MULTI-LEVEL SECURE ENCRYPTION FOR DISTRIBUTED SIMULATION

APPLICATION OF FORTEZZA TO DIS

Carl Muckenhirn - SPARTA, Inc., Columbia, MD
Amitabh Dey, Jim Watson, Hector Correa - SPARTA, Inc., Orlando, FL
Mike Garnsey - STRICOM, Orlando, FL

ABSTRACT

Realistic combined arms training and mission rehearsal, particularly at the command level, often requires the use of classified information. Typically such exercises are performed in system high security enclaves that do not accurately represent the battle space. The ability to train in a multi-level secure distributed simulation environment would permit a more realistic emulation of real warfare which is increasingly influenced by information warfare. A concept for implementing encryption to support multi-level secure distributed simulation is described. The concept makes use of hardware and software components developed as a part of the National Security Agency sponsored Multi-level Information Systems Security Initiative (MISSI). A principal element of the concept is the securing of sensitive information at the point of origin through encryption at the application level. This represents a major shift from the usual bulk encryption at the system high enclave boundary and potentially makes possible multi-level secure information flow within a simulation as well as between distributed enclaves at differing levels of security.

The scope of this paper is focused on the technical feasibility of application level information encryption within a distributed simulation and between distributed simulation sites. Security issues associated with setting up and processing secure information flows within a distributed multi-level secure network configuration are addressed; however, it is assumed that a common security policy has been defined satisfactory to participants operating at differing security levels within the distributed simulation federation.

A planned international demonstration of the Fortezza-based MLS concept is described. The demonstration will consist of a simple military battle interaction between three widely distributed MODSAF simulation workstations, two located in the United States (STRICOM and SPARTA in Orlando, Florida) and the third in Europe (TNO-FEL in the Netherlands). Selected data labeled and handled as secure during the simulation execution will only be viewable at certified locations. Projected estimates of the effect of Fortezza response on the interactive simulation are presented and implications discussed.

AUTHORS' BIOGRAPHY

Carl Muckenhirn - SPARTA Chief Engineer for NSA MISSI Program. MISSI objective is to provide a comprehensive multi-level secure solution for government and commercial applications. Principal developer of the application level encryption concept for MLS.

Amitabh Dey - Chief Engineer of SPARTA DIS Directorate and technical lead of the network MLS demonstration. Developer of first web-based distributed simulation database (SIMWORLD Prototype).

Jim Watson - Manager of SPARTA DIS Directorate and principal developer of the network MLS demonstration concept. Technical Manager of SPARTA DIS projects under STRICOM's ADST I Program. SPARTA PM for Joint SIMulation System (JSIMS) Program.

Hector Correa - SPARTA Staff Engineer responsible for MODSAF to FORTEZZA Interface.

Mike Garnsey - STRICOM COTR and international liaison for the MLS Concept Development BAA project.

MULTI-LEVEL SECURE ENCRYPTION FOR DISTRIBUTED SIMULATION

APPLICATION OF FORTEZZA TO DIS

Carl Muckenhirn - SPARTA, Inc., Columbia, MD
Amitabh Dey, Jim Watson, Hector Correa - SPARTA, Inc., Orlando, FL
Mike Garnsey - STRICOM, Orlando, FL

INTRODUCTION

To date, security for distributed simulations has been relegated to a network service. In order to meet the demands of simulation architectures such as the DMSO HLA security should be exercised closer to the actual consumers and producers of sensitive–and potentially classified–information. Eventually, support of multi-level simulations (a single simulation operating on, and producing, information at more than one security level (classification, compartment, caveat) will require the simulation (or a simulation framework) to directly access or perform security services.

The National Security Agency's Multi-level Information Systems Security Initiative or MISSI, is producing technical security solutions which may be applied to the modeling and simulation problem. Of particular interest is use of the Fortezza CryptoCard to secure modeling and simulation applications.

The objective of this paper is to describe a concept and demonstration of multi-level secure encryption at the application level supporting a multi-level secure distributed simulation. How this capability could enable multi-level distributed simulation for training and mission rehearsal applications is also discussed.

STATEMENT OF THE PROBLEM

For some time, DIS exercises have been limited by various security issues. These have ranged from pedestrian concerns about the performance of particular security equipment, to critical concerns of classification and security accreditation mis-matches between environments. Segregation and isolation of information among exercise participants is also a major concern. Segregation may be needed due to national policies (i.e., US NOFORN restrictions) or proprietary concerns.

In discussions with SPARTA, STRICOM expressed a desire to provide a security solution which will allow US and allied simulation activities to execute cooperative exercises containing sensitive information over unprotected networks. In particular, STRICOM is working with its British and Dutch counterparts and would like to provide a method of protecting information exchanged among the parties as well as allowing parties to restrict access of the other parties as needed.

The immediate problem is to provide a protection mechanism, without export encumbrances, to US allied simulation activities. This mechanism must provide to the participants the ability to securely share information (ultimately classified information).

BACKGROUND

NSA's Multi-level Information System Security Initiative, has developed key components and software to meet multi-level secure information system requirements for the operational forces. Concepts, hardware and software are now coming available which will also enable a multi-level secure training environment. Development of the distributed simulation application using MISSI program components is being undertaken as a part of STRICOM concept development efforts and is projected to enable similar MLS capabilities in the JSIMS and NASM distributed simulation systems.

Current M&S Security Approaches

Current practice within the DoD modeling and simulation community for protection of classified activities fall into three basic camps. The first is the traditional DoD isolation of the classified computation within a physically secured enclave. The systems, if more than one is involved, are interconnected via standard networking technologies and they all operate in a "System High" or "Dedicated" mode (see Figure 1).

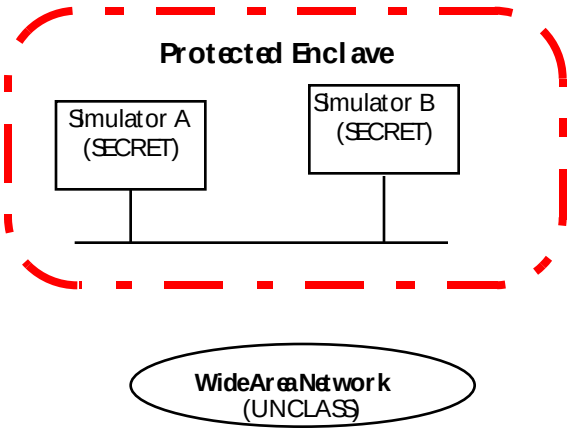


Figure 1. System High Protected Enclave Network

This approach requires that all players in the exercise be cleared to the same level. For many activities this is not an issue, but for large exercises, requiring many players, possibly from allied or coalition, the ability to clear all players for all information in the exercise may not exist.

The next approach basically extends the boundaries of the "protected enclave" through the use of encryption devices on a point to point basis. This is the model employed by the Warbreaker system. In this case, again, all simulations operate at the same classification level in either a "System High" or "Dedicated" mode (see Figure 2). This model can provide good performance for distributed simulations, but at the expense of dedicated telecommunications circuits between participating enclaves. For example, existing encryption devices (such as the KG-81, and KG-19x) can be used to protect channels at speeds up to DS-3 (45 Mbps), but a separate channel is required between each site with two encryptors on each link.

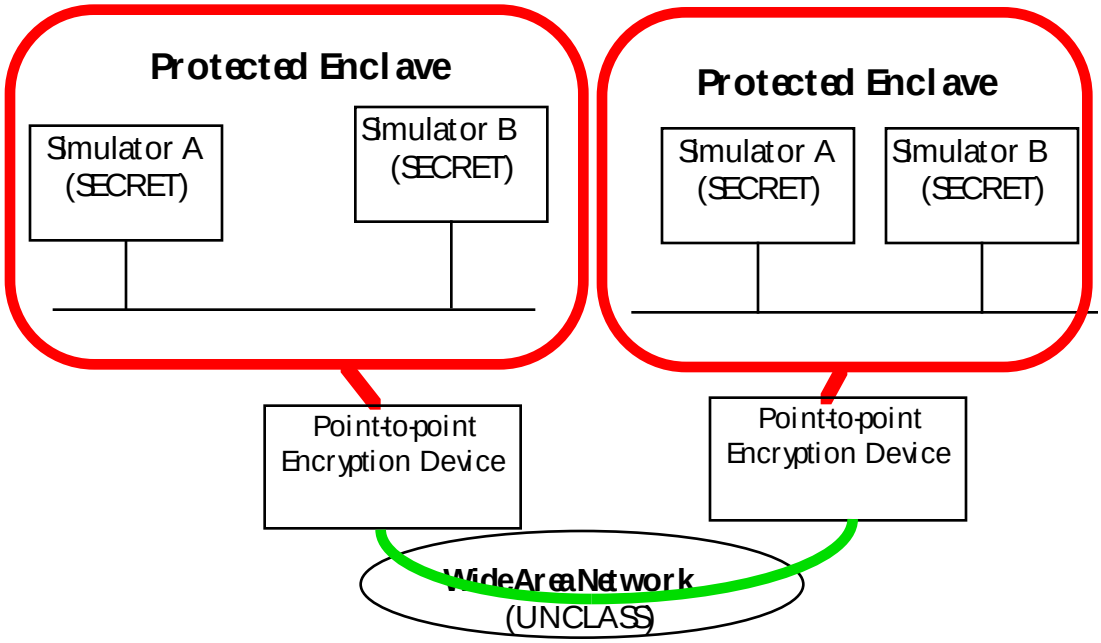


Figure 2. System High Interconnected Enclaves

The third security option is that employed by the Defense Simulation Internet (DSI). This approach is basically an extension of the second approach with protected enclaves interconnected over networked connections rather than point-to-point connections (see Figure 3). Theoretically this architecture provides the ability for distributed simulations to interact with an arbitrary number of protected enclaves through the use of a single network connection and single network encryption device. This approach also holds the prospect of supporting multicast network transport. In practice this has not been as successful as possible due to limitations of the available network level encryption systems and the expanding demands of DIS simulation activities. In addition to the currently experienced performance problems, this architecture still does not provide any protection beyond the "enclave" level.

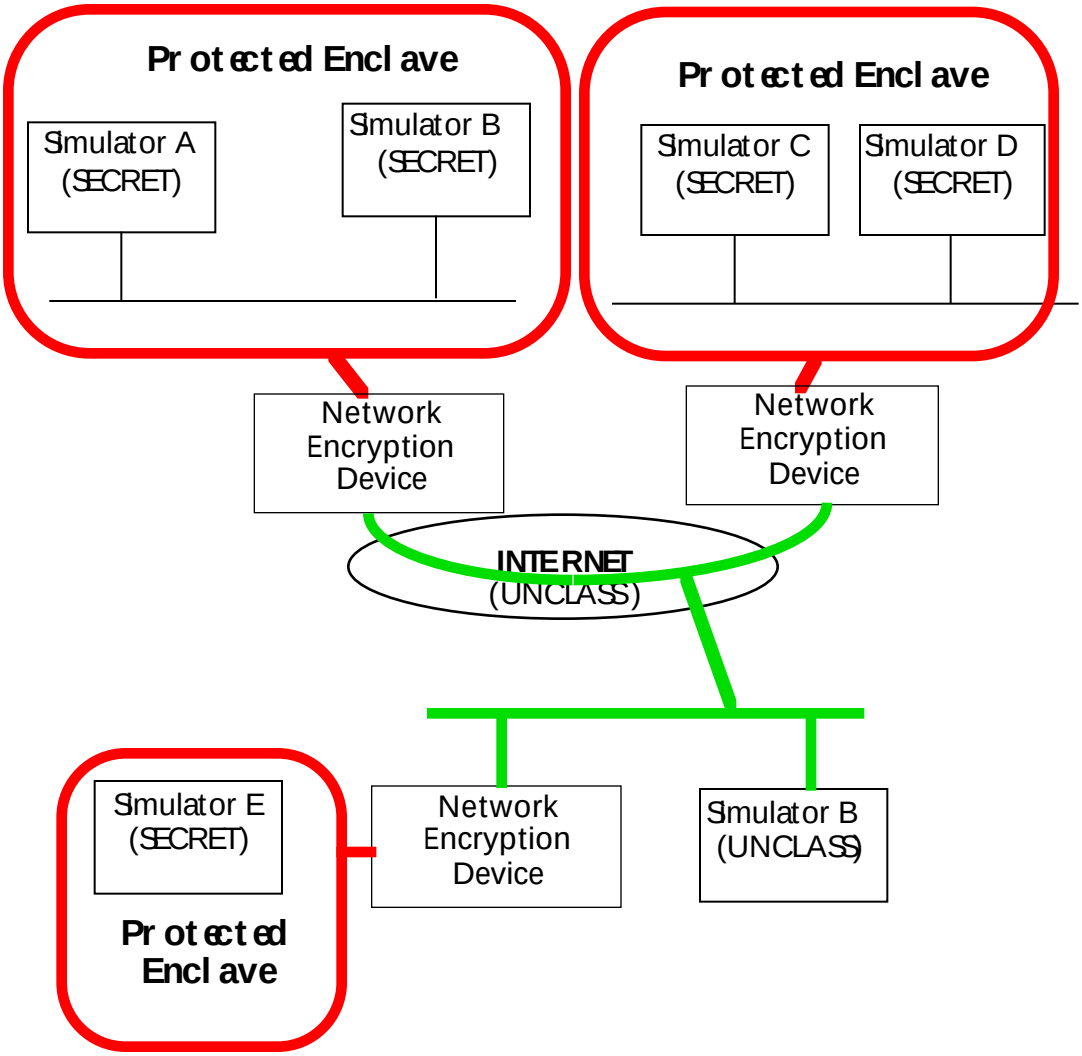
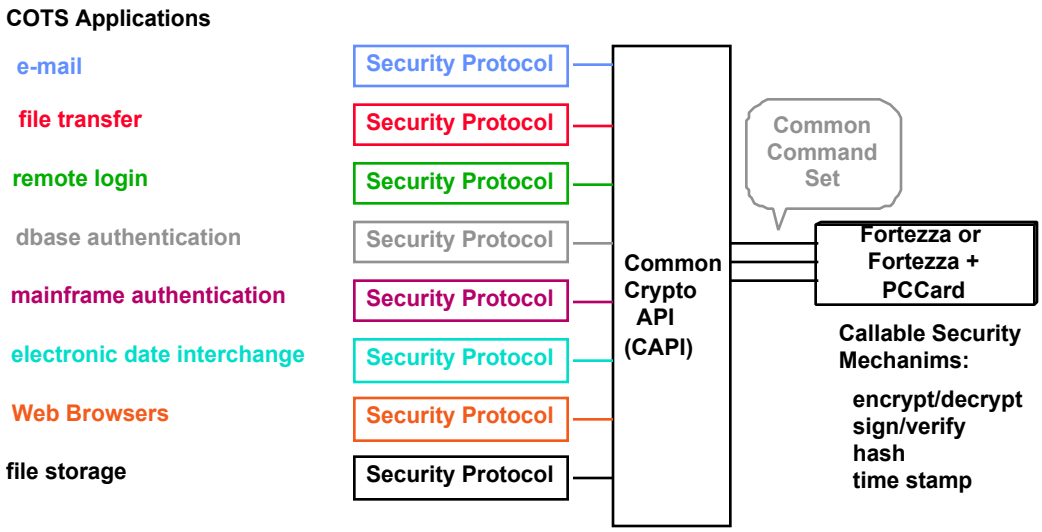


Figure 3. DSI/Networked Encryption Model

In the case of the DSI model, the DSI network can support (from a security viewpoint) multiple simultaneous, but non interacting, simulation exercises at differing security levels. While this is an advance and allows for more widespread use of the DSI infrastructure, the security limitations still require each participant in an exercise to be cleared to the same level. The remainder of this paper describes the current state of the art in security technologies and how they may be applied to M&S activities to achieve more realistic and hopefully more effective training.

MISSI APPLICATIONS LAYER CRYPTO CONCEPT



Security Technology State of the Art

The National Security Agency's (NSA) Multilevel Information Systems Security Initiative (MISSI) is aimed at providing security solutions to a wide variety of DoD information systems applications. Implementation of the security solutions is accomplished through the use of several "building block" security products.

Cryptographic Card Building Block Products

PC Card (PCMCIA) format cryptographic devices which are used in this project provide data encryption/decryption, data integrity, user identification and authentication, and user non-repudiation functions. There are two basic versions: Fortezza – for use in sensitive but unclassified (SBU) environments and Secret environments under certain circumstances; Krypton – for all levels of classification, with implementation restrictions.

A wide variety of applications have been enabled to use the Fortezza card, including:

- e-mail
- file transfer, storage
- EDI/EC
- remote login
- search/retrieval
- dbase access authentication
- World Wide Web

Secure Computing Building Block Products

Of particular interest to this project, cryptographic cards provide the ability to apply security functions and services to data at the application level. In order to obtain confidence that those services and functions are exercised as the application developer desires and user requires, secure computing products are needed. These products provide security functions including:

- data labeling and separation
- activity audit
- cryptographic card invocation, and

- verified system access.

As important as the functions provided, secure computing products also provide assurance that those services are correctly applied. These assurances are obtained at various levels, and are confirmed through independent evaluation of the products to the Department of Defense Trusted Computer System Evaluation Criteria (DoD 5200.28-STD), *a.k.a.* "The Orange Book." There are many secure computing products currently available including:

- Trusted Information Systems with Trusted MACH and Trusted Xenix
- Gemini GTNP
- Microsoft NT
- HP UX, BLS
- IBM MVS
- SecureWare SCO UNIX
- HFSI STOP XTS300
- Secure Computing Corp. LOCKix
- Sun Microsystems, Solaris Compartmented Mode Workstation

In addition to the Secure computing products, which provide generalized operating system services, there are several vendors, including Oracle, Sybase, and Informix, offering secure database products. These products are designed to provide security specifically within the database context and can be used to implement datacentric security policies. To be fully secure these products are designed to run on one of the above mentioned secure operating systems.

Firewall Building Blocks

Firewalls consist of components placed between two nets such that (1) all traffic passes through the components (2) only authorized traffic is allowed to pass and (3) components are immune to penetration. Firewall components include: computer platforms; filtering routers; applications software; integrated authentication functions.

In-Line Network Encryptors (INE)

INE are bulk encryption devices which provide security between enterprises across transport nets. Typically placed at the enterprise / transport net boundary, these applications include: Security for high speed, multimedia applications, e.g. Defense Simulation Internet; Secure Virtual Circuit via DISN, e.g. TS/SCI Overlay Net; Defense Megacenters.

Programs that are now in process include: Fastlane for ATM Networks; KG-189 for SONET Networks. Existing Products include: Link encryptors (KG-84, et al); network encryptors (Network Encryption System (NES); and CANEWARE.

Proof of Concept Approach

Rather than securing a DIS exercise at the communications network, and accepting the drawbacks embodied in that approach, (performance bottleneck, single-level exercises), we propose to provide security at the simulation application level through the use of MISSI technology. The current MISSI approach is to migrate security services from application independent areas (such as a communications network) to application dependent areas for systems and applications which are capable of, or require, identification and segregation of information. Distributed combat simulation is such a case.

We propose to demonstrate the efficiency of providing security services, using Fortezza technology, at the simulation application to network interface. Figure 4 is an adaptation of a figure from the 1995 *DIS Vision* which depicts encryption/decryption of information at the application interface by application calls. Placing security at this level allows the simulation host (and its applications) to segregate and protect PDUs based on simulation/exercise specific security policies. In the current environments, such an architecture may be used to isolate various categories of information at the same security level (i.e. caveats within SECRET). Migration of the simulation host operating system to a trusted platform (such as Trusted Mach, a Compartmented Mode Workstation) will allow segregation of information of several security levels.

Technical implementation of this architecture will be achieved by integrating the Fortezza security services into the DIS Interface Library (DIL). Integration at this level will allow security services to be applied directly from the simulation (through an expanded DIL API), on a per host address basis (where addresses may be multi-cast addresses), or on a per PDU-type basis.

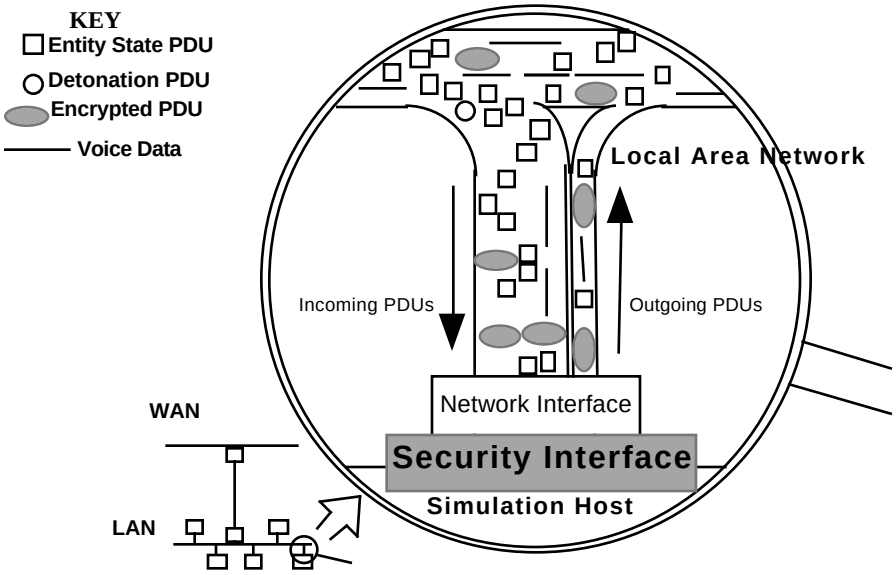


Figure 4. Secured Simulation Host to LAN Interface

Initially, the system will be configured to perform security services on a per host or per PDU-type basis, that is all PDUs destined for a particular host, or of a particular type, will be protected in the same manner (e.g. encrypted). This will allow unmodified DIS simulations (such as MODSAF) to exchange information through a Fortezza protected channel.

Integration of Fortezza with the DIS Interface Library is quite similar to other Fortezza integration efforts to date. In particular, SPARTA's work integrating Fortezza with Electronic Data Interchange (EDI) transaction systems provides a similar model. In both cases, the underlying protocol being secured is "stateless" with each "package" being an atomic event. These stateless protocols ease development since no persistent state must be kept on each package as it is transmitted, and all information required to determine the security services is included in the package.

The architecture of a Fortezza integrated simulator is shown in Figure 5. Most of the security components are non-developmental items. The only development required is in the DIL/Security interface which interfaces the security services with the DIS Interface Library. The scope of work for the DIL/Security Interface entails designing the secured DIS PDU format, developing the interface mechanism/API between the DIL and Fortezza subsystem, and developing the "security API" which may be exported to simulation applications.

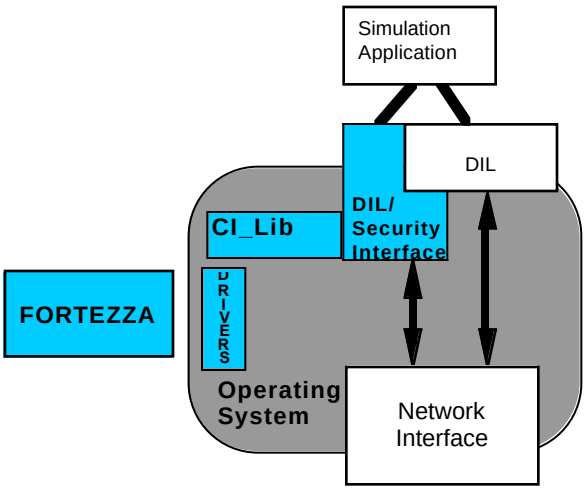


Figure 5. Proof of Concept Software Architecture

Demonstration Scenario

In order to examine issues surrounding this architecture, SPARTA in conjunction with STRICOM (US) and TNO-FEL (Netherlands), will operate multiple MODSAF semi-automated force generators in simple multi-level secure scenarios.

MISSI Fortezza encryption technology will be employed to selectively encrypt information which will only be available to certified node workstations in the network. Unclassified versions of the secure object state descriptions will be generated for viewing synchronization on all nodes.

Figure 6 shows one of these scenarios, using RED, BLUE and GOLD players. The system is set to allow RED forces to interoperate and hide/protect certain information from the BLUE forces and *vice versa*. The GOLD players are able to receive and interact with both sets of forces. Segregation of information is enforced by selective distribution of cryptographic keys to the parties. In particular, the RED forces will only exchange keys with other RED forces and the GOLD players, similarly, the BLUE forces will exchange keys with other BLUE forces and the GOLD players

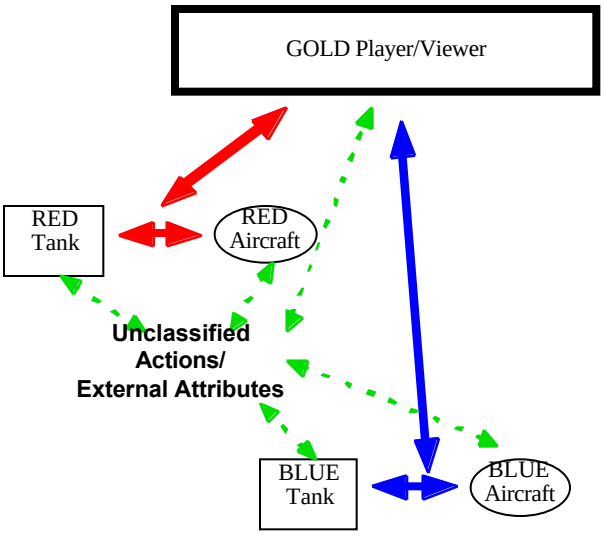


Figure 6. MLS Scenario

Technical Issues Addressed

The planned demonstration is being used to address several important Modeling and Simulation issues. The first objective is the analysis and testing of the Fortezza system performance in distributed simulation applications. Measurement of the throughput, delay, and overhead characteristics of a DIS PDU level security system will be made. These measurements will then be compared and contrasted with performance of the existing DSI network based approach.

Second, this project initiates the required exploration and quantification of issues surrounding development and implementation of "multi-level" secure simulations. In general this will include policy as well as technical elements. Specific issues of immediate interest here are: how will a simulation (MODSAF for example) interface to other distributed simulations at different security levels? What are the technical implications of implementing labeling within a simulation? How will such simulations interface with the DIS or HLA infrastructure such as JSIMS? Can mechanisms assuring multiple single level simulations execute securely within a single simulator, operating from the same databases?

Projected Results

Arrangements for the planned Netherlands / US interactive demonstration have been agreed upon. Allocation of priority for setup and scheduling of the WAN is in progress. Actual results of the long haul network interaction will be provided in a subsequent paper as soon as available. Projected results based on DIS network test data and NSA benchmarks of Fortezza performance provide initial insight into expected distributed simulation response. A discussion of these estimates, lessons learned to date and implications for additional effort needed to achieve a viable multi-level secure simulation capability follows.

A replica of the planned long haul experiment described earlier was modeled between the SPARTA, STRICOM and TNO network nodes. Encryption/decryption overhead estimates are based on reference benchmark data obtained from NSA using a SUN (UNIX) platform driving a Fortezza card reader. The SPARTA-developed Fortezza performance meter measured command performance, computed throughput and message overhead. Average command time recorded was 282 msec, zero byte message time was 51 msec and throughput of 2.4 Mbits/sec was achieved. The throughput was limited by the commercial PCMCIA card interface not the Fortezza processor (which at 40Mhz and 8 bits per clock runs at 320 Mbps). An average PDU generation rate of approximately 10-15 PDUs per second for a pair of tanks during a ground engagement was assumed based on prior observed DIS results. These were conservatively taken to be all entity state PDUs of 1.528 kbit message length.

The vignette battle exercise is initialized by the designated battle master who first exchanges security profile certificates using a security key management system (assumed to be in place). This action pre-authorizes the interactive exchange of sensitive simulation object states between compartmented players so that repeated verification of certificates is avoided during the simulation. This effectively removes the major command latency associated with the Fortezza authentication hand shake.

The planned laydown of four tank platoons 1 TNO, 2 US and 1 threat is then deployed and the vignette tank battle engagement initiated. The graphic presentation of the battle at each of the three node sites differs dependent on the security certificate held at individual host platforms. It was assumed that two of the platoons encrypt for four pairs of tanks. A total of 40 PDUs/sec or about 61 kbits/sec then need to be encrypted and subsequently decrypted. At 2.4 Mbits/sec throughput rate, about 25 msec would be required to encrypt and send all the required data with each PDU experiencing a dominant startup latency of 51 msec. This is well within the 100 msec DIS latency requirement, indicating the current Fortezza hardware should accommodate the distributed ground battle of this experiment satisfactorily.

Conclusions

Our estimates indicate that Fortezza should perform adequately using the existing PCMCIA card bus interface (2.4 Mb/sec throughput). The average key setup command execution time of 282 msec and 51 msec message startup time are relatively large but should allow messaging within the 100 msec DIS total latency requirement. It should be noted that the NSA results were taken from early Fortezza units which were subsequently improved. No measurements for the production version were available at this writing but improved performance observations further reinforce the positive conclusions.

The next commercial PCMCIA interface (Cardbus) to be used in near term Fortezza cards has a maximum projected throughput on the order of 1 Gbits/sec. This level of throughput will be more than adequate to support interactive simulation.

A significant bandwidth advantage is projected for application level encryption in support of larger scale exercises. This results from the fact that the much smaller set of messages specifically requiring classification will be encrypted as compared with total bulk encryption at the enclave boundary. This together with the more selective multicast group vs broadcast transmission should effectively reduce network traffic and further support scale up of multi-level secure battle space objects. The distribution of the encryption load across the many simulation work stations instead of at the enclave guard should also effectively reduce the guard requirement and potential throughput bottleneck.

A related detail of the command latency issue is the fact that as Fortezza is currently designed, only 8 keys can be active on a card at a time. It can be imagined that for a large scale combat simulation there could be more than 8 different objects requiring interchange of multi-level secure information. If this occurs, then activation of new keys from the certificate library will each incur the large command latency. This would introduce a consequent unacceptable “jerkiness” in the graphic displays. This suggests that an alternative version of Fortezza may be useful for larger scale simulation MLS intensive applications which allocate a larger number of active keys.

An additional lesson derived from the development to date was an awareness of the short list of platform drivers which are required to use the Fortezza card. A Fortezza driver for the SGI operating system, for example, was not readily available. A dated IRIX OS version was located through NSA channels. The MODSAF version in general use is SGI based. This created a delay in testing the MODSAF simulation interface code to Fortezza.

The modification of the MODSAF output module to incorporate selective Fortezza commands is an example of potential changes which will be required for all user software needing encryption services. This was not trivial, partly because the MODSAF code has had multiple developers and is not uniformly documented. This effort may be significant dependent on the output structure and number of applications needing to produce or use secure output messages. Standardization of the security interface as an integral part of the simulation architecture is planned for the JSIMS enterprise.

Work Remaining to be Done

An evident remaining effort is the WAN demonstration experiment. In addition to the technical issues associated with the long haul coordination and execution are the procedural and classified policy barriers to intergovernmental security development which have begun to be addressed with STRICOM support and NSA backing. Further discussion of these important policy issues is beyond the scope of this paper.

A precursor to the WAN test is a local network LAN mockup. This effort would simulate the long haul three node interconnect in the same lab and then be distributed locally between STRICOM and SPARTA's Orlando facility. This will serve as a network functional test and as a no latency reference for comparison with the later WAN test. It is expected that these test modes will be demonstrated shortly after final arrangements can be made between TNO-FEL and STRICOM.

Of broader interest is the extended use of the application level MLS concept demonstrated to be feasible in these experiments. The designation and execution of secure data transfer from within the application is a basic INFOSEC feature planned for general MLS communication in the JSIMS federated simulation system and its companion service simulations. To provide a closer test of the JSIMS MLS concept, an HLA-compliant implementation is recommended which also models the encrypted distribution of simulation messages through the DMSO Run Time Interface(RTI) or an HLA-compliant equivalent. Incorporation of message indexing/labeling used in the DMSO interest management concept to manage logically segregated multi-cast groups is an additional useful effort. A demonstration of a secure multi-cast group segregated from unclassified multi-cast groups would confirm the virtual separation of potentially high value classified information within the distributed information stream.

Summary

This effort is the first known set of experiments selectively encrypting information generated by a simulation application. The subsequent trans-mission, decryption and use by another remotely distributed simulation provide the basic functions needed for secure information flow within a distributed wargaming simulation.

Projected results indicate the software feasibility of multi level secure information control from a simulation application will be demonstrated. Near term availability of adequate hardware components further indicates that multi-level secure distributed simulation is technically achievable.

For use in advanced wargaming federations such as JSIMS and companion service simulations (NASM, WARSIM, JSIMS Maritime) ,demonstration of effective application level MLS in an HLA-compliant RTI would be useful and timely. Extension of techniques initiated by this effort could be modified to perform directly pertinent multicast group interest management. This is a recommended follow-on development task. A successful demonstration effort should be possible within the next year, reinforcing the achievement of a robust MLS simulation capability within the five to eight year development windows of JSIMS and related programs.