Snow Leopard Cloud: A Multi-national Education Training and Experimentation Cloud and Its Security Challenges

Erdal Cayirci[1], Chunming Rong[1], Wim Huiskamp[2], and Cor Verkoelen[2]

[1] Electrical Engineering & Computer Science Department,
NATO Joint Warfare Center / University of Stavanger,
Stavanger, Norway
{erdal.cayirci,chunming.rong}@uis.no
[2] TNO Defence, Safety and Security,
The Hague, The Netherlands
{wim.huiskamp,cor.verkoelen}@tno.nl

Abstract. Military/civilian education training and experimentation networks (ETEN) are an important application area for the cloud computing concept. However, major security challenges have to be overcome to realize an ETEN. These challenges can be categorized as security challenges typical to any cloud and multi-level security challenges specific to an ETEN environment. The cloud approach for ETEN is introduced and its security challenges are explained in this paper.

Keywords: Snow Leopard, military simulation, training, shared scenarios, LVC, multi-resolution simulation, exercise, experiment.

1 Introduction

In recent years, modern armed forces have been developing their persistent networks for training, education and experimentation. The US Joint National Training Capability (JNTC) [1], which provides a persistent network for joint (i.e., multi-service, army, navy, air force and marines together) training services, is an example. The North Atlantic Treaty Organization (NATO) is also developing a persistent training capability for NATO, its nations and partners. This initiative is lead by NATO ACT (Allied Command Transformation) and is known as Program Snow Leopard. The enabling network for Snow Leopard is called NATO Education and Training Network (NETN) [2, 3]. The NATO Modeling and Simulation Task Group MSG-068 has been tasked to develop NETN standards and recommendations and to demonstrate their practicality.

Snow Leopard will use the MSG-068 NETN recommendations for delivering to the Alliance and its Partners a persistent, distributed education and training capability that supports training spanning from strategic down to tactical level across the full spectrum of operations, leveraging national expertise and capabilities. Snow Leopard has four pillars organized as separate projects: advanced distributed learning (ADL),

M.G. Jaatun, G. Zhao, and C. Rong (Eds.): CloudCom 2009, LNCS 5931, pp. 57–68, 2009.

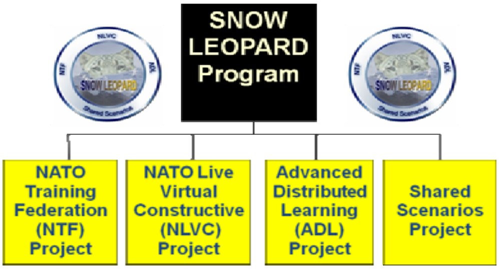
SNOW LEOPARD Program
NATO Training Federation (NTF) Project
NATO Live Virtual Constructive (NLVC) Project
Advanced Distributed Learning (ADL) Project
Shared Scenarios Project

Fig. 1. The Structure of Snow Leopard

shared scenarios, NATO Training Federation (NTF) and NATO Live, Virtual, Constructive (NLVC) federation. These pillars will be available as services to NATO Headquarters, Nations and Partners over a persistent network.

Snow Leopard connectivity should be flexible in the sense that nations and organizations that have access to the Snow Leopard infrastructure will be able to perform exercises or experiments in different configurations. In some cases all nations may want to join a specific event, in other cases, a (small) number of nations may use Snow Leopard for a particular training exercise or mission preparation event. The preparation time to set up a particular event should be minimized as a result of the permanent character of Snow Leopard.

The following applications are foreseen in Snow Leopard:

- Simulation systems (including simulated radio and data links), possibly with hardware in the loop for training purposes.
- Command and control (C2) systems, mainly identical to the applications that are used operationally.
- Video teleconferencing (VTC) for exercise mission briefings, mission planning and after action review. VTC is also used for technical briefings, technical planning and technical after action review.
- VoIP for technical management and control (before, during and after the exercise).
- Network remote management, control and monitoring.
- Network time synchronization (using Network Time Protocol NTP).

Classified data storage and data exchange for planning, training, results, documentation and shared scenarios should also be accessible from all sites [13]. This includes:

- E-mail
- Webservers and collaborative workspaces
- FTP servers (e.g. to distribute scenario data)

A subset of these services and data can be classified as NATO Secret, and may be accessible only for a subset of users. Nations or organizations that are not involved in a particular event taking place on the Snow Leopard infrastructure should not have access to the data related to that event. Therefore, security services are also required for the realization of the concept.

Two NATO training centers have an important role in the implementation of Snow Leopard: Joint Forces Training Center (JFTC) in Bydgoszcz, Poland and Joint Warfare Center (JWC) in Stavanger, Norway, which are responsible for tactical and operational/higher level training respectively. JFTC will be the hub for tactical level live, virtual and constructive simulations called NATO Live Virtual Constructive (NLVC) federation. On the other hand JWC is the hub for another simulation federation called NATO Training Federation (NTF). JFTC and JWC will start providing services from new facilities in 2010 and 2011 respectively. In new facilities both para-virtualization and clustering techniques will be used extensively for operating system, platform, network and application virtualizations.

The MSG-068 TG has already made some key decisions for the simulation infrastructure to fulfill the Snow Leopard requirements: Interoperability between live, virtual and constructive simulations will be based on the High Level Architecture (HLA, IEEE 1516 [7-11]), as agreed by NATO STANAG 4603 [14] and NATO M&S Master Plan [13]. A modular federation object model (FOM) [1, 10] approach will be applied to extend the well-known HLA real-time platform reference FOM (RPR FOM V2). The Combined Federated Battle Laboratories Network (CFBLNet) will provide the secure network link among JWC, JFTC, NATO, Partner and Contact Nations. NETN will allow the centers, headquarters and units in these nations to dynamically access the training, education and experimentation resources, i.e., software, platforms, architectures and data available in JWC and JFTC, as well as in the nations.

Snow Leopard can be a good candidate to create a multi-national joint education, training and experimentation cloud (ETEC). NETN can be perceived as a very large cloud public to accredited sites in nations, and also connects other national private clouds like JNTC. It can provide:

- Shared resources applications like joint exercise management module (JEMM) and joint exercise scenario tool (JEST), simulation systems like joint theater level simulation (JTLS), joint conflict and tactical simulation (JCATS) and virtual battlespace simulation (VBS2)[4] in the form of software as a service (SaaS)
- Central Runtime Infrastructure (RTI) component of HLA, HLA federation execution control tools, exercise logging services, database management systems, Wiki and other web services in the form of platform as a service (PaaS)
- CFBLNet, video teleconference (VTC), voice over IP (VoIP), network control and monitoring, network time protocol servers and other infrastructure elements in the form of infrastructure as a service (IaaS).

An ETEC can also be very useful for civilian purposes like training and education for large scale complex crises response operations because:

- A common architecture and collaboration environment is needed also for civilian purposes, such as, complex national or multinational crises management.
- For local crises management training, small organizations often cannot afford maintaining an organization and architecture for exercising and training.

ETEC can provide not only IaaS, PaaS and SaaS but also other services like exercise/training planning and management. Therefore, ETEC is a very attractive concept for Snow Leopard. However security is a major challenge for the realization of ETEC concept. In this paper we introduce ETEC for Snow Leopard and its security challenges. In Section 2 the conventional approach proposed by MSG-068 and our ETEC approach are introduced and compared. Then we examine the security challenges typical for any cloud in Section 3. Multi level security (MLS) is not a necessity but may increase ETEC capabilities and efficiency considerably. In Section 4 various forms and challenges of MLS are introduced. We conclude our paper in Section 5.

2 ETEC Architecture for Snow Leopard and Its Advantages

In the first quarter of 2009, MSG-068 completed the technical recommendations for Snow Leopard, and the Taskgroup tested the practicality of the recommendations in experiments throughout 2009. The current design of Snow Leopard, i.e., new facilities and MSG-068 recommendations, is depicted in Figure 2.

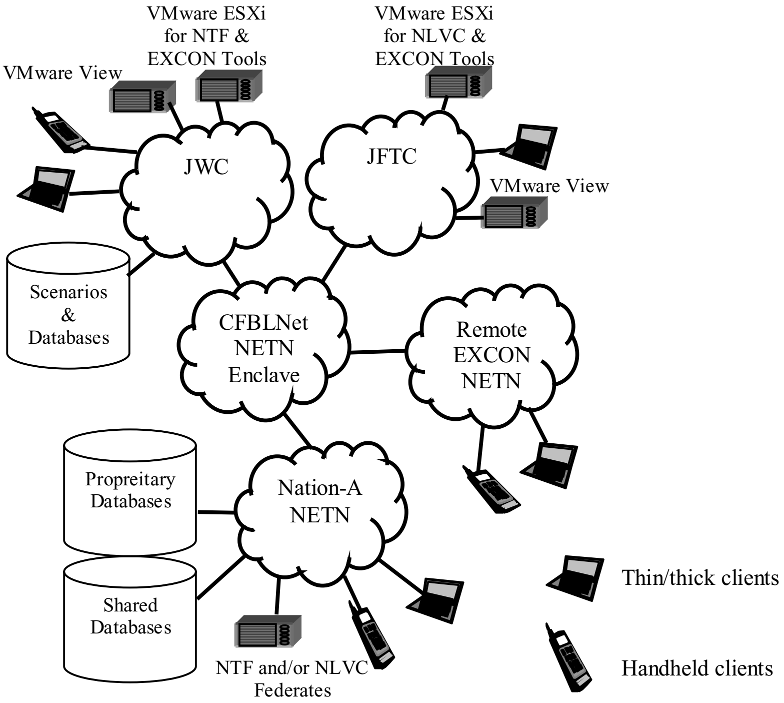

Fig. 2. NETN as it is designed

MSG-068 recommends CFBLNet as the networking infrastructure for Snow Leopard. CFBLNet is a network built and maintained by its members. The network consists of sites, national *Point of Presence* (PoPs), infrastructure, services and knowledge management. The national/organizational PoP is the connection from the national/organizational *Wide Area network* (WAN) to the international part of the CFBLNet WAN. The CFBLNet *BlackBone* (i.e., Black backbone) provides a common, closed, unclassified IP routed network layer implementation using a mixture of both ATM and IP bearer networks. Its primary purpose is to transport encrypted traffic throughout the network. *Enclaves* are the cryptographic protected networks on top of the CFBLNet BlackBone. Each enclave has a *classification* and a *marking* indicating security level and the countries allowed connecting. CFBLNet enclaves can be accredited upto NATO Secret level events. The classification, i.e., NATO Secret, NATO Restricted, NATO Unclassified and Unlimited, of an enclave can change from one event to another. However, an enclave can only have a single classification level at a time. It is possible to connect an enclave to other NATO networks. In this case guards (data-diodes) and firewalls are used to apply strict flow control mechanisms.

MSG-068 also recommends an RPR2 based FOM and HLA 1516-2009 for federating live virtual constructive simulations. The reference Federation Agreement and FOM Document (FAFD) for NETN was completed in May 2009. Since this topic is outside the scope of this paper, we do not give the details about FAFD. Interested reader can find more detailed information about FAFD in [1, 11, 12].

Two important parts of NETN will be JFTC and JWC local area networks (LAN) which consist of completely virtualized services. These networks and all the virtualized functional area services (FAS) running on them will be carefully designed and accredited for each event, i.e., an exercise or experimentation, through a process, which typically lasts 12 months.

Most challenging FAS in this environment are related to computer assisted exercise (CAX) support. There are four classes of CAX services: CAX planning and management, complex military simulation systems, interfaces between simulation and C2 systems and experimentation services. Especially the simulation tools are different from typical services. They are a very complex set of processes that work together and interact with each other. Therefore, JWC is rigorously testing virtualization environments (VMware ESXi and VMware View) for the simulation tools. Most of the results from the preliminary tests run in a small testbed in Stavanger, Norway were positive. Some minor problems were corrected by configuration changes, i.e., higher RAM available, etc. In October 2009, the fully virtualized architecture for computer assisted exercises will be tested for the first time during a major exercise.

In the following years, a new set of services will be introduced with Snow Leopard. The services that include also the new tools can be categorized as follows:

- Advanced distributed learning tools and databases
- Shared scenario and database resources
- NATO training federation (NTF), i.e., an HLA federation made up of constructive, virtual and live simulation systems (Note that NTF was already successfully used in a major exercise).

- NATO live virtual constructive (NLVC) federation for low level tactical training
- Exercise/experiment planning and management tools, such as joint exercise management module (JEMM) and joint exercise scenario tool (JEST)
- All kinds of functional area services (FAS), such as command and control (C2) systems, logistics systems and operational planning tools.

The infrastructure for Snow Leopard, i.e., NETN, is already partly available in JWC and JFTC. NETN will extend it mainly with distributed exercise control (EXCON) capabilities and an architecture that allows national simulation and C2 systems to join NTF or NLVC.

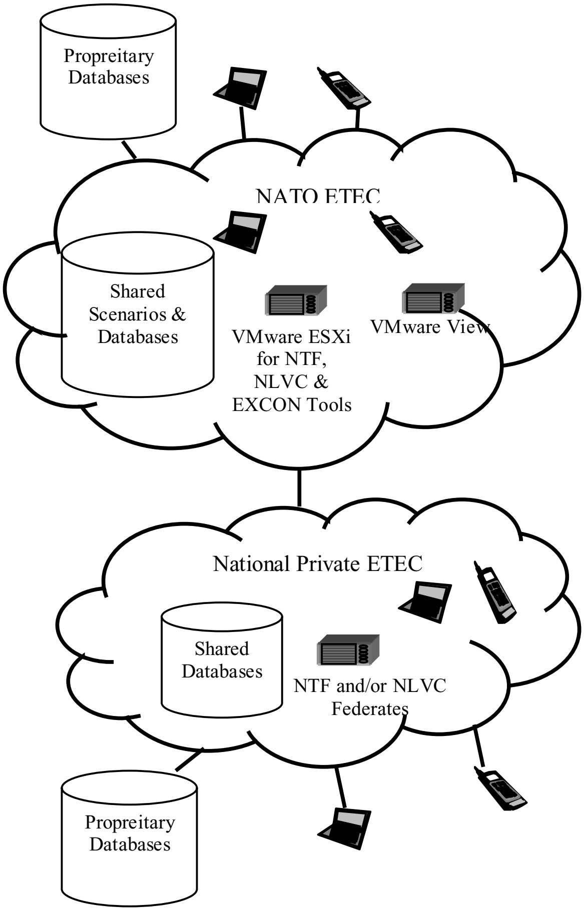

Fig. 3. NATO education training and experimentation cloud

Figure 3 shows the proposed ETEC approach for NETN, which can further increase the efficiency and flexibility of NETN. JWC and JFTC facilities and infrastructure allow quick adaptation of the ETEC approach. National private ETECs can also join the NATO ETEC to create more flexibility and extensive usage. Therefore, we can perceive the overall architecture as a hybrid cloud that has both public and private components. Propriety databases can also be used with this cloud. They may remain outside of the ETEC, but can become available through a controlled access from inside the ETEC. A NATO ETEC can reduce the cost of NATO exercises and experiments considerably because:

- Handheld devices and terminals cheaper than typical client workstations, can use all the services in ETEC without any configuration requirement as long as they can gain access to the ETEC.
- Hardware for servers are procured for only one site.
- Software licenses are obtained for only one site. Licenses may be shared between users that don't require permanent use. For example, VBS2.
- Software and hardware configurations and upgrades are carried out at only one site. Therefore operations and maintenance costs are reduced.

Nations and Partners can use this architecture not only for NATO exercises but also to train their tactical forces for coalition operations more efficiently and less costly. For example several nations can train their tactical forces for a coalition operation without involving any NATO Headquarters by using NATO ETEC. Moreover, such an ETEC can be opened for UN and other international governmental and non-governmental organizations, which cannot afford to procure and maintain such a complex training and experimentation cloud.

However the ETEC approach for NETN also has many challenges and most of these challenges are related to security, especially to multi-level security. In the following sections we explain the security challenges of ETEC.

3 Security Challenges for Cloud Computing

Major security challenges for ETEC, which are also typical for any cloud, can be listed as follows:

Privacy: Users must rely on the ETEC administration for the protection of their privacy and security of their proprietary data because the first and most important difference of ETEC from the conventional approach is that the users do not own the hardware and software. Instead they receive the services available in ETEC based on a per use service model. For a NATO ETEC, there are two sides of this issue: nations and national data, NATO and NATO data. This issue can be even more challenging if Partner and Contact nations are allowed to use NATO ETEC resources. It may be needed to keep some data always invisible to some ETEC users. Alternatively, some data provided by a NATO organization or a nation for use during an event may not be releasable to the participants although they are using it during the event. For example, the JWC exercise flow (JEMM) database for an exercise is not releasable to any nation or NATO organization after that exercise ends. This policy is implemented because some parts of the exercise data can be used in the next exercise. When these data are prematurely available to the training audience of the next exercise it may hinder achieving the exercise objectives. It may be desirable to use own data that is secured locally while receiving IaaS, PaaS and SaaS from ETEC, and sharing these data only with the users approved by the owner of the data. Data segregation, which ensures that reliable encryption is always available, is also an issue related to privacy. Of course encryption brings up the requirement for a secure, efficient and practical key distribution scheme. It is not easy to design a secure key distribution scheme for such a dynamic and flexible environment.

Anonymity and Traffic Analysis: Not only the private data owned by a particular user, but also the anonymity of the users may need to be protected. In addition, ETEC should prevent users from unauthorized analysis of the network traffic to derive some information about the operational postures of the units. For example certain patterns of network traffic among certain headquarters before an air-to-ground attack package starts flying in a simulation during an exercise may be very important intelligence for a user that represents the opposing forces. Therefore, ETEC should protect anonymity and prevent (undesired) traffic analysis. Keeping the data and service locations anonymous and using techniques like load balancing both for servers and networking resources can help dealing with this issue.

Single Point to Attack and Single Point of Failure: Although centralization of services increases the security of a system by reducing the size of infrastructure to protect, that also creates points of gravitation for attacks. Services in a cloud can be a very attractive target for hackers. Moreover, when a system is hacked and/or fails, the impact is much bigger comparing to distributed computation approaches. Therefore, ETEC requires comprehensive intrusion prevention, detection and response techniques and fault tolerance measures. Actually we can state that both clustering and para-virtualization techniques that will be used in JWC and JFTC are naturally fault tolerant. Still there are key services, and when one of them are compromised, all elements in the cloud can be affected.

Large Databases and High Number of Clients: The centralization of services also reduces the probability of configuration errors since there is no need for local system administrators. Therefore, at the first glance it looks like the points that can be exploited by the hackers are less comparing to the conventional approach. However, a cloud typically has huge number of users, much bigger databases and a much higher number of processes. This creates new opportunities for denial of service attacks. For example a single malicious user that uses multiple identities, i.e., sybil attack, can attempt to consume as much system resources as possible. The cloud can be accessible from many different points by many users using generic and simple client devices, it is therefore not an easy task to detect an intruder. Huge databases, high number of users and services also make the detection of bugs, covert channels and bypasses a very difficult task. Therefore each module, component and their contents should be carefully verified and accredited before putting into service. This may increase the time required to modify a cloud or adding a new piece of data or software into it.

Denial of Service (DoS) Attacks in Medium Access Control (MAC) and Higher Layers of Networking Protocols: Malicious intermediate nodes in the routes between the users/clients and centralized services can degrade the service quality. Although this kind of attacks is not specific to cloud computing, users of clouds are more sensitive to it because they are highly dependent on the centralized resources. Resource centralization also makes the organization of such attacks easier. Some examples for this kind of attacks are as follows:

- A malicious node may **selectively forward** the packets coming from the cloud or the users. Although the attack is organized in network layer, it has also effects in transport layer. In transport layer protocols like TCP, a missing packet indicates congestion, which means reducing the transmission speed by starting slow start process from the beginning. Since the malicious node drops only some random packets, it is not easy to discover it.
- A malicious node may not forward any packet to or from a cloud. This attack has a bigger impact comparing to selective forwarding. However, it is also easier to detect and recover from.
- A malicious node can do **acknowledgement spoofing**. There are various impacts of this. By acknowledgement spoofing congestion can be created. Alternatively, acknowledgements can be replayed, which indicates negative acknowledgement in various TCP derivatives like TCP-Reno.
- If wireless links are involved in any part of the communications, the security risks are even higher. For example, clear to send (CTS) signals can be jammed to organize very cost effective and practical jamming attacks in MAC layer for IEEE 802.11. Similarly, request to send signals broadcasted periodically can jam a wireless IEEE 802.11 channel very effectively.

Self-configuring, Self-optimizing, Self-monitoring and Self-healing Procedures: Cloud computing requires algorithms for self configuration, self optimization, self monitoring and self healing. These processes may create opportunities to exploit for security attacks because of two reasons: First their implementation may have some bugs, and a hacker can use those bugs to gain access to a service. Second, a hacker may make these processes misbehave to degrade the services or to gain access to a service. For example a malicious user may change some system variables to show a system resource busy, and make a load balancing algorithm assign no task to the system resource, which is available in reality.

4 Multi-Level Security for ETEC

All the security challenges explained in Section 3 are also valid for an ETEC. In addition to those, an ETEC, especially a NATO ETEC, has another major challenge, which is multi-level security (MLS). Within current collective mission simulation environments all security domains are required to agree on a common security classification. Information kept within each security domain must then be altered to comply with the agreed common security classification. This requires a costly and time consuming effort per collective mission simulation (re)configuration. There is an increasing need for a security solution that enables the sharing of simulation information across these security domains to establish collective simulations without a potential information leakage and confidentiality breach. This problem of information flow has been identified in the NATO M&S Master Plan [13] (Section 3.9).

In the current NETN design, an enclave in CFBLNet can have a single security classification. This means that only users that have a security clearance equal to or higher than the security classification of the enclave can access the enclave, and data that has higher classification level cannot be processed in the enclave. CFBLNet procedures allow changing the security level of an enclave from time to time. However, an enclave can have only a single security classification level at a time. There can be multiple enclaves for NETN with different security classification. Each of these enclaves means separate clouds that require separate servers, i.e., both hardware and software. This can be called multiple single level security (MSL), and seems the only practical option in the beginning. It is also possible to connect enclaves with different security classification through mail guards and firewalls that apply strict flow control mechanisms (e.g. data diodes).

Benefits of a NATO ETEC can be fully achieved when true multi level security (MLS) is realized. That means all users with different clearances can access a cloud, and an automated security mechanism can guarantee the following:

- A user cannot access a service that has higher security classification than his/her clearance. Please note that a service can be software, platform, infrastructure or data in ETEC.
- A process can read and write an object if it has a classification level equal to the classification of the object.
- A process can read an object with a classification label of a lower level than its own clearance.
- A process cannot write to an object with a lower classification level to prevent leakage.
- A process cannot read or write to an object that has higher classification level, which is also related to the first item in this list.

A reliable ***flow control*** mechanism is required in order to meet these requirements. That can be achieved by labeling each data item, service and user with its security classification and clearance, and by implementing procedures for the automated security mechanism based on these labels. Of course, ***service labeling*** is a major challenge when it is an ETEC because an ETEC is characterized by huge number of users and very large databases. Moreover, ***clearance management*** for the users in such a dynamic environment with so many users is not an easy task. We expect that service labeling and clearance management for an ETEC will be much more complex than key management in mobile ad hoc networks.

Efficient ***sanitization*** techniques allow a reader to see parts of a document, which has security classification lower or equal to his/her clearance, although the classification of the overall document is higher. Sanitization is almost a “mission impossible”. First, sanitization requires an intelligence to decide which parts of a service cannot be seen by a particular user and should be removed before serving the user. Second, it also requires an effective and scalable implementation for high number of users and large databases. Please note that some of the services in ETEC, such as live and virtual simulations are real time services and have very stringent latency constraints. Moreover, utilities in some applications make this task harder. For example, some documents may keep editing information to be capable for undoing changes later. Therefore, the parts deleted during sanitization can be undone if the mechanism misses those utilities.

Information kept within a simulator includes for instance models, attributes and values. In relation to simulation new factors complicate the problem of sanitization:

- The value as such of a particular object may be unclassified (e.g. a geographical position as shown on a C2 system), but derived values may be classified under certain conditions. For example, velocity of the object can be derived from its position updates. The average velocity may be unclassified, however, the breaking capabilities or turn rates (when avoiding threats) may be classified.
- Combinations of unclassified values may disclose classified data. For example, position information of a strike package provides details about the doctrines that are used for specific operations.
- Data rates as such may provide classified information.

The ongoing MLS research activity investigates, through use-cases, how information classification and release within the simulation context should be handled. The techniques developed for flow control and sanitization of simulation data should be carefully designed such that adversaries cannot find and exploit covert channels or bypass the security mechanisms.

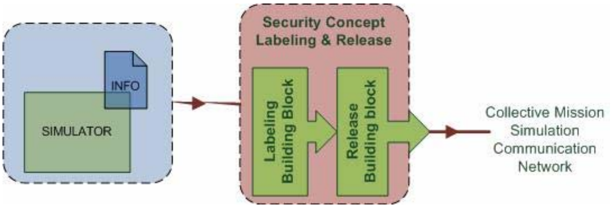

Fig. 4. Labeling and release mechanism for simulations

Finaly HLA components and procedures like object models, RTI and FEDEP may have a role in enhancing security in an ETEC. The information elements of the simulation are described within the Federation Object Model. The FOM is used to determine and define classified information elements. The actual prevention of releasing classified information is initially based on the individual classified information elements using some kind of release mechanism that is integrated into the HLA middleware (RTI).

The proposed security mechanisms/processes to prevent information leakage should become an integral part of the simulator development process, such as the HLA FEDEP (or its successor DSEEP) process.

5 Conclusion

The ACT Program Snow Leopard is aiming to deliver a persistent network that consists of ADL, shared scenarios and live, virtual, constructive simulation capabilities. MSG-068 NETN TG is developing standards and recommendations to be used by Snow Leopard. Technical recommendations are almost completed and testing of these recommendations has started. Virtualization related testing were conducted during a large military exercise in late October 2009. The experimentation and demonstration for overall NETN recommendations will be conducted during a large standalone experiment event in the second half of 2010. These efforts can lead to a multi national education training and experimentation cloud. However, the cloud approach has some major security challenges to tackle with first. Some of these challenges are typical to any cloud. There are also multi level security requirements for fully utilizing ETEC concept. Concepts for addressing MLS in distributed simulation environments have been identified and will be developed and tested in the following years. Once developed and validated, these measures will greatly enhance the advantages and flexibility of ETEC for distributed training in a multi-national context.

References

1. Lofstrand, B., Khayari, R., Keller, K., Greiwe, K., Hulten, T., Bowers, A., Faye, J.-P.: Logistic FOM Module in Snow Leopard: Recommendations by MSG-068 NATO Education and Training Network Task Group. In: Fall Simulation Interoperability Workshop (SIW) (September 2009)
2. Cayirci, E.: Exercise Structure for Distributed Multi-resolution NATO Computer Assisted Exercises. In: ITEC 2007 (May 2007)
3. Cayirci, E.: Distributed Multi-resolution Computer Assisted Exercises. In: NATO Modelling and Simulation Conference (October 2007)
4. Cayirci, E., Marincic, D.: Computer Assisted Exercises and Training: A Reference Guide. John Wiley and Sons, Chichester (2009)
5. McGowan, G., Raney, C.: Integrating Multi-Level Security into the Joint Warfighter Training Environment. In: The Interservice/Industry Training, Simulation & Education Conference (I/ITSEC), Orlando (2008)
6. Knapp, G.F.: The Joint National Training Capability, The cornerstone of Training Transformation. In: NATO Modelling and Simulation Conference, Koblenz (2004)
7. IEEE Std 1516 TM -2000: IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) - Framework and Rules
8. IEEE 1516.1TM -2000: IEEE Standard for Modeling and Simulation (M&S)
9. High Level Architecture (HLA) - Federate Interface Specification
10. IEEE 1516.2TM -2000: IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) - Object Model Template (OMT) Specification
11. IEEE Standard1516.3-2000, IEEE Recommended Practice for High Level Architecture (HLA) Federation and Development and Execution Process FEDEP
12. MSG-068 NETN TG Technical Report Draft 1.3, NATO Modeling and Simulation Group, NATO Research and Technology Organization, Paris (2009)
13. NATO M&S Masterplan (AC/323 (SGMS) D/2 Version 1.0 (1998)
14. NATO STANAG 4603 Modelling and Simulation Architecture Standards for technical interoperability: High Level Architecture (HLA)