A **BSTTech Consulting** Technical White Paper

Unit 2, 32 Northbourne Ave
Canberra, ACT 2601
Phone (02) 6247 3372
www.bsttechconsulting.com

MuSE and Computer Security

An Overview of the
Multi Level Security Environment (MuSE) model
A new perspective for securely managing and sharing security classified information

Technical Whitepaper

By Bruce Talbot, Chief Technology Officer

Contents

Introduction

The ability to provide secure and controlled access to information at varying levels of security classification has long been seen as the 'holy grail' of secure computing.

The limitations of early computing hardware and software meant that the only way to secure and manage different security classified systems and compartmented information was to build individual 'air gapped' networks. Whilst successful at securing information, this approach created islands of isolated information and systems that prevented the timely sharing of critical operational information and has meant the inability to share lower classified information such as corporate applications or systems connected to the internet. This requirement for 'air gapped' systems has made the management of classified information expensive and time-consuming often requiring the duplication of processes, hardware, software, system administration, support and maintenance and personnel.

Where sharing is required it has usually been done either by 'sneaker-net' or by tightly controlled guards or gateways that generally required manual management and has very limited throughput capacity.

The increased amount of computing power available in the desktop systems of today's users provide the basis of the demand for greater sharing of data, and also provide the power to address the data sharing needs and redefine the Multi-Level Security (MLS) challenge.

This White Paper discusses the traditional approaches to the challenge of MLS, and proposes an alternative, information centric, approach to achieving secure information management across different security domains.

Problem Statement

Today organisational and operational efficiency is more and more dependent upon ubiquitous access to information to enable more informed and timely decisions making.

Government agencies hold ever increasing amounts of digital data, most of which requires protection from unauthorised access and disclosure. In addition there is an increasing need to share information (in whole or in part) with other Government agencies. At the Protected and Highly Protected levels where the unauthorised disclosure of information may result in harm or death of people it is vital that information is controlled.

The need to use information more effectively and more quickly is also required by all Government departments and commercial organisations where sensitive information is critical to business functions - for example Financial Services.

Traditionally, sensitive information and documents have been secured through the use of isolated systems or computer networks (Standalone or Compartmented Modes of operation). This has been achieved through either manual processes or automated connections via highly controlled information 'guards' (firewalls and 'data diodes') to monitor and securely control the transfer of information. Key drivers of the explosion in the number of separate or compartmented networks have been:

- the range of security classifications and compartments of data; and
- the requirements to ensure segregation between compartments or communities of interest.

Within the Australian Government there are multiple security classifications for information, for example; Unclassified (Public Use), Unclassified (Official Use), In-Confidence, Protected and Highly Protected. Within these classifications there can be many separate logical compartments providing further logical access to meet the 'Need to Know' requirements of the data owners. The problem is compounded when there is a 'Need to Share' and link with the networks of other countries, potentially requiring access to many systems at once to meet the command and control needs of coalition military operations.

In today's environment, where the transfer of information is permitted, the use of hardware oriented MLS Gateways or Guards provide the access enforcement method to share information. The principal method used to achieve this is via 'Information Push' (messaging etc) where the owner of the information 'pushes' it to those who require it. This method offers minimal if any capacity for the user to drive the information acquisition process.

The need to increase information sharing is generating strong pressure to relax current information doctrinal and policy constraints to allow greater exchange of operational information which increases the overall risk of inappropriate use of or access to the information. Hardware based data separation systems make information sharing very difficult to achieve.

From a lifecycle management perspective the costs of running separate information systems is very high, incorporating the direct costs of establishing, managing and sustaining multiple networks, as well as the lost opportunity and operational costs incurred through the inability to share and integrate information effectively.

Use of Information

In considering the issue of secure information management it is useful to address two particular forms of electronic information, namely 'Information at Rest' and 'Information on the Move':

Information at Rest

Information at Rest forms the largest part of the intellectual capital of any organisation. It may be:

- unstructured information stored in file systems or Document Management Systems such as documents, spreadsheets, email archives and diagrams etc; or
- structured information within databases and Knowledge Management Systems.

All of this information can be characterised as static requiring search engines, data mining tools and/or manual intervention to provide organisational value.

A common concern of Senior Executives is their ability to discover and access their organisation's 'information at rest' in a timely fashion. Another concern is that senior executives have access to all of the relevant information on a particular topic, to enable, for example, a Departmental Secretary to confidently certify to Government that all applicable documents have been provided in respect of a particular matter.

Information on the Move

'Information on the Move' tends to be the high value, short term data on which business decisions are made or directions are provided. It is most often found in email, bulletin boards, chat and instant messaging systems.

To be truly effective; a MLS information management solution needs to:

- provide protection for data in all its forms;

- supply user based context;
- support both information push and pull; and
- support the full enterprise.

Traditional Approaches

The technology approaches used to address secure information management in the past can be broadly classified into the following types:

- Cross Domain information transfer systems;
- Knowledge Management Systems;
- Trusted Operating Systems and Databases; and
- Presentation Management systems.

Cross Domain Transfer

As noted in the introduction, Cross Domain Gateways were the initial mechanisms used to transfer data between the separate or 'air-gapped' islands of secure information created by the compartmentalisation approach. Cross Domain Gateways are most suitable for 'Information on the Move'. In a Cross Domain solution, hardware based systems provide a trusted mechanism to allow the transfer of information from 'lower' to 'higher' information security domains. (A recent exception to this is the ability to provide Cross Domain Web Browsing from high to low security domains or between domains of similar classification but owned by different organisations / countries) which was used to share information between various intelligence agencies and statutory authorities.

Cross Domain solutions are usually limited to a small number of applications or protocols, and are highly structured and complex to install / accredit and manage. Located on the boundary of a security zone, a Cross Domain solution can provide the authorisation and authentication management system for access to a set of published knowledge documents or, more commonly, allow the 'push' transfer of information from one security domain to another.

The key limitations of a Cross Domain solution are that it:

- only exposes predefined information to external users (information 'Push');
- only supports short duration high value information through messaging systems (user to user, machine to user and machine to machine);
- requires high levels of management; and
- is a boundary service which does not support information sharing within the enterprise.

Knowledge Management Systems

Knowledge Management Systems (KMS) are well suited to 'Information at Rest'. By enforcing or allowing the codification, mark-up and subsequent management of information against business rules, through the definition of additional document metadata, a KMS is potentially able to expose appropriate static information to internal and external users as required or defined. Typical KMS systems include:

- Sharepoint
- Trim
- Corporate Data Stores

For a KMS to be effective a well structured metadata regime and knowledge management structure is required. The ability to define and map metadata to the needs of the business is a critical element in the ability to use a KMS for information segregation.

Some of the limitations of a Knowledge Management Solution are that it:

- requires an extensive information architecture development to ensure information is appropriately codified;
- supports 'Information at Rest' well but does not support 'Information on the Move'. (information 'Pull');

- requires high levels of management or embedded business processes to ensure information is not orphaned; and
- is an enterprise service which does not readily support remote or external information users.

Trusted Operating Systems

Within single discrete environments, information security has been achieved through Trusted Operating Systems. Early efforts at creating Multi-Level Security solutions looked at the development of operating systems that addressed all of the functions necessary to achieve information tagging and segregation.

Research and Development of the Trusted OS has been on-going since 1970s with developments remaining consistent with advances in operating systems, system security technologies, and network infrastructure; although often several years behind.

The concepts of MAC (Mandatory Access Control) and RBAC (Role-Based Access Control) are core models in the design of security policy for Trusted OS. In addition, the clear separation of enforcement mechanism and policy application, such as GFAC (Generalized Framework for Access Control) and Flask, has dominated the architecture of Trusted OS. The principal strategy of a Trusted OS is to provide enhanced access control models beyond traditional schemes and to ensure that the enhanced security is implemented external to the data and presentation layers.

A basic concept is that only the security administrator can configure the security policy thereby achieving Mandatory Access Control (MAC). This enforced logical access model compels a given access context to keep its mandated information flow as orchestrated by the security administrator. Most research has concentrated on the enforcement of security policy: access control models, and enforcement architecture. Important factors in implementation have been flexibility and minimising the performance penalty during enforcement.

Trusted operating systems classify stored information and provide separated security mechanisms for ensuring the secrecy, integrity and availability of the stored information.

The limitations of reliance on a Trusted Operating System solution are that:

- it mandates a homogeneous system and application architecture throughout the enterprise from the client to the server;
- it supports ‘Information at Rest’ well but does not support ‘Information on the Move’. (information ‘Pull’);
- Trusted OSes are not well supported by common COTS applications (eMail, Finance, HR etc); and
- an enterprise service does not readily support remote / external information users.

Presentation Management Systems

Much work has been done using presentation management systems (such as Compartmented Mode Workstations (CMW)) for the handling of secure information. The use of a single screen and keyboard to view multiple applications or environmental windows, with each window representing a different security domain, is a logical extension of the use of a Trusted Operating System and provides increased functionality and security over traditional Trusted OS systems.

On the surface, a CMW solution provides capabilities which support information sharing options. CMW, a type of secure operating system specified by the DIA in the 1980s, is typically described as "B1-plus," which is shorthand for having the features of a B1 secure system - according to the National Security Agency's Orange Book - as well as a few features added by prospective users such as secure windowing and trusted labelling in windows, trusted networking, trusted path and least-privilege capability.

Several vendors manufacture CMW solutions including HP, Sun and TCS although there is no common interoperability standard which necessitates the adoption of a single vendor approach to implementation.

An alternative Presentation Management system to a CMW solution is a solution such as the Tenix Interactive Link technologies. This provides a CMW link capability in an external device as well as supporting Keyboard / Video / Mouse (KVM) switching between systems. This solution is more technology agnostic on the client side, but the costs and management effort are proportionally higher, due to the additional infrastructure.

The limitations of reliance on a Presentation Management solution are that:

- it mandates a homogeneous client and server architecture throughout the enterprise;
- it requires 'wrapping' of applications and systems to provide connectivity and labelling;
- it supports information 'write up' easily but not 'write down';
- CMW systems are not well supported with common COTS applications (eMail, Finance, HR etc);
- CMW systems have a finite number of security labels / zones available as these labels need to be coded into the OS; and
- Presentation Management is an enterprise service which does not readily support remote / external information users.

An Alternative Solution

To achieve the goal of ubiquitous information sharing across multiple security environments; a MLS system requires functions and elements that span all of the technology components previously addressed. A solution will need to have:

- the RBAC and MAC controls of a Trusted OS;
- the information presentation capability of a Presentation Management system;
- Knowledge Management capabilities for 'Information at Rest' and Cross Domain capabilities for external and security boundaries for 'Information on the Move'.
- the ability to support a heterogeneous client and application environment to allow information to be shared across the wide variety of information consumers and COTS applications that support the Enterprise.

BSTTech has developed the MuSE (Multi-Level Security Environment) - a vendor agnostic Secure Information Management capability which provides:

- Attribute Based Access Control as a part of an Identity Management regime;
- Knowledge Management through enforced meta-data management providing 'Information at Rest' management;
- Client Device and systems management to ensure information integrity;
- Encrypted and managed session management to ensure confidentiality;
- Dynamic Location, Role and User awareness;
- Layered security for Defence-in-Depth;
- SOA systems for application and information integration;
- Presentation and Device context management to support 'Information on the Move'; and
- an Audit and Compliance regime.

BSTTech, in the development of MuSE, has adopted several approaches that replicate the functionality and capability of Trusted OS, Knowledge Management systems, Cross Domain protection and Presentation Management systems to provide an enterprise wide, secure information management solution.

The MuSE architecture includes:

- the separation of roles / functions and enforcement between solution components;
- Super-user containment and control;

- dynamic presentation of information within a business context; and
- application integration through SOA.

Some of the specific capabilities that are required to support an enterprise wide MuSE implementation are:

- Identity Management;
- Device Management;
- Session Management;
- Meta data Management;
- Business Process Management;
- Integration Management; and
- Security Management.

Identity Management

Central to the concept of providing information on demand is the ability to control and manage electronic identities. Current commercial OS and application identity management does not provide the separation of security controls / policy and authentication required by a Trusted OS and only provides a coarse grained access control methodology based around group/folder membership.

The move to a pervasive 'information on demand' environment, with internal and external users being able to access the information appropriate to their function and context, requires the adoption of alternate access control methodologies. The US has already shown interest in the ability to use Attribute Based Access Control (ABAC)[1] [2] as the future methodology to support dynamic access regimes suitable for cross government information sharing.

MuSE already supports ABAC through the creation of an Identity Management (IdM) regime that supports the mandated collection and management of defined user metadata to achieve the business need to segregate information. The IdM system then uses this metadata to dynamically create:

- access controls within the presentation layer;
- groups at the OS level; and
- session management controls for enterprise and federated users to ensure a consistent and enforced management of information.

The IdM capability supports the devolved control of selected user metadata to community of interest (COI) managers whilst retaining the core user functions with the enterprise identity administrators. This allows for controlled access to information compartments based on the business logic most suited to the COI whilst maintaining the integrity of the IdM core information.

Device Management

The management and control of endpoint devices is a critical element of a MLS system. To ensure information integrity and confidentiality there needs to be the ability to control, monitor, and allow:

- access to external storage;
- access to remote applications; and
- users the ability to add/change hardware.

Current practice is based on a 'least' privilege model on a standard SOE (hardware and software) for each environment or domain. Whilst this provides for a baseline device security posture, it does not allow any security classification granularity in terms of users or devices.

The release of information to an authorised user should also be driven by whether it is appropriate to present the content to the particular device that the user is logged on to. This allows a user with a high clearance to access the same data from different devices and, if appropriate, see only the information relevant to their particular work-area or role. As an example, the information/system view that an Engineer has at his own workstation could be much reduced if viewing the same structure in an open area such as a library or through a Remote Access solution.

[1] DARPA Development Spiral 1A announced by John Grimes at the 2008 Warfighter Conferrence.
[2] 2008, Sparta Data sheet on ABAC resulting from DARPA research

MuSE device management supports the identification of each information access device, as well as the device and environmental attributes required to meet the security of a particular document (e.g. whether copying to a USB device is allowed). This is achieved through the development of a "Digital DNA" profile or security rating for each access device.

The "Digital DNA" identifies the computer or device seeking to access classified information using a correlation of features including:

- the physical configuration;
- the IP address assigned;
- multiple electronic serial numbers;
- allocated digital certificates; and
- possibly some sub-component identification.

As an example – the Digital DNA would show "Computer "RUS_101133" is an Intel P4 – 3000 with CPU ID 40127789, MAC Address 000a0c3412, contains 2 GB RAM, 1 SATA HDD (MAXTOR) Serial No 123456-001, conforms to software build "SOE-234 Alpha", has no spyware installed, no printer connected, has a valid PKI certificate provided by the System Root CA)", is located in Building No 124 and is able to access documents and information cleared to 'Protected'.

This "Digital DNA" clearly identifies each information access point, and that it conforms to its recorded profile, enabling a compliance check against the device constraints mandated by a "smart tagged" document.

Session Management

Session management is the ability to dynamically create an access profile related to the features of a particular session. MuSE supports the creation of session ID tokens / certificates based on the attributes of the user, the location and the client access device.

The session management process is as follows:

1. At login, a user's ID and device ID are validated and the device profile compared to the approved profile to ensure compliance;
2. The user's physical location (as defined by the network port and recorded profile) is also validated - users attempting to login from inappropriate locations (e.g. rooms with no security clearance) may be denied access to certain/all documents;
3. Information on the attributes of the user (clearance level, role), device configuration (e.g. with/without printer/media attachments) and location are combined to create a session ID which is uses defined business rules to determine accessibility to information based on the meta data tags associated with each document.

This use of session management allows highly granular control over information down to the smallest information element, for example allowing paragraph level grading and control for classified documents. In addition a session can be immediately terminated in the event of a breach of policy, a change in session or device DNA or change in a user's information access rights.

Metadata Management

MuSE supports the enforced smart tagging of documents based on a defined metadata taxonomy. Providers of information apply multiple metadata tags that flag precisely the security attributes and consumption rights (use) of the document, for matching with the attributes of authorised users. Individual tags may be optional, manually input or automatically collected either as required by a policy or business rules, ensuring that valid document control information is maintained.

MuSE uses metadata and business rules to enable the matching of users to requested information. BSTTech has extensive experience in the establishment of metadata schemas in Defence and other Government high security environments.

Business Process Management (BPM)

The use of business process management is a critical component within a MuSE solution. The business processes provide the enforcement mechanisms and controls for metadata, publishing, separation of roles and functions and support for the SOA elements of the solution.

Within the context of the MuSE system, BPM is formally applied to traditional tasks and outputs as well as to the management of middleware processes and the integration of application software tasks.

The MuSE BPM enables automation of the complex security driven interaction between users and the system, and provides the enterprise content management capabilities.

Integration Management

Pervasive information access requires the ability to integrate data across multiple tiers and systems. MuSE uses a Service Oriented Architecture (SOA) integration approach to enable comprehensive end-to-end data integration and management, and to connect heterogeneous data sources and applications \to deliver clean, accurate, and timely data across the enterprise.

The use of a standards-based SOA framework simplifies data management functions like extract, load, and transform (ELT); data quality; data profiling; and master data management. In addition the use of a SOA solution with an integrated Business Process Management component extends the use of the SOA framework into a data management capability for the enterprise. The SOA platform allows information sources to be labelled and tagged, automatically applying metadata tags to the information being received from these sources and adding them to the repository. This allows external connections and their information to be accurately tagged ensuring that information arriving through these connections can be securely managed.

Security Management

All aspects of MuSE are managed and monitored by the central audit system. Information and System access is logged in detail and associated with the user information, machine profile, and date and time to provide a complete audit trail.

By default, no data can be accessed from any device managed by MuSE without a request to the Security Administrator or a pre-determined data access policy. Specific USB data stores, DVD and CD drives or media can be pre-authorised or authorised remotely to allow data input and transfer.

The role structure used by MuSE can be configured to not allow a single person to upload information or to run an executable file. Patch management and system maintenance can require a MuSE Security Officer to confirm that patches and executables have been uploaded and only then will a Maintenance Officer be authorised to apply the patches through the software management interface. The use of authorised software configurations is recorded against each individual computer on the network to update the DNA signature and provide for a rebuild to the DNA baseline in the event of a mismatch.

Any unauthorised connection attempt will generate events for the Security and System Administrators while automatically disabling the device's network connection or, for known systems, rebuilding its system to an approved configuration. System Administrators can review the baseline of individual computers and computer groups attached to the network and can carry out conformance checks against a security baseline to verify a system's accreditation as and when required.

MuSE Administrators can be prevented from having any visibility of the data content of the systems they manage. To perform their duties, they can view systems and information repositories, but not the contents unless specifically authorised to do so.

The MuSE Identity Management elements ensure user authentication; and metadata tagging and strong access controls enable the separation of system access from content access. Centralised reporting of events for security and systems management provides a single picture of activity across the network and an auditable review of all user actions.

Implementation / Approach

MuSE relies on a thorough understanding of the use of information and the business activities within an enterprise. Whilst BSTTech has developed a stand-alone variation of the system, the use of a mature MuSE solution will not often be within a 'green fields site'. As such the solution will, and can, leverage the existing capabilities and applications of the existing environment.

BSTTech has developed a security architecture maturity model that allows an organisation to assess the maturity of its 'as is' information environment against their desired 'to be' state. This maturity assessment enables development of a technology agnostic roadmap for achieving the desired secure information management end state.

To implement a MuSE solution BSTTech recommends you:

1. Have or develop an information metadata model and standard to enable tagging;
2. Document the required business processes and policies;
3. Document information exchange requirements, connections and interfaces;
4. Define a knowledge management standard;
5. Create a current state Enterprise Architecture;
6. Map the desired state to the organisational baseline to assess its 'maturity';
7. Define the scalability/supportability standards;
8. Develop a technical implementation plan;
9. Install a central pilot and policy system to establish a baseline;
10. Incrementally add capability and new geographic sites.

Summary

BST through the development of MuSE offers an alternative approach to address the secure information management needs of users, while addressing the limitations of current approaches to MLS solutions. The benefits of this approach include:

- Reduction of costly duplication and time-consuming manual processes;
- Faster information access within COIs;
- Leverage of existing capabilities and technology;
- Reduced implementation risk through the use of COTS;
- Comprehensive security auditing;
- Attribute Based Access Control mechanisms, that can protect highly classified information,
- Allowing information with differing security classifications to reside securely within the same system, and
- Access to appropriately cleared users to see only appropriate information they are entitled to as a single network experience

BSTTech Consulting Pty Ltd.

BSTTech Consulting is a Canberra based company with over 35 years of experience servicing Defence and Government customers. BSTTech Consulting is able to provide vendor neutral advice on:

- Secure information management;
- Computer Forensics
- Information and Systems Security;
- Service Oriented Architectures;
- Identity Management;
- Storage Systems Design;
- Systems Architecture and Design; and
- Communications Systems.