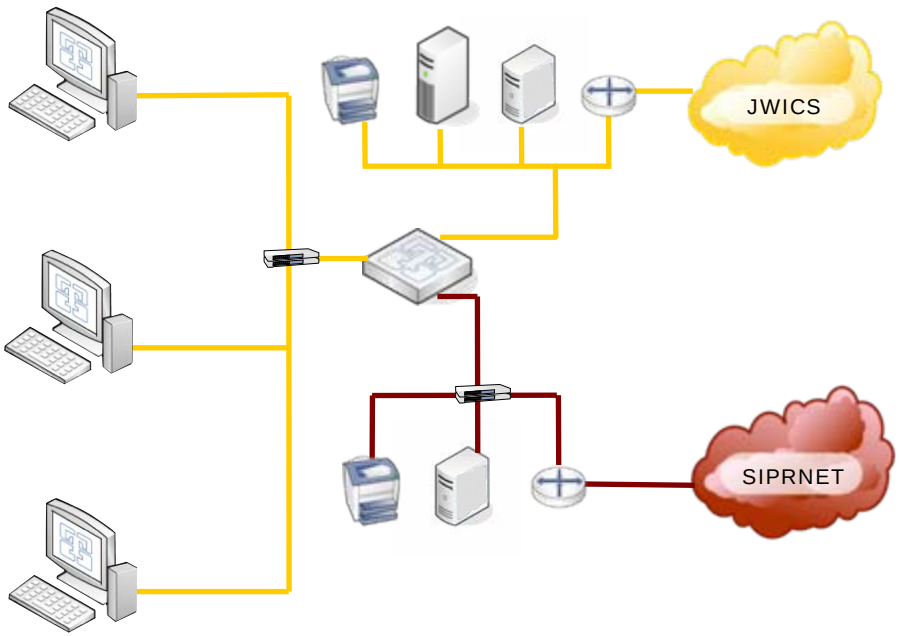
Courtesy of NSA

U.S. Coast Guard
SecureOffice NetTop2 – Thin Client

Homeland Security

United States Coast Guard

Semper Paratus



Coast Guard Intelligence Program (CGIP)

Offers simultaneous secure access to Microsoft applications running at different security levels from a single desktop that:

- Enhances interagency information exchange;
- Makes intelligence data sharing and dissemination seamless for production and tactical operations; and
- Furthers intelligence information sharing and collaboration with other Intelligence Community members.

September 2006: ATO issued in TSABI

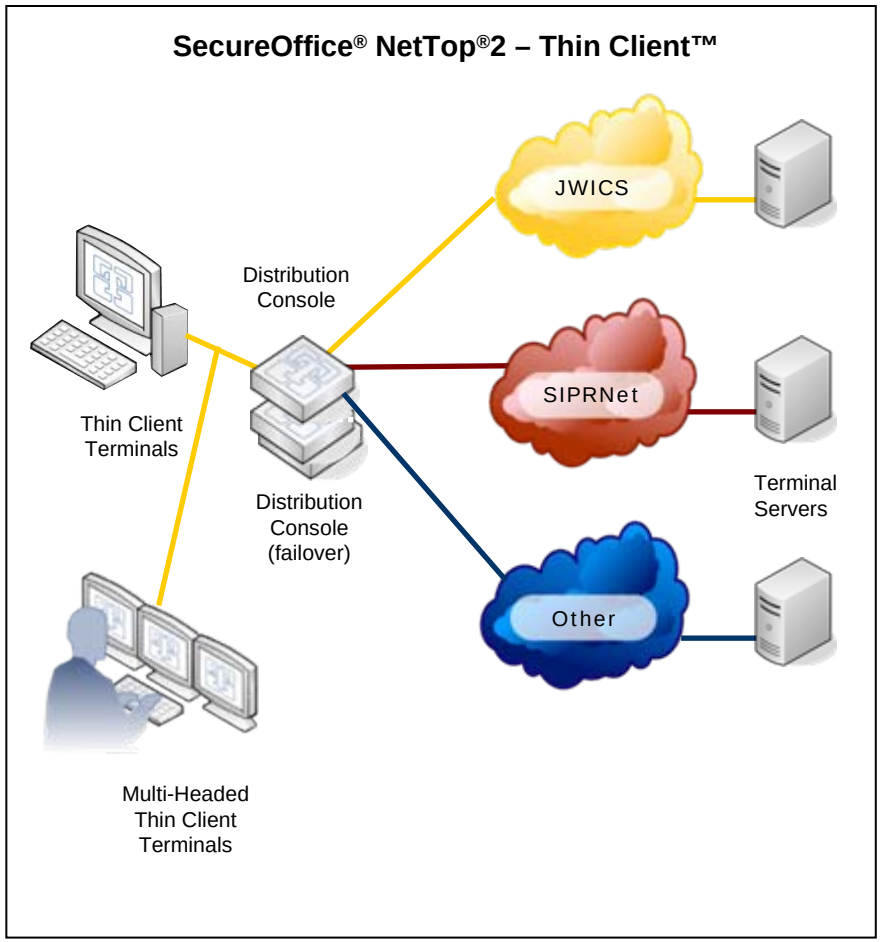
Source: U.S. Coast Guard Unclassified SSA

SecureOffice® NetTop2 – Thin Client
User Interface

UNCLASSIFIED -- Classification labels for example purposes only

SecureOffice® NetTop®2 – Thin Client™

Pushing Trust to the Edge



Multi-Domain Access in a Low Cost Thin Client Environment

Access functionality with Thin Client, and Linux Platform benefits

Features:

- Evolved from NetTop CRADA with NSA and work that originated from TCS Trusted Workstation – Thin Client (Trusted Solaris based, part of DoDIIS Trusted Workstation)
- Inexpensive commodity thin client appliances provide users with a multi-level display to networks operating at differing classification levels
  - Provides access to Windows applications via Citrix or rdesktop
- Distribution console functions similar to a security access point, multilevel router, and a configuration manager for the clients

SecureOffice® NetTop®2 – Thin Client™

Thin Client

User options include Thin Client appliances or Thin Client Laptop

- SELinux based system runs directly on Thin Client
- Thin Clients execute from Flash memory requiring no hard disk
- Authenticates with Distribution Console for access and configuration
- CAC compatible with optional Smart Card reader
- Low administration costs – flash at install
- Minimal user training – point and click ..
- Inexpensive appliances
  - neoware or WYSE
  - Multiple monitor support
- Standard PCs or laptops can also be used as thin client

SecureOffice® NetTop®2 – Thin Client™
Distribution Console

Distribution Console controls all networking and routing functions providing a secure gateway to single level networks

- SELinux based system
- Multilevel network gateway to single level networks
  - A NIC configured for each system high network
- Graphical Administration tools for system setup
- Maintains common configuration for Thin Clients
- Authentication server for Thin Client users
  - Replicates Active Directory usernames / passwords
  - Locally managed
- Audit server for Thin Clients and Distribution Console
- Easily supports a C-class network with a single Distribution Console
- Automatic failover and “load distribution”
- Runs on Linux-compatible hardware
  - From a 1U rack mountable to desktop servers
  - IBM xSeries the Target Operating Environment for Common Criteria and TCS certified for NetTop2 operation

SecureOffice NetTop2
TC and DC Common Security Features

- SELinux based systems
- Appliance model
- Controlled interface; not a cross domain solution – does not pass data between levels
- Secured with both Type Enforcement and MLS Policy
- Supports MITRE label encoding format
  - Clear concise labelling
- Added support for multilevel X windows
- Minimal administration with graphical interface (no command line and no Trusted Linux knowledge required)
- Automatic configuration of IP based firewalls and SELinux Policy on both the TCs and DC
  - Limited to only those hosts required for operation
- Strong passwords, auditing, etc per DoD security requirements
  - DCID 6/3 PL4 and SABI compliance at both the operating system and application
- File integrity check

Thin Client Security Features

- Stripped down SELinux based system, running directly on Thin Client
- SELinux enforcement cannot be disabled
- Executes from FLASH memory
  - SELinux based OS converted to a read-only file system
  - Less then 400 MB and validated at startup
  - Minimal user functionality – limited to accessing existing MS Windows servers
- Multilevel Device allocation with GUI
  - Audio and CAC reader
- Limited functionality led to ease of evaluation and testing (from security point of view)
  - No command line access
  - Only Citrix or rdesktop applications available
- No read down or write up between Citrix or rdesktop applications (type enforcement)
- No data stored on the Thin Client (only the “image” of application and data being remotely displayed)
- Encrypted communications between Citrix and rdesktop clients and servers
- No administrator access (local or remote)

Distribution Console Security Features

- DC provides secure multilevel data exchange between NetTop2 TCs and authorized dissimilar single level Windows networks
  - Strong encrypted communications between TCs and DC – IKE and IPSEC with 256 bit keyed AES
  - Single multilevel network connection between TCs and DC
    - CIPSO, moving to labeled IPSEC
  - Each external network is connected to the DC with a dedicated NIC
- “Authenticates” Thin Client by confirming configuration, MAC address, and certificate
- Audit aggregator for TCs and DC
- Updates (new levels and servers) automatically grabbed from TCs
- Automatic SELinux policy creation (passes to the Thin Client)

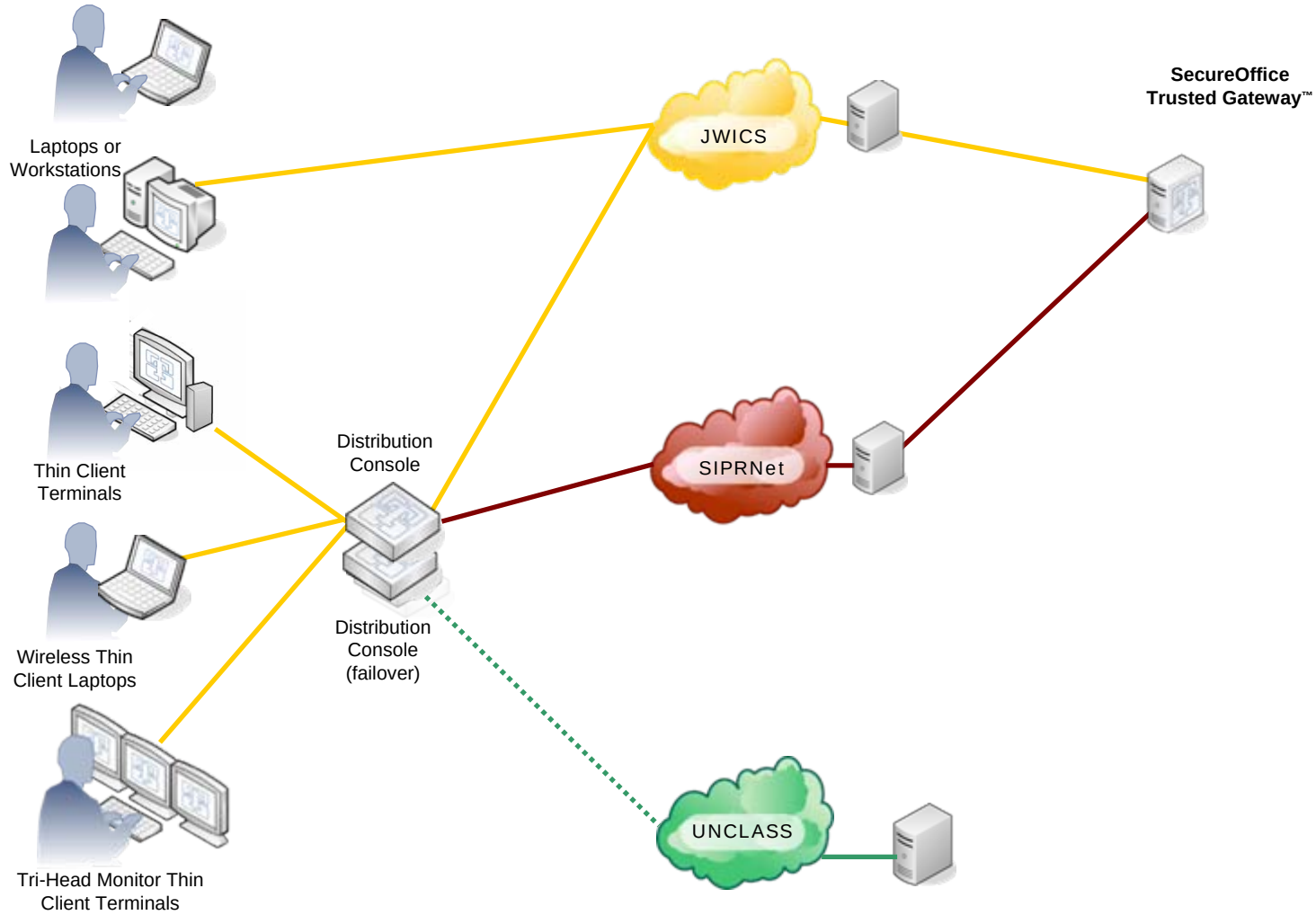
Certification and Accreditation Status

- For TS and Secret Connectivity
  - TSABI - DCID 6/3 process
    - SSAA Documentation and CT&E test cases completed
    - Beta 1 and Beta 2 testing completed by DIA
    - Awarded an ATO in Sept 06
    - System now in operation
- For Secret to Unclass Connectivity
  - CDS (SABI) – DIACAP process
    - Currently in Phase II
      - Phase I CDA complete
      - Awaiting to enter CT&E testing at NSA
      - Hope to complete sometime in ’07 (contact CG for exact details)

Next Steps

- Provide a cross domain transfer capability to facilitate the secure transfer of information
- Leverage off of DTW program for PL5 connectivity to Unclassified

USCG Integrated Solution – Next Steps



SELinux Lessons Learned

- SELinux based solution has demonstrated excellent performance, high security, ease of use, and hardware flexibility
- Solution utilizes both MLS and TE policy
  - Enhanced security
  - Familiar MLS look and feel
- Created “internal” tools until upstream support available
  - Necessary for initial productization
  - Now porting to latest release – RHEL5
- Open source benefits
  - Pros
    - Lot of tools available
    - Provide “most” functionality
  - Cons
    - Can be difficult to configure
    - May require modification desired functionality
- Features had to be added/modified
  - Trusted X-Windows
  - User friendly security labels
  - MLS policy
  - CIPSO networking

Others Lessons Learned

- SELinux provides the building blocks for enhanced security
  - Must be constructed to provide to meet user functionality and needed PL4 requirements
- Most users have no UNIX or Trusted OS experience
  - Client interface must be graphical and very easy to use
- Most Administrators have no UNIX or Trusted OS experience
  - Administration must be appliance-like
    - GUIs do everything
  - Some clients do not allow command access to their Admins
    - Cannot vi files, modify policy, etc
- When going through C&A process, security requirements take precedent over usability
  - Designed the system based on Intel/DoD security requirements
    - CC evaluation is considered, but the Intel/DoD security requirements must be met

Thank You

For Additional Questions, call:

George Kamis
CTO
(703) 537- 4310
kamis@TrustedCS.com

TRUSTED COMPUTER SOLUTIONS

www.TrustedCS.com