MSG-168 Lecture Series on
Modelling and Simulation as a Service (MSaaS)

6. Overview of Security for MSaaS

14. Security Challenges

16. Data-Centric v Network-Centric Approach

Efthimios (Mike) Douklias
Naval Information Warfare Center (NIWC) Pacific
Author Address
UNITED STATED OF AMERICA

mike.d.douklias@navy.mil/douklias@gmail.com

ABSTRACT

NATO and nations use simulation environments for various purposes, such as training, capability development, mission rehearsal, and decision support in acquisition processes. Consequently, Modelling and Simulation (M&S) has become a critical capability for the alliance and its nations. M&S products are highly valuable resources and it is essential that M&S products, data and processes are conveniently accessible to a large number of users as often as possible. However, achieving interoperability between simulation systems and ensuring credibility of results currently requires large efforts with regards to time, personnel and budget.

Recent developments in cloud computing technology and service-oriented architectures offer opportunities to better utilize M&S capabilities in order to satisfy NATO critical needs. M&S as a Service (MSaaS) is a new concept that includes service orientation and the provision of M&S applications via the as-a-service model of cloud computing to enable more composable simulation environments that can be deployed and executed on-demand.

In this paper, I will be exploring the following topics:

- *Overview of Security for MSaaS*
- *Technical Reference Architecture*
- *Composition Technical Approach*
- *Execution in the Cloud*
- *Security Challenges*
- *Data-Centric v Network-Centric Approach*

1.0 OVERVIEW OF CYBERSECURITY FOR MSAAS

One of the most important concern expressed by stakeholders were Vulnerability (Cybersecurity) of their models, products and systems in the cloud environment.

We need to identify related Cybersecurity frameworks and roadmaps that will affect the selection of key

MSaaS technologies, and facilitate network interoperability at future milestones as well as identify the importance and dependencies of obtaining security accreditation of key services and technologies. At the same time, we need to implement and enforce cybersecurity policies for M&S services. Overall, cybersecurity is about Securing and Protecting the "DATA", through a secure Framework.

M&S products are highly valuable to NATO and military organizations, and it is essential that M&S products, data and processes to be under cyber hygiene with an acceptable security posture and at the same time, conveniently accessible to a large number of users whenever and wherever needed. Therefore, a new "M&S ecosystem" is required where M&S products can be more readily identified and accessed by a large number of users to meet their specific requirements. This "as a Service" paradigm has to support stand-alone use as well as integration of multiple simulated and real systems into a unified simulation environment whenever the need arises.

Ensuring the proper cybersecurity is intrinsically related to the cloud computing service model (Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)) and to the deployment model (Public, Private, Hybrid, or Community) that best fits the Consumer's mission and cybersecurity requirements. The Consumer must evaluate the particular cybersecurity requirements in the specific architectural context, and map them to proper security controls and practices in technical, operational, and management classes. While the Cloud Security Reference Architecture [NIST 500-299] possesses a rich body of knowledge of general network security and information security, both in theory and in practice, it also addresses the cloud-specific security requirements triggered by characteristics unique to the cloud, such as decreased visibility and control by consumers. Cloud security frameworks including information management within an infrastructure shall support the cloud implementers, providers and consumers. However, MSG-136 recognizes that a more tailored approach may be needed to exploit MSaaS specific capabilities and proposes to develop additional guidelines as part of the work.

It is anticipated that future military capabilities, including training, mission planning and decision making will be provided through increased use of M&S. Currently, majority of all training is accomplished at a lab in a closed and controlled network. However, there are currently two main barriers: the perceived cost, and the time taken to compose and develop simulation environments. Furthermore, limited credibility resulting from unknown factors and ad-hoc processes is still a serious problem.

1.1 Cloud Computing

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models. (NIST SP 800-145).

- Essential Characteristics:
  - On-demand self-service
  - Broad network access
  - Resource pooling
  - Rapid elasticity
  - Measured service

- Service Models:
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)

- Deployment Models:
  - Private cloud
  - Community cloud
  - Public cloud
  - Hybrid cloud

1.2 Cybersecurity

DoDI8500.01 defines cybersecurity as "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

The ability to protect or defend the use of cyberspace from cyber-attacks. (CNSSI-4009).

The objectives of cybersecurity is to make sure all products and access controls to the products and services are secured and protected. We should implement a secure information/data flow exchange, access controls, eliminate attack vectors, secure hygiene and balanced protection of the confidentiality, integrity and availability (CIA) of data in a cloud environment. At the same time, we need to give flexibility and freedom of the development lifecycle.

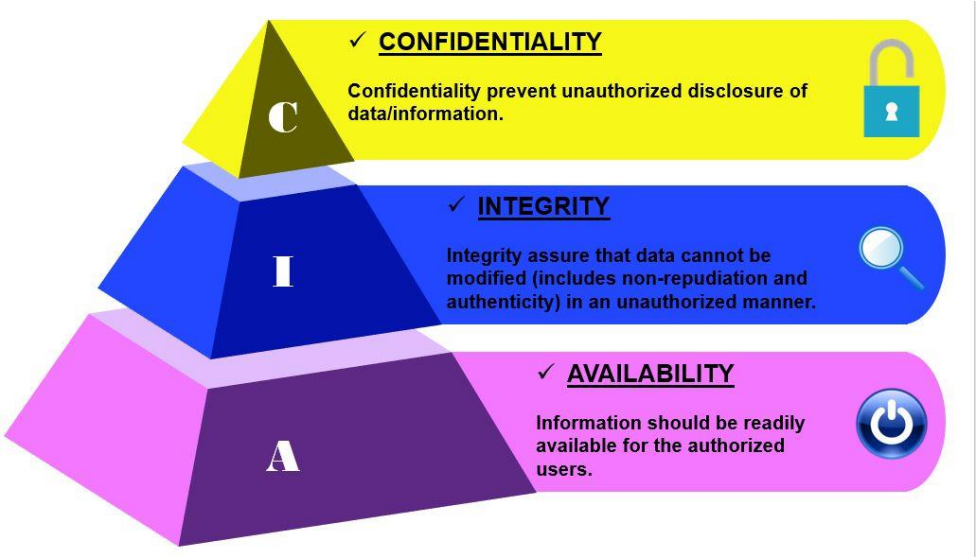

Figure 1 Confidentiality, Integrity, Availability

The correct cybersecurity implementation will safeguard our stakeholders by employing a secure posture, for accessed services, data, account information, classification, classification upgraded by aggregation, and Personally Identifiable Information (PII).

They are multiple layers of cybersecurity:

- Cloud Cybersecurity controls
  - Cryptography
    - Data security at-rest

        - In-transit
        - Data sovereignty
        - Authorized communication between services
        - Use of encrypted channels for all communications

    - Firewalls & Network Monitoring
        - Operational monitoring, reporting and response

    - Vulnerability Testing
        - Perimeter security (backhaul, on premise or cleansheet)
        - Network Intrusion Detection
        - Network Prevention Detection

    - Access Control Methods
        - Identity and Access Management (IdAM)

    - Software Assurance
        - Application security

- Physical Security

    - Hardware security

- Data Loss Protection (DLP)

- Governance

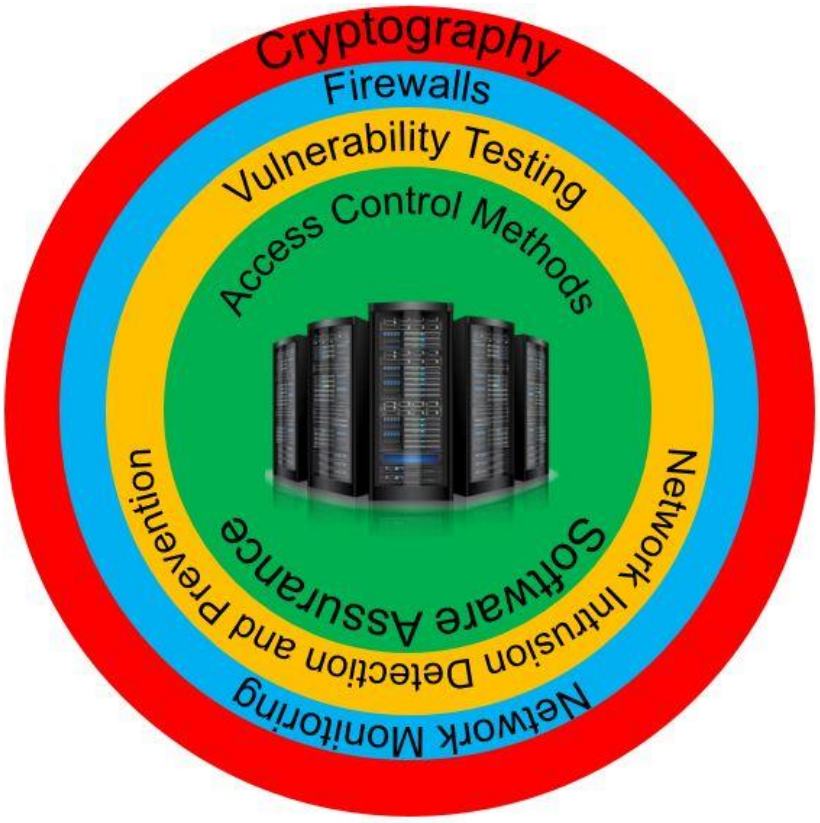

Figure 2 Layers of security

2.0 CYBERSECURITY CHALLENGES

Cybersecurity challenges are different when we move the services and products to the cloud environment for a lab environment. We must concern ourselves with the complications of multiple organizations having access to our products and more importantly, our data. We cannot manage what we cannot control, and we cannot control what we do not manage.

We need to be absolutely certain that we …

- Develop and maintain a clear understanding of what controls the Cloud Service Provider (CSP) provide in Cloud Service Agreements (CSAs)
- Need to depend and approve on CSPs and third-party providers numerous security controls
- Maintain appropriate controls independent of vendor provisions
- Design and configure controls that work well in multiple cloud environments and integrate well with open standards
- Ensure CSPs provide full visibility into their security controls and procedures, as well as any exposure incidents

Questions that we need to ask ourselves …

- Who will do Continuously Monitor, Audit, Report & Risk Manage the data?
  - Roles and Responsibilities
  - Cloud service agreement (CSA)
  - Security controls
  - Data Loss Protection

- How do we effectively protect/secure the data?
  - Business Processes
  - Defence-in-Depth (Perimeter security, IDS, IPS)
  - Cryptography (at-rest, in-transit)
  - Identity Management
  - Access Control

- Where does the protected data reside and where is it stored?
  - Multiple tenants
  - Country laws
  - Sovereignty

2.1 Cybersecurity guidelines

We should be implementing the following guidelines:

- Software assessments
  - Implement software assessment into a measureable process
  - Divide the process into different phases/steps
  - Assign specific criteria to each phase
  - Check the criteria with suitable tools
  - Evaluate results based on standardized models

- Use defined standards for application development (secure software stack)

- Use of secure coding best practices, code analysis and dynamic scanning

- Establish an acceptable common criteria threshold level for incoming services. These criteria will ensure the product is assessed for risk management in the concepts of CIA tenets.
  - Provide a hardened baseline for software application
  - Use vulnerability scores as one of the factors into the common criteria
  - Evaluate the Ports/Protocols/Services, threat/attack vectors, security posture of the service
  - Vulnerability Risk should be calculated by the Severity, Impact, Likelihood, and Confidence values
  - The threshold level product outcome will define the risk assessment of the service within the cloud environment

- Use metadata for security & classification tagging

- Assurance that the data/information is trustworthy and accurate

- Data confidentiality that limits access to information/data

2.2 Cybersecurity Assessment Steps

Cybersecurity Assessment is a process intended to ensure that software to be deployed in a cloud environment has a specific level of cybersecurity. It is a process that is divided into five steps. Each step reviews the software from a different perspective. The overall goal is to ensure a high level of CIA. For this purpose, there are specific criteria for each phase, which are evaluated according to a uniform evaluation standard. This ensures that the individual software systems can be compared with each other. Most of the criteria can be tested for their security with well-known and widely accepted security software. At the end of the process, based on the results of each phase, an assessment must be made as to whether the software (simulation service) is safe enough to be hosted in the cloud environment or not. While 100% security is highly unlikely, this process contributes to a consistent and reproducible security analysis that will increase IT security. The process is not a guide to the secure operation of a cloud infrastructure, but only to ensure that only security-tested software are imbedded into the cloud environment.

Step 1 - Software Architecture Assessment

The goal of the first step is to get an overall view of the system. This includes the determination of the individual system components, its implementation according to design patterns and technologies, the offered cryptographic functions, patch management of the developers and software dependencies. In this step, we analyse the threats that can occur on the architecture. A study of the documentation and used technologies are necessary. As in any other steps, it is important to scale the individual criteria with a score to achieve a comparable overall result for each phase.

Step 2 - Static Code Analysis

The goal of step 2 is to identify security flaws before they become noticeable at runtime. For this purpose, the source code goes through a static analysis scanning with suitable tools looking for specific patterns that indicate potential security flaws.

Step 3 - Host Based Intrusion Detection System (HIDS) / Malware Scan

The goal of step 3 is to detect potential malware in the software system. There are a number of free and cost-based commercial tools capable of providing this. Some programs are specialized to detect rootkits for example, compared to other products that are generally looking for malware. It may be useful to combine several products.

Step 4 – Dynamic Scan

The goal of step 4 is to check the remote-services against known vulnerabilities. All services accessible via TCP and UDP are examined for vulnerabilities using specific signatures. In the simplest way, the type and version of the server software is determined and compared with a regularly updated database for vulnerabilities.

Step 5 - Fuzzing / Load Test

The goal of step 5 is to discover common vulnerabilities without having access to the source code. The system is brought to the limit of its specification by regular test data in order to find errors that are difficult to find by simple function tests. In addition, each input interface of the system is supplied with randomly generated data at the same time the response is monitored. This allows faults in the input handling to be actively found.

Decision

As already indicated in the introduction, it is important to evaluate the criteria of each step with a score. The criteria of a step are summarized and weighted. The Authorized Officer will indicate the overall security risk threshold value. If a threshold is exceeded, regardless of whether it is a step or the overall result of the process, the software cannot be included in the environment.

2.3 Access Control Plan

Access Control Plan defines the policy which describes the purpose, scope, roles, responsibilities, management commitment, compliance, and coordination among NATO organizational entities. It further establishes streamlined procedures, within NATO MSaaS Information Technology (IT), to implement this policy and associated access security controls. This policy and procedure guidance allows the MSaaS IT to manage risks from information asset access through the establishment of an effective Access Control program.

2.4 Identity Access Management (IdAM)

Identity and access management (IdaM) is the process of managing the authentication of user access to a system and/or network. It gives users access to the networks and systems they need, while restricting access to those they do not by creating a unique digital identity.

The username/password combination is becoming obsolete and not secure. The new normal is to use multifactor authentication. The next generation of identity management is behavioural authentication.

Behavioural authentication is a risk-based approach by building a continuous authentication. Behavioural data is collected over time, which will enable machine-learning-driven approaches to correctly identify the identity of the user. Behavioural authentication provides continuous authentication security for account access and transactions by continuously monitoring and scoring, in real-time, the way users interact with their computers and mobile devices via mouse movements, keystroke, and gesture dynamics. These actions, recorded and learned over time, are mapped to the returning user to generate a risk score. When the behaviour of the user, trying to log in, does not match the known user model, the security platform can initiate “stepped up” authentication. This can include requiring additional biometric authentication (i.e. face recognition or fingerprint scan), correct response to a security question, or prompting for a secure one-time password.

3.0 DATA-CENTRIC VS. NETWORK-CENTRIC APPROACH

Data-centric (or Database-centric) architecture has several and distinct meanings, but all meanings are related to software architecture in which the Database plays crucial roles in the architecture. When we mention data-centric in a cloud environment we’re implying a shared database as the basis for communicating between services in distributed computing applications, instead of a direct inter-process communication via message passing through network infrastructure.

The benefit of data-centric architecture, in a distributed environment, is that it simplifies the design by utilizing database management systems (DBMS) that provide transaction processing and indexing to achieve a higher degree of reliability and performance. At the same time, all services states are shared through the DBMS. By implementing the DBMS with clustering capabilities, the services can communicate through multiple cloud environments, while enhancing the security, fault-tolerance, and scalability. Data-centric

favours shared data models over allowing each application to have its own, idiosyncratic data model.

A data-centric model removes the need for application interoperability. By standardizing the data structures and data exchanges, all services can be interoperable. Since all the data is captured within the DBMS, data analysis, data analytics and data monitoring is easier to achieve. Focusing on data interoperability instead on transport and application will reduce costs and inefficiencies associated with application interoperability and network data segregation, while also increasing information availability. Similarly, the implementation of strong identity management, data optimization/standardization, data security and data analytics, will help address defence information security needs while increasing information discoverability and sharing. Focusing on the information-sharing problem in addition to the information security requirement requires an evolution from a 1980s network-centric model to a more modern data management model.

In the modern world of the web, data is the key component of information. The data can be used within the computing application or combined with other data to create information by using business models and calculated algorithms to produce aggregate knowledge. Access to the data is by the advertised Application Programming Interfaces (API). The below figure represents the interaction between the layers of the architecture from the services and the web interfaces all the way to DMBS through API calls.

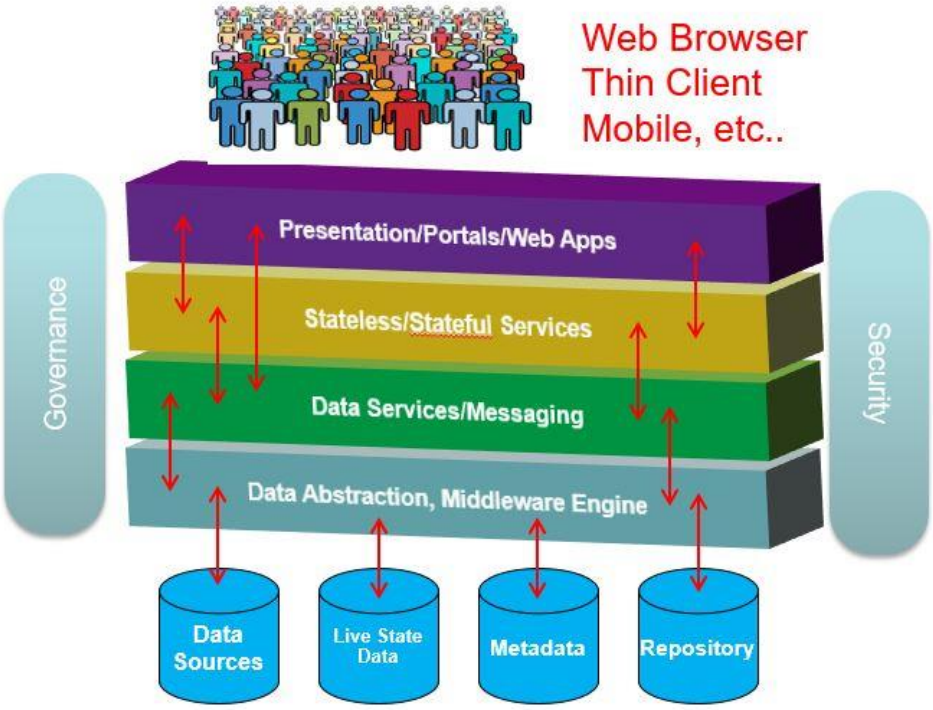

Figure 3 Service Architecture