Secure Cross Domain Operation

Sanjay Khetia, Daran Crush
QinetiQ
Farnborough, UK
skhetia@QinetiQ.com, dfcrush@QinetiQ.com

ABSTRACT

There is an increasing need to perform Live Virtual and Constructive (LVC) based experimentation and training involving users and systems at different levels of clearance, classification and commercial boundaries. We have been researching this area, which has been fruitful in identifying requirements and innovative solutions. This thought leading paper shares our views on the challenges and discusses promising solutions to meet these requirements.

The paper discusses requirements from multiple perspectives, such as the users, infrastructures, applications, simulation systems and intellectual property. We highlight the challenges of protecting against leakage of sensitive information and also from the risk of compromising system integrity from malicious data.

A view on some of the costs, risks and limitation drivers are explored alongside the advantages and disadvantages of candidate architectures. We will be drawing on our experiences of delivering training and experimentation services, utilising modular flexible architectures that allow common, highly configurable content checking in conjunction with a variety of interface protocols.

The paper describes examples of how we have addressed the cross domain challenge and closes with a view of the remaining challenges.

ABOUT THE AUTHORS

Sanjay Khetia is the Chief Architect for Training and Simulation Services within QinetiQ. He is a strategic thought leader, a technical SME with over 12 years of demonstrable track record of designing, developing and delivering simulation and training concepts, solutions and services to the defence sector. One of Sanjay's key achievements was to ensure the capture and effective delivery of the Mission Training through Distributed Simulation Capability Concept Demonstrator (MTDS CCD) and the Distributed Synthetic Air Land Training (DSALT) programme - both multi-million pound activities with complex Industry, MOD and military relationships.

Sanjay is also the chair of the Training and Simulation Services Innovation Board. With his passion for innovation and technology he is arguably one of the "people who know how" to help evolve and translate requirements into technical solutions for both the military and commercial markets; domestic and international. As a result he is QinetiQ's solution lead for the MOD's Defence Operational Training Capability (Air) programme and a number of international mission training opportunities.

Daran Crush is a skilled systems engineer, which has led to him working across a wide range of MOD programmes throughout his 22 year career at QinetiQ. Daran's skills centre on supporting a client through the initial identification of their problem to the design and implementation of a technical solution within a complex stakeholder or technical environment. Daran's expertise includes the application of simulation and modelling to training, experimentation, testing, battlespace architecture, secure networking, facility construction and operation, and he has a specialism in the use of modelling, simulation and synthetic environments across a wide range of application areas.

Secure Cross Domain Operation

Sanjay Khetia, Daran Crush
QinetiQ
Farnborough, UK
skhetia@qinetiq.com, dfcrush@QinetiQ.com

INTRODUCTION

The operation of any network of information processing systems (including training systems and simulators) is subject to a set of rules governing the type of data that can be stored, manipulated or exchanged with systems in its network or beyond its local or national boundary.

In the UK the rules are applied by the Defence Security and Standards (DSAS) Accreditors who within the MoD are bound by the Manual of Security (JSP440) [1] and guidance from the UK National Technical Authority (Communication and Electronics Security Group (CESG). All the rules for accreditation are based on the UK Security Policy Framework.

The process of accreditation is based in the initial instance on the type of data being processed or exchanged by a target system. The same rules can be applied where information is exchanged at the same Protective Marking (PM) or irrespective of the PM.

Issues escalate when information is required to be exchanged between systems that have different PM. This paper provides an introduction to a possible solution for these issues and is specifically targeting simulation systems operating in Local Area Network (LAN) and Wide Area Network (WAN) connected environments where connection will be to other nation's networks or to systems operating at a PM below or above their own PM.

Other research [2][3][4] has identified a number means to technically implement some aspects of Multi Level Security and concluded that Cross Domain Security is the way forward but only when policy and process issues have been resolved. This paper presents a technical implementation that provides an integrated solution that mixes guards, diodes and labeling and release techniques to provide an overall solution. This solution is built on practical experience from the UK MoD Distributed Synthetic Air Land Training (DSALT) programme and an ongoing relationship with the UK accreditation bodies.

BACKGROUND

UK Policy

The security and accreditation of network is governed by the UK HMG Security Policy Framework, this is promulgated in to the MoD Service Arms as the Joint Service Publication (JSP) 440 Manual of Security.

The design and installation of a secure information processing system is reviewed and approved by an Accreditor (Acc) from Defence Security and Standards. Installation is also subject to the rules and conventions dictated in JSP 480: The Rules for Installation of Security Electronic Information Systems, Co-ordinating Installation Design Authority (CIDA).

At the initial design review stage DSAS Acc will require a security risk assessment; this is directed to be UK HMG IS1 but with a DSAS Acc approval risk assessment can be done using the Domain Based security assessment process. Both methods are comparable and will result in an initial risk assessment.

The risk assessment will account for:

- Physical security issues with the proposed location of the installation,
- Its proposed operating environment,

- Its national security sensitivity,
- The criticality of the system to the business.

The DSAS Acc will also examine the Criticality Level (CL) associated with the proposed system. The CL is related to the level of redundancy, network protection and availability and the need to process critical defence operational information. The output from the Risk Assessment is a tabulated set of categorised risks (High, Medium or Low). Mitigation is required of all Risk in the High category. Some of the Medium category risks may be accepted. All of these factors will affect the security requirements and subsequent design for the information processing system.

Type of system operation

The types of operation are defined in JSP440 Sect 8 Pt2 as:

- Dedicated Security Mode is a mode of operation in which all the users of a system are cleared to know and have access to all the data it handles. The system does not enforce national security rules or 'need-to-know' and little or no technical security functionality is required.
- System High Security Mode is a mode of operation in which the users of a system are all cleared for, and have formal access approval for, all the information handled by it. Not all users, however, actually need-to-know about all of the data. In this mode of operation Discretionary Access Control (DAC) may be applied.
- Compartmented Security Mode is a mode of operation in which the users are all cleared for, but do not have formal access approval for, all the data handled by the Compartmented Mode system; users only have access within their need to know requirements and are given access to some of the data by means of Mandatory Access Controls (MAC).
- Multi-level Secure (MLS) Mode is a mode of operation in which a computer system handles data at various protective markings etc, but for which there are users not cleared for all that data and whose access to the data must be controlled in accordance with their clearance and need to know. The electronic system is relied upon to enforce the national security rules.

Each of the above types of operation will have specific system design issues and this paper focuses on those associated with the operation of systems providing interconnection with or between systems operating a number of differing PMs.

DEFINITION OF EXCHANGE REQUIREMENTS

The exchange of data can be defined by either the protective marking of the data set or the global protective marking of the subject systems. Protective marking of the data sets requires special data labeling systems not currently in use in simulation networks. Normal accreditation processes will define the global protective marking of the system which usually dictates that system running in the “System High” mode.

Across the boundary protocol sets for Simulation Operation

In a large simulation network providing not only the platform simulation but an element of event management and directed simulation for event authenticity the main protocol sets expected to be visible within the network and likely to be exchanged across the local network boundary during a multi-site event are detailed below.

The protocols used across the boundary will be:

1. H323 Video protocol for Video teleconferencing, this is used both during engineering and Briefing and De-briefing during events. The Video stream cannot be electronically mediated for security therefore it must be considered to be operating at the protective marking of the event.
2. Voice over IP is a digitally encoded telephone protocol and like the video conferencing system must be considered to be operating at the event protective marking.
3. Simulated radio is another digitally encoded analogue signal but this will be in use during the event by trainees as it carries the radio simulation data. Similar rule to the first two protocols.
4. Email this is an Internet standard protocol and can be mediated by electronic means.
5. FTP etc. the protocol can be read and mediated by an electronic system.

6. Simulation environment data is a very structured protocol ideal for electronic manipulation and filtering. For example DIS (Distributed Interactive Simulation IEEE1278) has been used as the protocol for simulation interoperability, but any other standard is equally applicable, such as HLA (High Level Architecture IEEE1516), DDS (Data Distribution Service [5]) or TENA (Test and Training Enabling Architecture [6]).
7. C2 component data exchange – operational data in standard formats exchanged between the C2 systems and the simulation systems. For example Web Mapped Services, Over The Horizon Gold (OTH Gold), jChat etc.
8. Briefing / De-briefing tools these are used in conjunction with the VTC system however they have a more structured content similar to the simulation environment data and can be mitigated by electronic means.
9. Admin functions these must be blocked at the network boundary as they allow manipulation of the operational parameters of the whole national LAN.

Other Protocols Across the boundary

In all large networks of computer systems, continual maintenance of services such as operating system software and malicious code protection is necessary. In the main it is most straightforward to connect directly to the supplier and accept their updates automatically.

Within classified systems this poses issues as it allows direct access between the classified and public network. These protocols can be accepted across the boundary if there is no bi-direction communication between the High and Low networks.

REQUIREMENTS FOR DATA EXCHANGE AT DIFFERING PROTECTIVE MARKING

Protection of national data sets

The protection of UK national data is defined in JSP440 and requires the protection of the national network boundary and the bearer systems carrying the data outside the LAN.

Boundary protection:

- To separate between networks carrying data at one level of difference in the protective marking the required level of evaluated device is to Common Criteria Evaluation Assurance Level (EAL) 4.
- Separation between higher protective marking and the Internet would have to be at EAL 6 or higher. The carriage of this higher protective marking data across the internet requires encryption, therefore the boundary device between the protectively marked network and the Internet would have to encrypt data passing across the boundary and also enforce the rule for downgrading of information JSP440 Part 5 Section 1 Chapter 1 paragraph 16.

Bearer protection:

- There are distinct types of bearer protection all of which require cryptographic equipment to encipher the data sets between the end points:
  - High Grade
  - Enhanced
  - Baseline
  - Commercial

Downgrading across the Boundary:

- Downgrading requires the originators consent; during a simulation event this will not be possible so and agreement will have to be sought prior to. Where an electronic solution is used to enforce the downgrading process CESG will need to evaluate both the technical architecture and the rule sets applied during each separate event.

The challenge is to ensure that there is no leakage of sensitive information or injection of malicious data that could compromise system integrity.

User / stakeholder perspectives

From a trainees and trainers perspective the view the operational environment represented by the training system must meet the training objectives and thus be implemented with the appropriate protectively marked systems and data defined by the training need. This may therefore require highly protectively marked data and systems for some type of training, such as mission rehearsal and less highly protectively marked data for others, such as individual procedures training. Further, within the UK, by default, different services clear their personnel to different levels of access. This has led to the situation where different training systems are implemented at different levels of protective marking and personnel have different levels clearance. The outcome of this is show in figure 1.

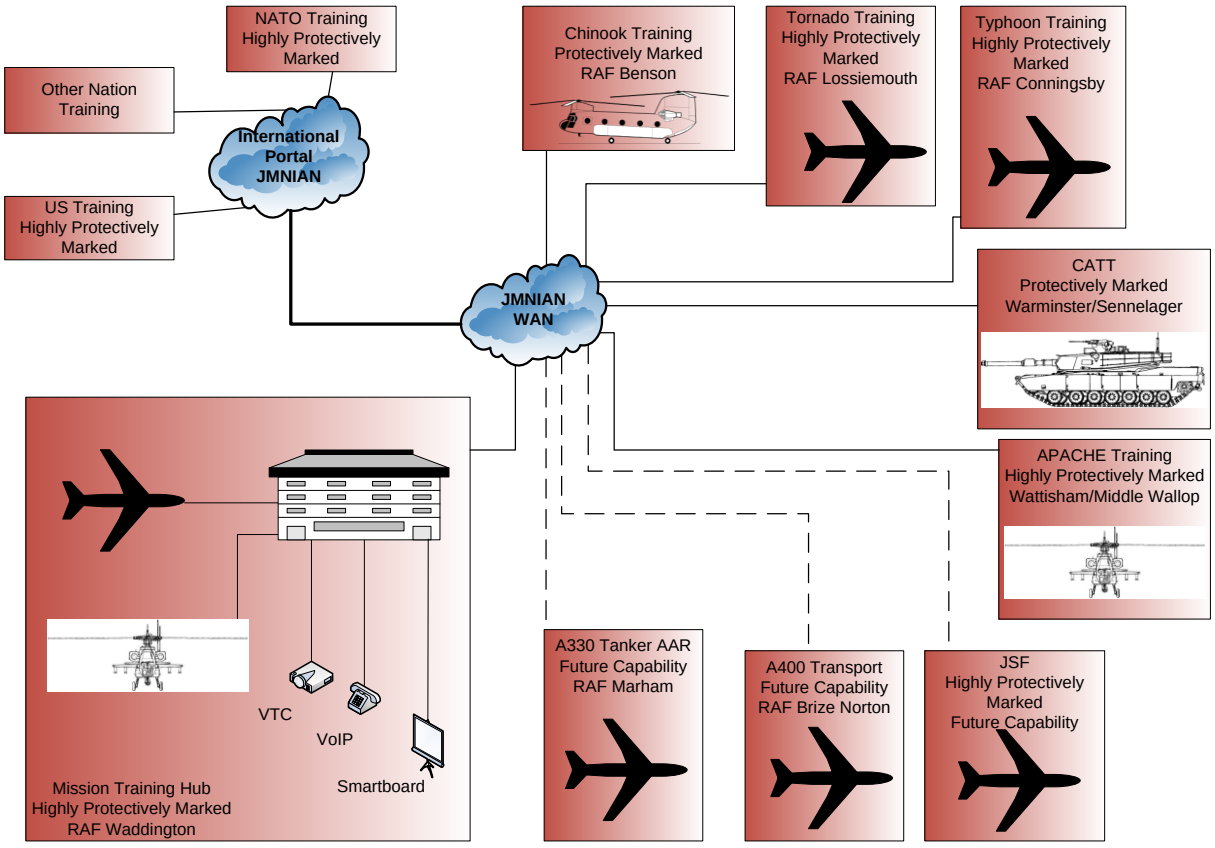

Figure 1 – Future and current UK training systems

From a systems builders and maintainers perspective the system will be constructed and operated at the protective marking level required by the training need. Further, the system may be designed such that some systems are partitioned onto different real of virtual networks to better manage resources, some of which may be at different protective marking levels. Additionally, the systems will need to be maintained and require access to and updates of some of the systems and data. Some of these updates may be provided by external entities, such as anti-virus software updates or operating system patches.

To achieve the recommendations described in the October 2010 Strategic Defence and Security Review (SDSR) White Paper [7] there is an expectation that the systems shown in figure 1 (and others not shown) will be regularly brought together in different compositions. This will require solutions to be developed that enables cross domain operation rather than the implementation of a "system high" approach. Additionally, the expected frequency and differing configurations of these compositions would have a significant accreditation burden (in the time to taken accredit and thus cost involved), therefore a different solution is required that would allow a more readily re-composable approach.

INFRASTRUCTURES

Current Training Environments

Current training environments share a range of different types of data to enable them to interoperate (see above). This data can be partitioned onto different real or virtual networks. A representation of this partitioning is shown in figure 2 with the boundary to external systems. This means of partitioning normally uses Virtual Local Area Networks (VLANs) which do not have any security enforcement features, provide multiple entry points to each system (i.e. each system could have 3 network connections), operational and management protocols operate on the same physical infrastructure and there is no data segregation.

In the future it is expected that interoperability between systems will become more common place, increasing the complexity of the connectivity and overall architecture. To manage this complexity and to ensure integrity a different approach is required that reduces the number of entry points to each system and that segregates different types of data.

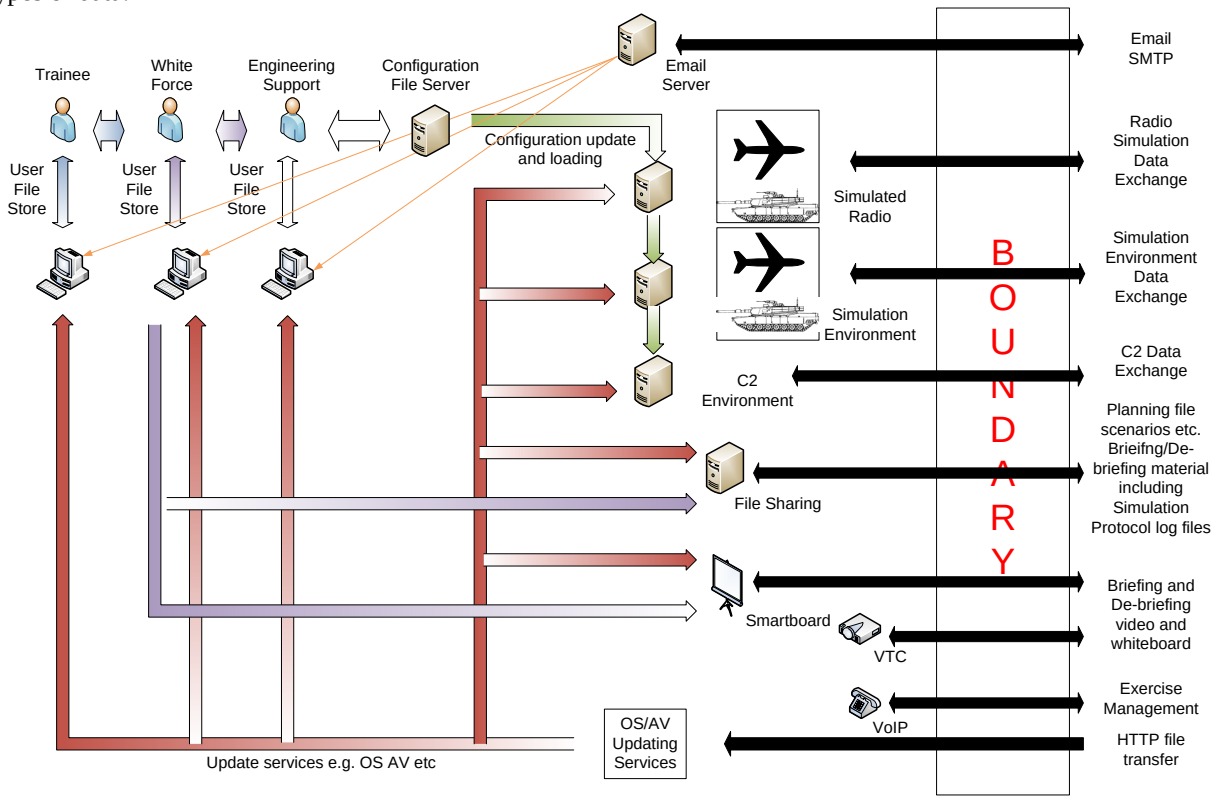

Figure 2 – 'Current architecture'

Guard Release

The Guard Release Procedure offers an alternative approach where the data stream and the content of the data are analysed both for malicious content and leakage of sensitive information.

A set of rules are generated for each of the different types of data. These can then be applied to the data stream to manipulate its content to ensure that is meets any protective marking constraints before it is transmitted. This process is shown in figure 3.

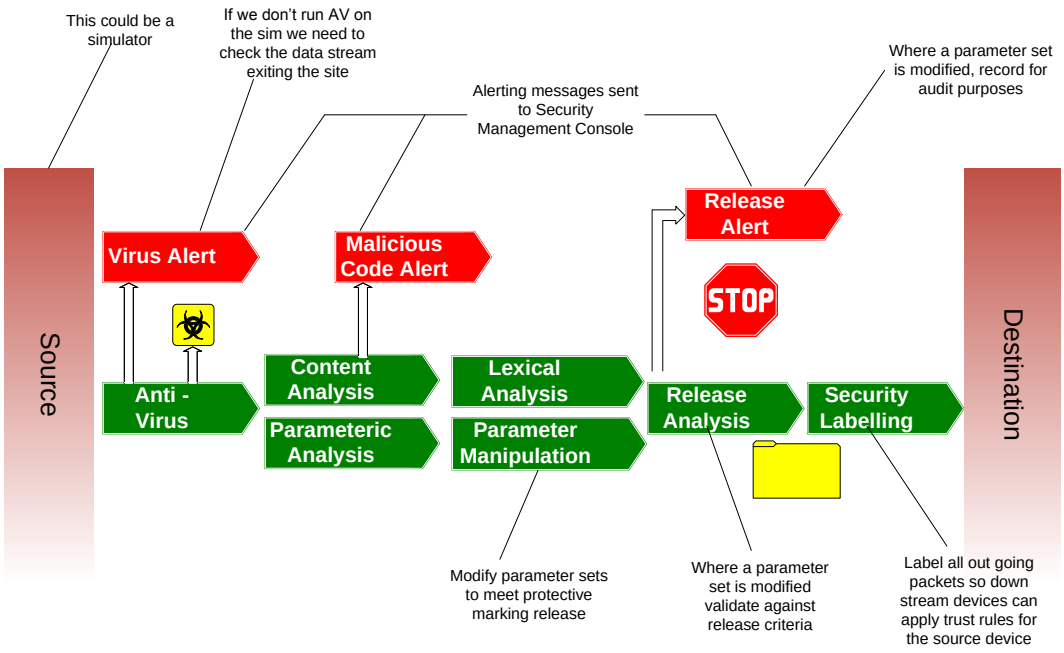

Figure 3 – Guard Release

This could be implemented either as a single point guard which could provide a single system, although this would require a complex set of rules and potentially introduce latency. A multi-point guard could be implemented with a guard for each of the data sources. This would potentially improve latency and reduce the complexity of the overall ruleset. The architecture for a multi-point boundary protection system is shown in figure 4.

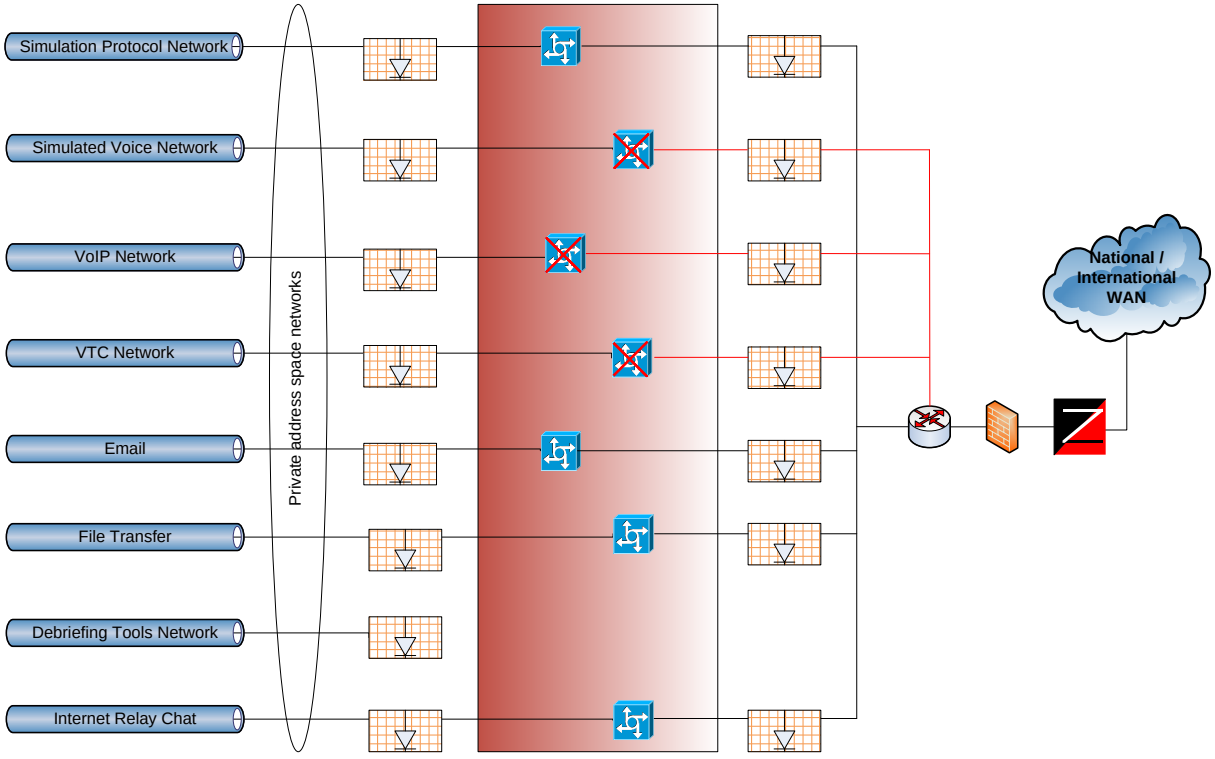

Figure 4 – Multi point boundary protection system

A similar boundary system will also be required to safeguard the simulation from malicious data from external systems while ensuring that it is maintained. To meet these requirements it will be necessary to setup untrusted servers on the outside of the boundary, these will collect the latest software and virus signature sets and provide them through the boundary as a file transfer service utilising a one way network device known as a Data Diode. This is a specific hardware set design to allow file transfer in one direction without allowing the normal signaling protocols used in IEE802.3 to return from the inside networks. Figure 5 shows how a simulation system can be protected while still ensuring that it can be updated.

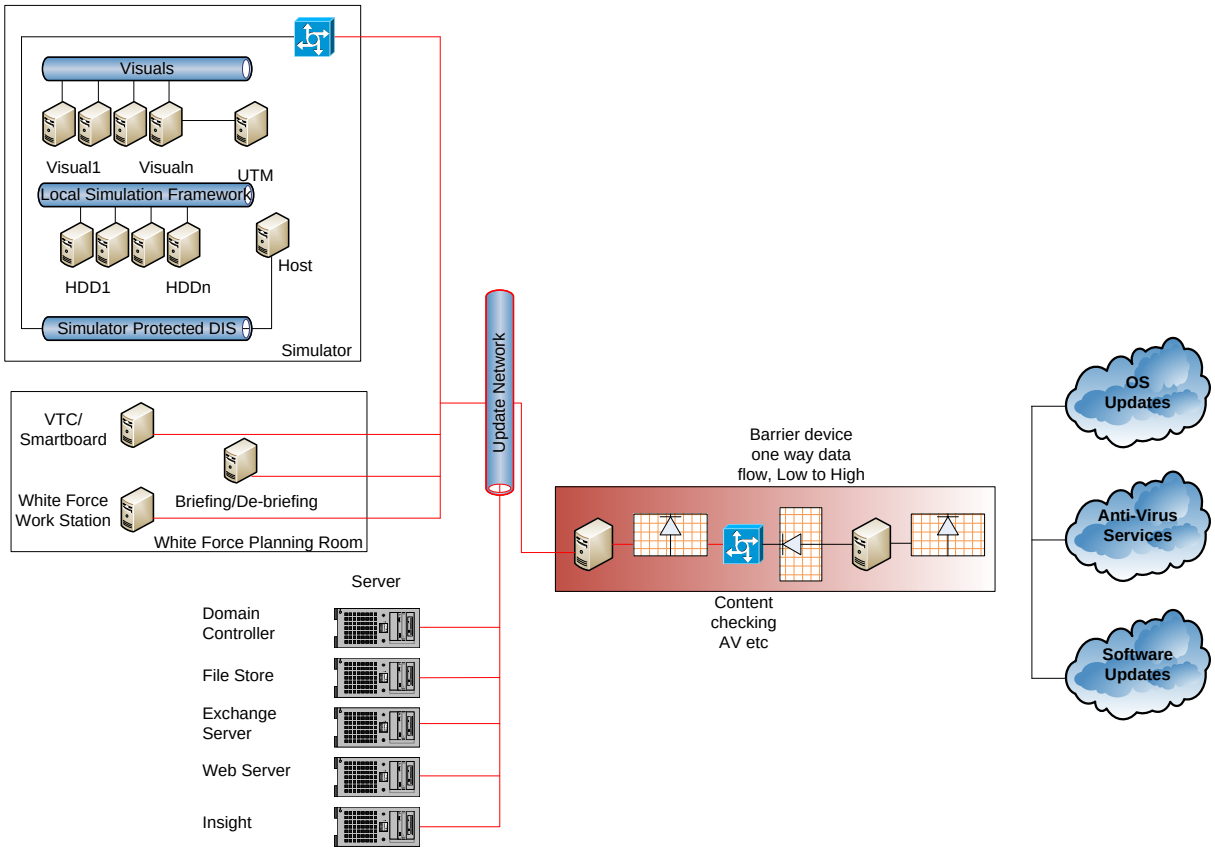

Figure 5 – Simulation Guard

The overall architecture, multi point boundary protection and simulation guard is shown in figure 6. Operating systems at high protective markings may require the use of extensive network monitoring for intrusion detection and intrusion prevention.

These systems are known as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). These IDS and IPS systems will form the core defence mechanism against malicious outsiders and covert insider attacks.

In order to lessen the impact of the network monitoring on the operational network passive network taps will be installed at strategic points in the system most notably either side of any security enforcing devices. The three monitoring system located in the centre of figure 6 would also relay alert messages through a one way system to the security management system on the right.

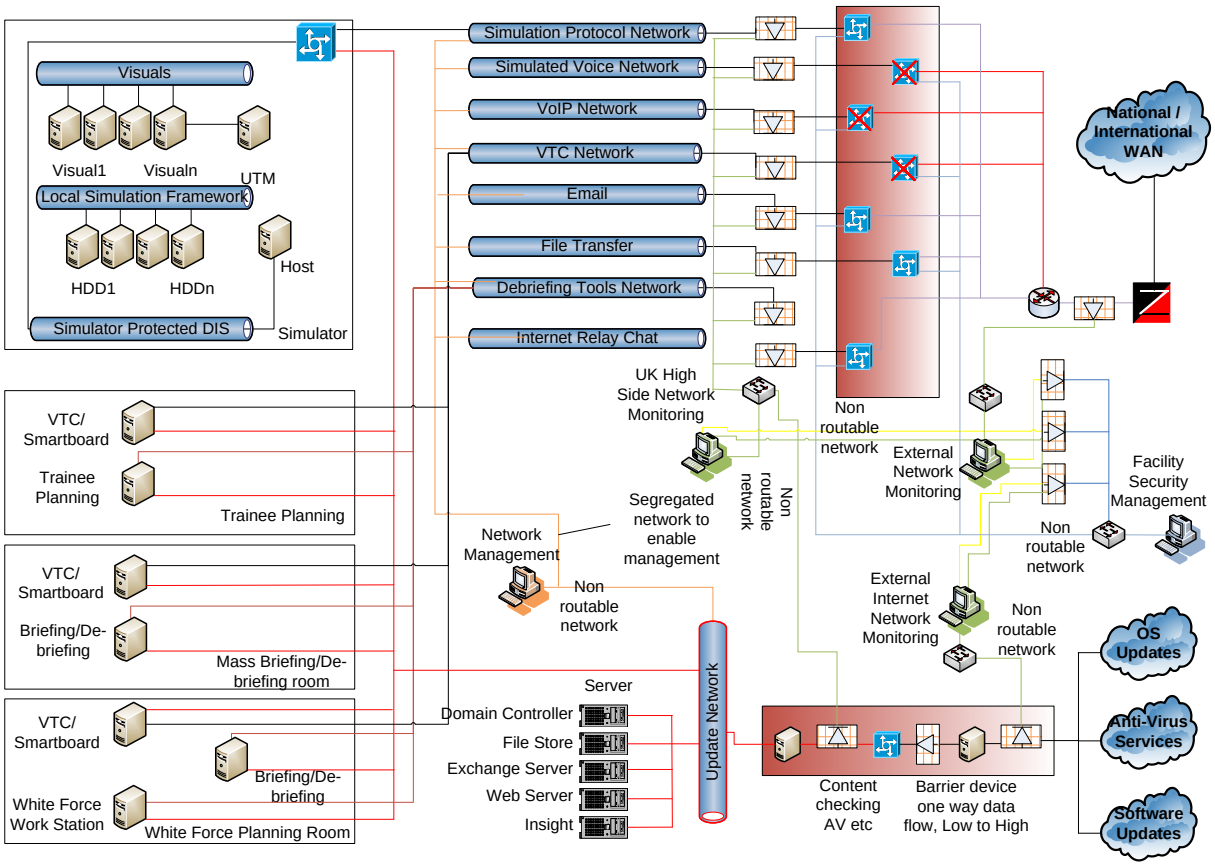

Figure 6 – Overall architecture

Design of the filtering systems will be a significant issue as the level of protection required to separate "highly protectively marked" systems from any level below will be to EAL6. To achieve EAL6 protection levels any device used on a network must show that it achieves a physical break between the Low side data stream and the High side data stream. Traditionally the change from a "highly protectively marked" level to a lower level is achieved by an "Air Gap" where a person would receive from the High side system examine the content and based on knowledge or authority would release the information to the lower level system by re-entering the information.

Where data sets are large and varied the rule set in an electronic information processing system would be similarly large and complex as the interaction between data items would have to be mitigated as well as the straight forward downgrading. Consequently in a large simulation network a single filtering system on the network national boundary will have a large rule set constantly being changed between events and requiring large effort and time to ratify.

When using unevaluated systems the issues are compounded:

- Untrusted software in both operating system and programs.
- Unlabelled data.
- Untrusted hardware.
- No recognised security enforcing functionality.

Risk reduction methods can be applied by providing a hardened shell to the untrusted systems. At the output from the system add a mediating filter with approved hardware which also provides data labelling for the outgoing data stream.

CONCLUSIONS

In this paper we have outlined the UK MOD accreditation policy, the types of modes of secure operation and the different types of information that a simulation system may generate. These information types identify the main set that a simulation system needs to achieve interoperability.

We have concluded from our experience that the way in which simulation systems are currently brought together, generally having to all operate at the same protective marking, is not sustainable if we are to meet the training challenges of the future.

We have identified a number of solutions to address different aspects of security. An overall implementation is proposed that brings a number of these solutions together to tackle the challenge of secure cross domain operation. This proposed implementation is built upon practical experience gained in the DSALT programme and through our close working relationship with the UK accreditation bodies.

ACKNOLEDGMENTS

Thanks to Peter Blake for his support in the production of this paper.

REFERENCES

1. Joint Service Publication 440, Defence Coordinating Installation Design Authority Manual of Regulations for Installation of Communication and Information Systems, Edition 16 (2011).
2. Croom-Johnson, S, (2013), From Multi Level Security to Cross Domain Solutions, Dstl/CR69986
3. NATO MSG-080, 'Security in Collective Mission Simulation'. http://www.cso.nato.int/ACTIVITY_META.asp?ACT=1884
4. Simulation Interoperability Standards Organisation (SISO) website. http://www.sisostds.org/
5. Data Distribution Service website. http://portals.omg.org/dds/
6. Test and Training Enabling Architecture (TENA) website. https://www.tena-sda.org/
7. Securing Britain in an Age of Uncertainty: 'The Strategic Defence and Security Review' (2010)