2005-06-00

MYSEA Testbed

Nguyen, Thuy D.; Levin, Timothy E.; Irvine, Cynthia E.

Proceedings from the 6th IEEE Systems, Man and Cybernetics Information Assurance Workshop, West Point, NY, June 2005, pp. 438-439.
https://hdl.handle.net/10945/7132

MYSEA Testbed

Thuy D. Nguyen, Timothy E. Levin, *Member IEEE*, Cynthia E. Irvine, *Senior Member, IEEE*
Computer Science Department, Naval Postgraduate School
833 Dyer Road, Code CS/Nt, Monterey, CA 93943-5118
tdnguyen@nps.edu, 831.656.3989, FAX: 831.656.3994

I. INTRODUCTION

The technical vision of the emerging net-centric Global Information Grid (GIG) encompasses support for high assurance authentication and multilevel security (MLS) as well as flexible, dynamic security policies. The GIG is intended to address the inefficient exchange of information in current military and intelligence operations that utilize a variety of specialized (so-called "stove-piped") systems. In this context, secure information access problems are exacerbated by the need to share information from networks at different classifications (e.g., Unclassified, Secret, and Top Secret) and within multinational coalitions in episodic, ad hoc situations.

These challenges provide the impetus for the creation of the Monterey Security Architecture (MYSEA) Testbed. The purpose of this Testbed is to support research in high assurance multilevel security (MLS) [1, 2] and dynamic security, two areas that are critical to the realization of the GIG's assured information sharing vision.

The MYSEA Testbed is an evolving environment that facilitates experimentation with the following (* denotes a future experiment):

- Assured authentication and trusted path access to MLS services
- Application of high assurance system-security technology to the integration of commercial and legacy components
- Centralized security management
- Integration of high assurance multilevel security with existing sensitive networks
- High assurance trusted communication channel techniques for managing access to classified networks
- Use of open architectures and standards
- Use of XML tags as security markings
- Secure single sign-on across multiple MLS servers
- High assurance component authentication and attestation*
- Secure collaborative information sharing*

Our experience to date regarding the construction of a test facility for high assurance MLS components and other emerging IA technologies associated with the GIG is summarized here. We have used the GIG as an exemplary framework, but any extended, rapidly evolving enterprise (e.g., government, or commercial) with information assets having a range of value and criticality as well as a range of users with different authorizations will have similar requirements.

This work was sponsored in part by the Office of Naval Research and the National Reconnaissance Office. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of either the Office of Naval Research or the National Reconnaissance Office.

II. TESTBED DESIGN OVERVIEW

The Testbed design is shown in Figure 1. The near-term goal is to demonstrate how U.S. participants can use a single commercial workstation for access to multilevel enclaves as well as to U.S. and coalition networks at different classification levels. Demonstration scenarios on the Testbed show that it is feasible to afford unmodified, popular desktop applications, e.g. the Microsoft Office suite, to clients in a MLS/Multiple Security Level (MSL) environment and to provide users within a community of interest network with web-based views of multilevel information.

Using predominantly COTS components, the Testbed provides an experimental environment for the following functionalities:

- True multilevel access to data at multiple levels of security using a single commercial workstation,
- Single-level-at-a-time access to sensitive single level networks (e.g., Unclassified and Secret enclaves) using a single commercial workstation,
- Use of heterogeneous operating systems, hardware components and applications,
- Use of a high assurance server as the locus of security policy enforcement,
- Use of hand held appliances for trusted path support
- Controlled interaction of disparate coalitions and enclaves, and
- Controlled Internet access.

Although Figure 1 shows only one MLS server, the MYSEA design supports a federation of MLS servers for better performance, scalability and reliability. The MYSEA server (hosted on an XTS-400) enforces a unified mandatory access control security policy, viz., confidentiality and integrity. The Trusted Path Extension (TPE) device is responsible for providing a secure interface for user interaction with selected MYSEA server security functions. After a successful login and session level negotiation via the trusted path, an MLS LAN user can access any data at the MYSEA server to which he is authorized by the security policy. The current MYSEA security policy allows reading information that is at the same or lower in sensitivity than the negotiated session level. All

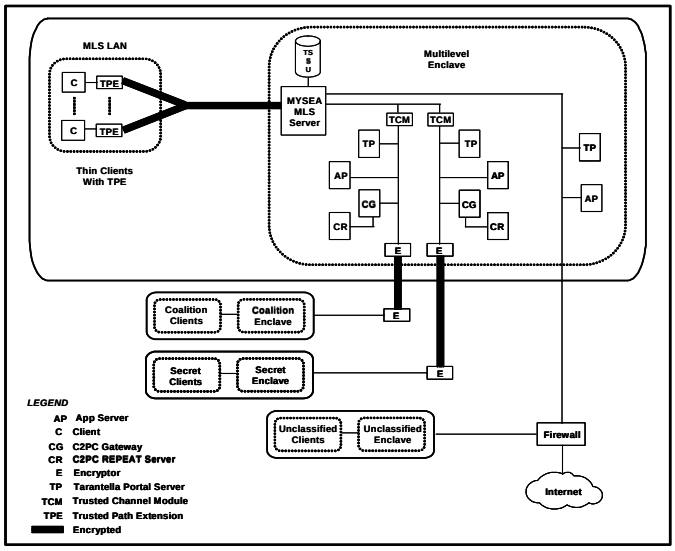

Figure 1. Testbed Topology

information written will be labeled at the negotiated session level.

Similarly, the Trusted Channel Module (TCM) device is a trusted component responsible for providing secure identification of single level networks connected to the MYSEA server. When one or more networks are connected to the MYSEA server via a given TCM, the network users can only access data on the MYSEA server at the classification level assigned to that TCM.

The Testbed is isolated from our campus intranet as well as the Internet, except for selected test scenarios that demonstrate access to the Internet.

III. ACCOMPLISHMENTS

Under development since 2004, the MYSEA Testbed is being constructed in phases. This section summarizes our accomplishments in the initial phase.

The MYSEA server in the Testbed is currently configured to run an Apache-like web server, and modified *sendmail* and *imapd* mail servers. After a successful login to the MYSEA server at an authorized session level via the TPE, a user on the MLS LAN can view web pages at the same or lower sensitivity level. The user can also exchange email with other users who are logged in at the same session level, and can read email at lower sensitivity levels that has been previously downloaded into the user's local mail storage. Furthermore, the user can run the following COTS applications via an integrated web portal interface: MS Office suite, MS Project, MS Outlook Express, C2P2 Client (running as a remote application on a remote application server).

The web portal server (currently Tarantella) provides to MLS LAN clients, via an integrated portal view, web-based applications that run on different server platforms (Windows, Unix, Linux). This permits the use of standard web browsers to access proprietary applications on the simulated legacy networks, e.g., Project or PowerPoint. The inclusion of web-enabling technology is part of the MYSEA's thin-client migration strategy.

The Command and Control Personal Computer (C2PC) system, a battlefield situational awareness tool, is used in the Testbed to demonstrate the ability to support existing mission-critical applications. The C2PC REPEAT track simulator feeds simulated tactical information to the C2PC Gateway and C2PC Clients. The C2PC Gateway provides tactical track data received from the REPEAT server to the C2PC Clients and forwards track updates from the C2PC Clients back to the REPEAT server.

Both military-grade Type 1 encryption devices (TACLANE encryptors) and commercial VPN appliances are used in the Testbed to simulate the protected end-to-end communication between the MLS controlled environment and remote single level networks. Two pairs of TACLANE encryptors with dummy test keys are used to simulate the encrypted channels required to protect data transmissions between networks that are geographically separated. For day-to-day testing, two pairs of Cisco IPsec VPN devices are used in place of the TACLANE devices, which require special handling.

A strict life cycle process has been put in place to provide stability and repeatability for tests and experiments. Only authorized personnel are granted access to the Testbed, and only stable hardware components and software releases may be installed on the Testbed. Changes to the Testbed undergo an extensive series of regression tests.

IV. FUTURE PLANS

In addition to conducting performance measurement and analysis to assess the overhead costs of the custom software, we also expect to incorporate into the Testbed the following functionalities that are currently under development:

- MLS services: NFS and SAMBA support
- "Stateless" MLS LAN clients with persistent user data and metadata stored on the MYSEA server
- Support for running remote client applications on the MYSEA server
- Provision of secure remote shell capability to both local and remote clients
- A proof-of-concept TCM prototype
- IPsec-based dynamic security services

V. REFERENCES

[1] Irvine, C. E., Levin, T. E., Nguyen, T. D., Shifflett, D., Khosalim, J., Clark, P. C., Wong, A., Afinidad, F., Bibighaus, D., and Sears, J., "Overview of a High Assurance Architecture for Distributed Multilevel Security," *Proceedings of the 2004 IEEE Systems Man and Cybernetics Information Assurance Workshop*, West Point, NY, June 2004, pp. 38-45.

[2] Irvine, C. E., Levin, T. E., Nguyen, T. D., and Dinolt, G. W., "The Trusted Computing Exemplar Project," *Proceedings of the 2004 IEEE Systems Man and Cybernetics Information Assurance Workshop*, West Point, NY, June 2004, pp. 109-115.