Multi-Level Security Applications

Justin Marston
CEO/Founder

BlueSpace Software Corporation
6300 Bridge Point Parkway
Austin, TX 78730

E: info@bluespace.com
P: (512) 637-7306
F: (512) 637-7324

BlueSpace is an enterprise software company, based in Austin, Texas, which creates multi-level secure (MLS) end user applications that can span multiple networks at different classification levels. BlueSpace's middleware strategy facilitates rapid application development, infrastructure consolidation and infrastructure neutrality. The continuing growth in the number of networks in the defense and intelligence communities has led to an increasing requirement for strategies that consolidate physical networks into logical networks running on consolidated infrastructure. This poster paper will survey Multi-Level Secure (MLS) applications that can be deployed on trusted desktops. MLS applications allow trusted desktop systems to go beyond infrastructure cost savings, delivering compelling capabilities for warfighters. Examples include an MLS email client that can provide a single inbox and calendar spanning multiple domains, an MLS search client that spans multiple networks, and an MLS C2 system that can provide a Unified Operating Picture, which consolidates separate Common Operating Pictures into a single view of the battle theater for joint and coalition operations. Multi level end-user applications will catalyse mission transformation in both communities, facilitating ‘all-source’ intelligence analysis, providing improved C2 awareness and orchestration, and ultimately reducing user frustration by enabling users to work seamlessly across network domains.
The continuing growth in the number of networks in the defense and intelligence communities has led to an increasing requirement for strategies to consolidate physical networks into logical networks running on consolidated infrastructure. This paper will survey Multi-Level Secure (MLS) applications that can be deployed on trusted desktops. MLS applications allow trusted desktop systems to go beyond infrastructure cost savings, delivering compelling capabilities for warfighters. Examples include an MLS email client that can provide a single inbox and calendar spanning multiple domains, as well as an MLS C2 system that can provide a Unified Operating Picture, which consolidates separate Common Operating Pictures into a single view of the battle theatre for joint and coalition operations.

**REQUIREMENT**

Historically, warfighters and intelligence analysts carried out most of their day-to-day work on one or two networks. This allowed intelligence analysis to be conducted based on data from a sensible number of source silos, and required only one or two Common Operating Pictures to represent ongoing operations. As joint and coalition missions grew in size and complexity, together with requirements for information sharing in the intelligence community, the number of networks grew organically based on permutations of access rights for collaborating parties.

Dealing with the ever-increasing number of networks in the defense and intelligence communities has become a strategic problem facing both mission owners and IT organizations.

**Mission Drivers**

Several factors have led to a recent explosion in the number of networks being used on a regular basis by a typical warfighter or intelligence analyst:

- **Information Sharing**: The 9/11 Report [1] in the US highlighted the lack of information sharing as a significant factor in the failure of the intelligence community to detect and intercept the 9/11 bombers. This led to a focus by the (newly created) Office of the Director of National Intelligence (ODNI) on improving information sharing and collaboration between the different agencies that make up the US intelligence community. The term ‘all-source’ intelligence analysis rose to prevalence during this period. With each intelligence agency having its own Top Secret network compartment, the number of networks with silos of information that intelligence analysts were called to draw on increased significantly.

- **Real-Time Intelligence**: The conflicts in Iraq and Afghanistan increased the need for more tactical intelligence that had greater time sensitivity. This reflects the transition from a large cold war adversary with strategic positioning to a more nimble and rapidly adaptable adversary such as the insurgents. The value of longer finished intelligence products decreased and the value of rapid tipping and message traffic increased. This led to the ‘write-to-release’ (or “Write for Maximum Utility”) policy [2] of creating intelligence at lower classification levels so it could be made immediately available to warfighters as opposed to going through multiple redaction and sanitization review cycles. This has increased pressure on intelligence analysts to create intelligence on Secret and even Unclassified networks so it can be acted on quickly by warfighters and NGOs.

- **Coalition Operations**: The number and complexity of coalition operations has grown significantly in the past decade – there is now a coalition component in almost every mission. The number of partners has also grown. At the Layered Assurance Workshop in San Antonio, Lt Col Diana Stanieszewski [3] from the CENTCOM J6 commented that the number of coalition partners at CENTCOM had increased from 36 at the start of operation Desert Storm to around 80 at the start of Operation Iraqi Freedom. The number of CENTRIX network domains in the US now numbers around 70. A single command tent in Afghanistan can now have up to 10 different networks provisioned inside it (US Secret, UK Secret, 2 Eyes, 4 Eyes, NATO Secret, ISAF Secret, Mission Secret, etc).

Network overload coupled with pressure to improve information sharing and collaboration has led to policy directives aimed at improving orchestration across network boundaries. The formation of the ODNI [4] was arguably the most high profile action that came out of these policy directives. The formation of the Unified Cross Domain Management Office (UCDMO) in July 2006 had particular relevance to the ‘multiple networks’ challenge. These directives, together with the underlying stimuli impeding mission effectiveness that caused them, can be translated into a set of mission requirements and a set of technology requirements.

**Mission Requirements**

The increasing number of networks being used by each warfighter and intelligence analyst has resulted in the following mission requirements:

- **Reduce Infrastructure Costs**: The costs of duplicated computer workstations, cryptographic hardware, network switches and cabling can be substantial. In addition to the initial acquisition costs, ongoing support and maintenance as well as power and cooling requirements drive costs upwards. A photograph of a user’s desk with separate systems is shown in Figure 1. The requirement is to reduce costs without sacrificing security – to consolidate infrastructure while preserving access controls.

1 BlueSpace Software Corp, 6300 Bridge Point Parkway, Suite 450 Bld 1, Austin, TX 78730, USA

© BlueSpace Software Corp 2011
• **Reduce User Interface Duplication:** Many users must now deal with multiple instances of the same application running on different networks. For example, a user may have five different instances of Microsoft Outlook, each with its own inbox and calendar. This can be frustrating, but other examples can be life threatening. Having multiple Common Operating Pictures at different security domains can increase the time taken to identify friend and foe, unnecessarily increasing the ‘fog of war’. The requirement is to reduce user interface duplication without sacrificing security – to consolidate the user experience while preserving access controls.

• **Improve Policy Adherence:** Achieving behavioural changes in the defense and intelligence communities can be very difficult, and certainly culture and training must be part of the equation. However, if the technology makes the desired user workflow convoluted or annoying, the barrier is significantly larger. At GEOINT 2009, Mr Robert Cardillo described the ‘15 degree rule’ [5] – if an intelligence analyst had to turn his/her body through more than 15 degrees or do more than three mouse clicks, he/she likely wouldn’t do it. The requirement is to improve policy adherence by providing operators with a seamless user experience that can span multiple networks.

These mission requirements have in turn led to a set of technology (and information assurance) requirements.

**Technology Requirements**

The technology requirements have primarily focused thus far on the mission requirement to reduce infrastructure costs:

• **Single Desktop Device:** Infrastructure consolidation starts with reducing the number of computers in a user’s office (see Figure 1). Rather than having many separate computers, the requirement is to be able to interact with data from multiple networks via a single computer.

• **Single Cable:** Consolidation of networking cables from many to a single cable running to each desktop has been a requirement for quite some time. It often involves cryptographic requirements for data being carried across the cables.

• **Single Server:** There has been a requirement to be able to support backend applications interfacing to data from multiple networks on a single server device. This requirement has, in general, been deemed less important than desktop consolidation, as there are typically large server farms on each network, allowing for utilization improvement and consolidation through standard (commercial) virtualization techniques.

• **Single User Interface:** In many ways, this has been a technical ‘holy grail’ requirement for a long time, but it has been challenging to achieve – primarily due to software architecture and information assurance reasons.

There are three different approaches to dealing with this set of technical requirements:

- Cross domain access
- Cross domain transfer
- Multi-level security

Note that the UCDMO manages the US baseline of approved (accredited) cross-domain and MLS systems, and it has categories for each of the three approaches listed above.

These different terms shall be defined and discussed in turn.

**COMPARISON OF APPROACHES**

**Terminology Definitions**

It is easy for terms such as cross domain and multi-level security to become significantly ‘muddled’ by imprecise usage in the community, just as the terms web 2.0, SOA and cloud have now become somewhat ‘fuzzy’.

The US Committee on National Security Systems (CNSS) is a committee with representation from 21 U.S. Government Executive Branch Departments and Agencies. CNSSI 4009 is an Information Assurance Glossary. [6]

CNSSI 4009 defines the term ‘cross domain solution’ as follows: “Information assurance solution that provides the ability to access or transfer information between two or more security domains.”

This definition is self-explanatory.

By contrast, CNSSI 4009 defines the term ‘multi-level security’ as: "Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization."

MLS requires a single system for users to access and edit (process) information at different security levels, while enforcing Mandatory Access Controls (MAC) – an MLS user interface.

Note that access control mechanisms in Microsoft Windows are, throughout the community, deemed to be of insufficient assurance to support separation of content at different...
classification levels for users with different clearances. These controls are termed Discretionary Access Controls, as they can be overcome by a reasonably motivated adversary.

Cross Domain Access

Cross-domain access allows for infrastructure cost reduction by consolidating multiple computer desktops into a single trusted computer device. Note that the term is sometimes used synonymously with Multiple Independent Levels of Security (MILS).

‘Thin’ instances rely on a PC workstation that acts as a trusted hypervisor, running multiple instances of Microsoft Windows connected to different networks. ‘Thin’ instances leverage a thin client device, running multiple Windows terminal sessions, each of which is connected to a different network. There are instances based on Solaris 10 TX, e.g. the AFRL Secure Access Baseline for the EnteRprise (SABER), which was formerly known as the DoDIIS Trusted Workstation (DTW) — shown in Figure 2. There are also SE Linux instances, such as the NSA High Assurance Platform (HAP) as implemented in the Trusted Virtualization Environment (TVE) from General Dynamics. There are also sets of emerging Real-Time Operating System (RTOS) based solutions, such as the One Box One Wire (OB1) solution being pioneered by CENTCOM, based on the Green Hills Integrity 178 operating system.

Figure 2. A SABER thin client [7]

While these cross-domain access solutions do facilitate infrastructure cost reduction ‘out of the box’, they do not significantly change the user experience. They are typically used in a similar manner to a Keyboard Video Mouse (KVM) switch, as the user must switch back and forth between multiple separate instances of Microsoft Windows, each with its own instance of an application such as Microsoft Outlook for email management. Having said this, the underlying technology may (depending on the specific implementation) be capable of supporting multi-level secure applications.

Cross Domain Transfer

Cross-domain transfer solutions can support all of the mission and technical requirements. However, to do so they require MAC to be broken by allowing the transfer of content between networks of different security levels. Cross-domain transfer is usually done through a hardened appliance, acting either as a data diode (unidirectional) or as a data guard (bidirectional). This appliance moves data between two networks, essentially relabeling it on the transfer. A user can access content from multiple networks via a single user interface, typically from a single level regular Windows PC. As the PCs on the users’ desks are single level (i.e. are connected to only one network), it isn’t a problem to connect to each one via a single network cable.

The challenge for cross-domain transfer methods is that they increase the surface area available for attack in government information systems. Content being elevated from a low-side network to a high-side network through a data guard can contain viruses or cross-site scripting attacks. Virus scanners and other mechanisms can reduce these risks, but users typically demand richer and richer content to be elevated (e.g. MS Office files), which makes it more difficult to protect against a well-motivated attacker. If downgrading content is allowed, the data guard typically relies on a dirty word scanner, which is fallible — content may still be highly classified even if it does not include a program name or other dirty word.

This second risk (inappropriate spillage of content to a low-side network) can actually cause cross-domain transfer solutions to have a negative impact on information sharing. Rather than increasing the confidence of organizations partnering together, this risk can instead cause organizations a great deal of concern about the likelihood of their content becoming disclosed, leading to the loss of a unit or asset.

There are use cases in which leveraging a data guard may be very sensible – when the data really needs to be moved between networks. However, data guards are often used to move data between networks purely to provide a ‘single view’ to an operator who had access to all the data in the first place (on separate networks). This is broadly deemed to be an inappropriate use of data guards, as it increases cyber security risks when alternative methods could achieve a similar result with a lower risk profile.

Ultimately, data guards tend to be employed as tactical solutions for specific pain points where information from one network must be made available to users on another network. The approach does have a real advantage in that a data guard does not mandate any requirements on the operator’s computer – an untrusted Windows PC will work just fine. In the real world, cross-domain transfer solutions are not employed to consolidate multiple computers into a single computer.

Multi-Level Security

Multi-level security can also support all of the mission and technical requirements. However, rather than breaking MAC and transferring content between network domains, MLS enforces MAC all the way through to the end user interface. From a mission requirements perspective, the user can have a single computer device on their desktop and it is typically an identical or very similar device to that used in the cross-domain access solution. However, rather than providing a separate instance of a user interface for each network domain, an MLS system orchestrates a single user interface that is connected to multiple networks at the same time.
For the user, this means a single inbox for all their email, or a single C2 system that spans what would otherwise be multiple separate Common Operating Pictures. Appropriately implemented, an MLS system can also help catalyse improved policy adherence in end users, as it provides a seamless interface that spans the different security domains. Creating a new piece of content on the appropriate network label can be made to be as simple as a single mouse click.

So if multi-level security can comply with all mission and technical requirements set out above, why hasn’t it become widely deployed? To answer this question, this paper will survey the history of MLS technologies, and critique the reasons for their failure to achieve broad adoption.

A BRIEF HISTORY OF MLS

MLS is not a new concept – it has its roots in the early periods of computing. With each generation of MLS technologies, attempts have been made to take MLS into mainstream usage, but broad adoption has failed to materialize in the defense and intelligence communities, let alone the broader commercial world. Key reasons behind this continuing failure have included:

• The requirement to have a trusted operating system on the user’s desktop computer.

• The tight coupling of end user applications to the underlying trusted operating system.

• The custom nature of MLS end user applications, requiring integration of labelling into the application code.

• The rise of Microsoft Windows as the dominant end user operating system, along with the massive investment in the commercial sector in software applications that are rich in functionality – setting user expectations.

• The size of the accreditation boundary, resulting in a significant cost and time burden on MLS programs.

This is now changing – in part due to the economic pressures for infrastructure cost reduction amidst significant growth in the number of networks to be supported, and in part due to the convergence of MLS with virtualization.

Early Period

MULTICS was created in 1965, and became a case study for Computer Science undergraduates in the 1980s. Its complexity led to its downfall, with UNIX coming to dominate early computer operating systems. This did not bode well for MLS systems, and the trend continued.

A set of other systems followed, such as Honeywell's SCOMP, USAF SACDIN, NSA Blacker, and Boeing's MLS LAN – none of them saw broad adoption throughout the community. Around the same time, during the 1980s, Microsoft began its ascendance to dominance in end user operating systems and office productivity applications.

Two trusted operating systems based on mainstream UNIX variants emerged in the 1990s – first Sun’s Trusted Solaris, and later SE Linux (developed primarily by NSA). The MLS solutions that have seen accreditation and usage after the turn of the century have been developed to run on these two operating systems. (Note there have also been trusted systems deployed on the XTS-400 operating system, but the majority if not all of these instances have been data guards).

MLS Solutions

Several software vendors have developed backend MLS applications in the past decade, with labelled databases being the primary category. Oracle developed Oracle Label Security (OLS) and Vault, predominantly targeted at the defense and intelligence communities. OLS incorporates a column in each database table for the label (the network from which the data came or with which it is associated). While this enables infrastructure consolidation on the backend, OLS cannot (by itself) enforce MAC in the end user interface.

MLS end user applications have, by contrast, been developed by system integrators, each of which has been tightly coupled with a government program office. Two examples are:

• Joint Coalition Data eXchange (JCDX) – an MLS C2 system funded by SPAWAR, developed by MAXIM (which was acquired by Accenture).

• Trusted Network Environment (TNE) – an MLS collaboration environment (email, file management, etc), developed by General Dynamics for an Air Force customer.

Both MLS solutions were developed to run natively on trusted UNIX based desktops – JCDX on HP UX then ported to SE Linux, TNE on Trusted Solaris 8 then ported to Solaris 10.

MLS applications with this type of design have historically struggled with the following challenges:

• The MLS applications have taken over responsibility for enforcing MAC from the trusted operating system, with a significant quantity of the code running with elevated privileges. This led to a large Trusted Computing Base, making patching difficult due to accreditation overhead.

• The tight coupling of the MLS applications with the operating system’s specific implementation of labelling has made porting to a new operating system (and even upgrading to the new version of the same operating system) very difficult.

• These two challenges combined have led to the user interface in systems of this type looking dated and legacy compared to single level Windows applications such as Microsoft Outlook and Google Earth.

• The tight coupling of hardware, software and configuration has also led to the systems being accredited and acquired as ‘black box’ systems – it was ‘all or nothing’. This did not reflect the increasing trend for mission offices and infrastructure offices to be managed separately, with a focus on service based delivery.

These challenges have caused MLS applications developed by integrators to be focused on a single or small number of customers. The development, sustainment and accreditation costs have become significant on a per seat basis. As a result, MLS applications developed by integrators have not achieved broad adoption throughout the defense and intelligence communities.
MLS and Virtualization Convergence

Light at the end of the tunnel for MLS has come in the form of virtualization technologies. Current cross domain access and MILS solutions rely on running Microsoft Windows at different security domains, either locally (using a trusted hypervisor workstation) or remotely (using a trusted thin client). SABER (Solaris TX), HAP (SE Linux), OB1 (Integrity) and other emerging RTOS based solutions all use this strategy. The user can access regular Windows applications. Seamless windowing (as illustrated in Figure 3) can allow the application windows running in each Windows OS instance to be decoupled from the underlying OS desktop.

The user can access regular Windows applications. Seamless windowing (as illustrated in Figure 3) can allow the application windows running in each Windows OS instance to be decoupled from the underlying OS desktop.

Figure 3. The impact of seamless windowing

Another key enabling factor has been the evolution of commercial and enterprise end user applications away from thick desktop applications towards service oriented architectures and web browser based applications. This has made accessing components of Commercial Off-The-Shelf (COTS) and custom applications far easier, and development much faster. Mashup solutions built upon applications that follow these modern architecture principles have seen rapid uptake in the commercial arena as part of web 2.0. Defense and intelligence agencies have embraced SOA as the foundation for network centric computing. Mashup applications have begun to be used in these communities in an attempt to enable better connectivity between the applications used by warfighters and intelligence analysts – to move away from many separate information systems.

Virtualization and mashups have been employed by a new wave of R&D projects and software vendors offering MLS applications.

MODERN MLS APPLICATIONS

BlueSpace is an enterprise software vendor that creates MLS end user applications and supporting middleware. Rather than attempting to integrate labelling throughout an application’s code base, BlueSpace has taken a virtualization approach to creating MLS editions of COTS applications. BlueSpace orchestrates a single user experience that spans single level applications running in multiple Windows OS instances.

BlueSpace MLS Applications

Specific examples include:

- **Unity**: An MLS email client that provides a single inbox and calendar spanning multiple security levels (the user interface is shown in Figure 4).
- **Discover**: An MLS search and collaboration application that enables an analyst to search content on multiple networks and collaborate with others on their results.
- **GeoSpace**: An MLS C2 client visualizing units and intelligence from multiple networks in a Unified Operating Picture inside Google Earth.

![Unity user interface](image)

Figure 4. Unity user interface

The MLS end user applications leverage unmodified versions of COTS software products as part of the end user interface – for example, in Figure 4, the Unity client uses the Outlook Web Access client to view, edit and reply to emails and calendar items. Note the labelled desktop in Figure 4 – each window is running at a different network domain, with yellow dominant to red and blue.

BlueSpace is grateful for R&D funding from NSA I813 for the S2 {search and share} program, which provided some components of the Discover solution. The S2 project was instigated under the auspices of the Comprehensive National Cybersecurity Initiative, with a focus on developing a higher assurance replacement candidate for the Multi-Domain Dissemination System (MDDS) – a cross-domain transfer search capability.

BlueSpace is also grateful to Hanscom, for partnering with BlueSpace on CWID 2010, using the GeoSpace product as the platform for an MLS C2 system. This participation was highlighted in a TV news piece by an MSNBC affiliate based on interviews with operators at JFCOM. [8]

BlueSpace Architecture

From an infrastructure perspective, these applications connect to multiple separate instances of backend applications. In the case of Unity, there is an unmodified Microsoft Exchange server running in each network domain, and a Unity Application Appliance that connects to each network, as shown in Figure 5.
R&D focused on a ‘Multi-Level App Store’ concept, in which an IT centric organization can host applications for the broader community, and integrate billing with other ‘on demand’ services.

A second area of R&D for BlueSpace is the mobile handset arena. There are now several options for MLS capable desktops, but there are no production devices for an MLS tablet or smartphone for tactical users. BlueSpace predicts that such devices will be created over the next 3-5 years, and intends to release tablet and mobile clients of its core MLS applications, so that users can access the same applications from different device types.

**RELEVANCE TO S&T**

The number of deployed, MLS capable desktops will increase significantly over the next five years, as all of the ‘four eyes’ countries have deployments in place or are planning significant implementations. BlueSpace estimates the number will grow from around 50,000 currently to over 500,000 by the end of 2015.

These seats will be fielded by programs such as CANES and NGEN in the Navy, SPAWAR has significant MLS experience (e.g. JCDX and MLTC). The Combatant Commands also have a history with MLS systems. SOCOM was an original champion of NetTop and then HAP / TVE, CENTCOM was the JCTD sponsor for OB1, and PACOM continues to work with NetTop. Many of these initiatives started life as S&T projects, and were later transferred to the acquisition organizations or J6 elements at the COCOMs.

The initial drivers for these programs have typically been improved energy efficiency and reduced infrastructure costs. However, these trusted desktops are also capable of becoming a platform for MLS applications. These applications will move such programs beyond infrastructure consolidation, providing transformational new capabilities to warfighters and intelligence analysts.

**REFERENCES**


Justin Marston is the Chief Executive Officer and Founder of BlueSpace Software Corporation, an enterprise software vendor based in Austin, TX, that specializes in multi-level security. Mr. Marston is a recognized expert in the MLS arena, having spoken at NSA, UCDMO, AFRL and USAF conferences on the topic. Email: justin.marston@bluespace.com; phone: +1 512 366 3940; fax: +1 512 637 7324.

© BlueSpace Software Corp 2011