Quantitative risk assessment to enhance aeromacs security in SESAR

Mohamed-Slim Ben Mahmoud, Nicolas Larrieu, Alain Pirovano

QUANTITATIVE RISK ASSESSMENT TO ENHANCE AEROMACS SECURITY IN SESAR

Mohamed Slim Ben Mahmoud, Nicolas Larrieu, Alain Pirovano
Communication, Navigation, and Surveillance (CNS) Department, LEOPART Research Team
Ecole Nationale de l'Aviation Civile (ENAC)
Toulouse, France

Abstract

This paper presents the simulation results relevant to the 15.2.7 Working Package of the European SESAR Project[1]. The main goal was to conduct a risk assessment of network security for the AeroMACS airport network. The risk analysis is based on a new approach for network security assessment that measures quantitatively the network risk level. Critical aspects such as the impact of a successful attack on a node and the risk propagation of that attack within an aeronautical wireless airport communication network have been taken into account. We specifically focus on the access network vulnerabilities, and a first network risk study is conducted for a predefined scenario. Some security guideline are provided to enhance the security policies and to improve the end-to-end security using some additional mechanisms such as certificate-based authentication.

I. Introduction and Problem Statement

The growing need for an efficient worldwide airspace system management, generated by an increasing traffic load, requires new capabilities for air-ground data communication technologies. In order to cope with these requirements, the Federal Aviation Administration (FAA) [1], EUROCONTROL [2], and the International Civil Aviation Organization (ICAO) [3] have jointly made specific recommendations for candidate technologies for the airport surface communication network. In the SESAR project [4], the Aeronautical Mobile Airport Communication System (AeroMACS) [5] technology is being developed in such a way as to provide next generation broadband and wireless data communications for airport surface applications (*i.e.* Air Traffic Control – ATC, Airline Operational Communications – AOC, and surface vehicle services). Indeed, the EUROCONTROL/FAA Action Plan 17 jointly identified and recommended this IEEE 802.16e-based system as the solution for the provision of dedicated aeronautical communication services on the airport surface utilizing proposed aeronautical C-band allocations. The AeroMACS technology, designed for short-range and high data rate communications, is very appropriate for the airport surface environment in terms of capability and performance.

AeroMACS should enable rapid and thorough airport communication improvements in forthcoming years. A properly designed, secure airport surface communication system will reliably interconnect pilots, aircraft, and surface equipments with air traffic controllers, airline and airport operators and stakeholders, and new and legacy data sources and applications. As the airport surface communication system involves many heterogeneous application flows, digital information security has been considered as one of the highest priority concerns in the air transport industry. Indeed, since AeroMACS is based on IEEE 802.16e/802.16-2009 [6] standards, it inherits some security flaws specific to the WIMAX technology. Thus, a network risk analysis should be conducted in order to properly design and deploy a secure airport surface communication system, where interconnected aircraft, pilots, air traffic controllers, airline and airport operators can reliably communicate. To mitigate these security issues, the European Sky ATM Research (SESAR) technological and operational program is working under the 15.2.7 Work Package to study the AeroMACS network security using an original risk methodology with propagation based quantitative assessment. Note that WP 15.2.7 *deals with* Airport Surface Datalink issues in general.

Risk assessment has been considered as an essential technique in evaluating the security of network information systems. Many proposals have

[1] *WP 15.2.7 deals with* Airport Surface Datalink issues.

978-1-4673-1900-3/12/$31.00 ©2012 IEEE

been made in this area to design new approaches allowing administrators and engineers to analyze the impact of any attack that could target their systems. Nevertheless, there is a lack of quantitative techniques and methods which take into account the inherent characteristics of a network such as interconnection between nodes. Besides, those standards and methods are related to information security in general and thus, are not entirely appropriate for the specific context of aeronautical communications.

As an example, Aeronautical Radio Incorporated (ARINC) introduced in 2005 the ARINC 811 report [7] entitled a commercial aircraft information security concepts of operation and process framework, but the presented risk assessment approach is static and evaluates damage produced by threats qualitatively, making results somewhat subjective.

Thus, in this paper, we summarize the main concepts of the quantitative approach for network security assessment that measures the network risk level based on critical aspects such as the impact of a successful attack on a node and the risk propagation of that attack within the network. We specifically focused on AeroMACS vulnerabilities, and a network risk study is conducted for a predefined scenario. Some comparative results regarding the authentication protocols (EAP[2] and RSA[3]) supported by the AeroMACS security are discussed. Finally, security guidance are provided to enhance the AeroMACS security features and to improve the end-to-end system security using some additional mechanisms such as certificate-based authentication.

Also, the network security risk assessment methodology applied in the SESAR WP 15.2.7 is transversal and compatible with the security risk assessment methodology used in the SESAR WP 16.2.3[4]. Indeed, the two studies do not have the same abstraction level: on the one hand, our model is applied in a limited scope (*i.e.* AeroMACS access network) and aims to help network designers make their choices (*e.g.* topology, security, risk). On the other hand, the WP 16.2.3 aims to support the development of security management systems in the scope of SESAR and do not focus specifically on the network security, neither the airport communication segment.

II. Aeronautical Mobile Airport Communication System

A. AeroMACS Applications and Operational Services

Potential AeroMACS applications may be grouped into three distinct categories based upon the potential service providers that are most likely to offer these services. In WP 15.2.7, we managed to group traffic flows according to the nature of the service and the affected network entities. This classification has been performed according to the EUROCONTROL/FAA Communications Operating Concept and Requirements for the Future Radio System (COCR) document [8] as the following:

- ***Air Traffic Services***: ATS are executed by air traffic controllers and aircraft. They may be conducted in any of the operational Airport (APT) areas (RAMP, GROUND or TOWER) at both arrival and departure phases. They support safety-critical traffic control operations and clearances. The AeroMACS technology is able to support many ATS operations in airport surface domain such as managing flight plans, evaluating flight conditions before take-off, or monitoring aircraft status;
- ***Airline Services***: AOC services are executed by Airline Controllers and aircraft. They are normally conducted in the RAMP area, but some of them can also be present in TOWER. They support monitoring and operation services that provide aircraft maintenance and boarding actions;
- ***Management Services***: mobile airport services such as surface vehicle services or port authority operations could be managed on the ground using AeroMACS (*e.g.* handover signalization, network management signalization, etc.). Management traffic flows include all the

[2] Enhanced Authentication Protocol (RFC 3748)
[3] Rivest, Aldman, Shamir: A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Comm. of the ACM, Vol 21, 1978.
[4] WP 16.2.3 aims to design new methodologies for security risk assessment.

non-operational message flows that enable signalization for network functions.

In addition, access network management flows are considered according to the WiMAX profile and Network Working Group (NWG) specifications [9]. For each service, we tried to clearly identify a set of information needed in the risk analysis:

- ***Security requirements***: expressed in terms of confidentiality, integrity and/or availability according to the COCRv2 document;
- ***End-to-end communications***: operational services could be unicast (one to one) or multicast/broadcast (one to many). This is an important parameter considering that the risk analysis is based on vulnerability exploit propagation between communicating nodes;
- ***Service directions***: services can be unidirectional, originated in ground or air domains, or bidirectional;
- ***Traffic profiles***: defined using the session duration per service instantiation and the frequency of use of the service in the airport surface domain. Traffic pattern can be different from one service to another: some are periodic (messages are sent in a deterministic frequency), others are potentially random (non predictable message transmission frequency).

It is possible that a single AeroMACS operator (*e.g.* ARINC [10], SITA [11]) can provide the infrastructure to convey all categories of services to all subscribers. However, depending on future SESAR policy decisions regarding competition for services, avionic certification issues, and integration of air traffic, airline, and airport services on a single AeroMACS infrastructure, there may be more than one AeroMACS infrastructure deployment at an airport (cf. the different network topologies discussed later in this paper).

B. AeroMACS Security Considerations

Even if AeroMACS is considered as the best candidate for broadband wireless airport access network, allowing many features with a lot of flexibility, its security is becoming a critical issue with the proliferation of wireless threats. Though incorporating some security methods, AeroMACS is still vulnerable to malicious attacks. Indeed, as far as the technology has been based on the IEEE 802.16e standard, it inherits many mobile WiMAX security vulnerabilities. These vulnerabilities can be grouped into three categories as follows:

- ***Unauthenticated messages***: most of the management messages defined in AeroMACS are integrity protected using a Hash-based Message Authentication Code (HMAC) [12] or alternatively by a Cipher-based Message Authentication Code (CMAC) [13]. However, some messages (*e.g.* MOB_TRF-IND, MOB_NBR-ADV, RNG-REQ) are not authenticated which leads to some vulnerability. Also, some management messages are sent over the broadcast management connection: authenticating this type of message becomes difficult since there is no common key to generate the message digest. Furthermore, a common key would not completely provide message integrity as mobile stations sharing the same key can forge these messages and generate false authentication digests.
- ***Unencrypted management communications***: when an initial network entry procedure begins between a Mobile Station (MS) and a Base Station (BS), many management messages (*e.g.* mobility parameters, power settings, security capabilities) are sent in clear. An adversary may eavesdrop these messages just by listening to the channel in order to establish detailed profiles for MS or BS. More specifically, when the Multicast and Broadcast Rekeying Algorithm (MBRA) is used, encryption keys called Group Traffic Encryption Keys (GTEKs) are distributed to all group members and encrypted using another key, namely the Group Key Encryption Key (GKEK). This GKEK symmetric key is shared and known by all groups which means that a malicious group member may use a new GKEK key to update request for the GTEK key and generate its own GTEK.

- ***Shared keys in Multicast and Broadcast services***: multicast and broadcast messages are encrypted and authenticated using a symmetric shared key between a BS and all MS belonging to the same group: this is an issue in the sense that any MS may impersonate the original BS by forging false multicast or broadcast messages.

Thus, many assumptions need to be analyzed and discussed before implementing and deploying the AeroMACS network infrastructure. The network risk assessment methodology we have developed is a valuable prerequisite in the sense that it could help us to determine which network topology or security policy (*i.e.* with the lowest network risk) provides the most secure system. In the next section, we summarize the main contributions which our risk assessment methodology can make to this research field.

II. An Algorithm for Quantitative Network Risk Assessment Based on Risk Propagation

A. Risk Assessment Principles

Risk assessment is a critical step in the network and information system security risk management lifecycle. Indeed, network security risk assessment could help security administrators to estimate potential damages caused by an illegal intrusion or attack on the system. As an intermediate step in the security risk management lifecycle, it allows us to evaluate the effectiveness of security countermeasures and decide which security policy offers a higher security level for the network. There are many risk management tools. Two examples of which are CCTA Risk Analysis and Management Method (CRAMM) [14] and Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [15].

These tools are compliant with information security standards proposed by the International Organization for Standardization (ISO) [16]. ISO has defined many standards related to information security such as the ISO 2700X [17] standard series. These ISO 2700X standards and methods are related to information security in general and thus, are not very relevant to the specific context of the aeronautical field. A risk management framework for aeronautical information and network security (*i.e.* document entitled ARINC 811) has been defined and introduced by Radio Incorporated (ARINC) in 2005 [18]. ARINC 811 provides additional guidance to deal with physical and operational constraints of aeronautical hardware and software assets relative to airlines, airports, aircraft or flights. The risk assessment approaches used in the risk management methods mentioned above are mostly static and evaluate damage produced by threats qualitatively, making results somewhat subjective. In fact, there are two main network risk assessment approaches:

- ***Qualitative risk assessment approaches***: these models rely on security specialist's expertise and, most of the time questionnaires are used to gather their opinions, as in [19];
- ***Quantitative risk assessment approaches***: these models use a plethora of parameters involved in the risk assessment process, they can be used and designed in many ways based on mathematical and theoretical models as in [20].

Qualitative risk assessment approaches have many shortcomings that can be classified according to three different points of view:

- ***Subjectivity***: as said before, qualitative risk assessment approaches rely on security experts' intuition and past experiences. Usually, a pedestrian risk evaluation is used, *i.e.* a ranking scale is defined (*e.g.* low, medium, or high).
- ***Efficiency***: when qualitative approaches are used, a security administrator is not able to compare two risks classified at the same level in the ranking scale. For instance, giving two Risks (*Risk A* and *Risk B)* ranked high, it would be impossible to compare them. Moreover, it is also impossible to estimate the distance between *Risk A* and *Risk B*. Finally, qualitative risk assessment methods are highly exposed to computation errors. Indeed, data collection analysis requires a human in the loop to complete this process.
- ***Cost***: qualitative security risk assessment approaches are expensive because of the human expertise required.

To some degree, quantitative risk assessment approaches could help to resolve the issues introduced above. Quantitative risk assessment allows a more accurate analysis of risk events compared to qualitative techniques. In fact, a plethora of parameters involved in the risk assessment process can be used and designed in many ways thanks to mathematical and theoretical models. The results are accurate and can be understood easily by administrators and engineers in order to enhance the security of the network. Automated tools are developed for this purpose and present the advantage of accelerating the assessment process and avoiding some computation errors. These errors may occur with qualitative techniques which are usually performed manually. Also, comparison is always possible because risks are evaluated with quantitative values. This is why we have chosen to design a quantitative risk assessment methodology in our research work. Besides, we also considered the risk propagation concept in the assessment algorithm. In fact, there are usually two types of network risk considered when a security risk assessment methodology is about to be designed:

- ***Individual risk per node***: this is the intrinsic risk evaluated on a node. It is deduced primarily by using the vulnerability that can be found for instance on a public vulnerability database such as the National Vulnerability Database (NVD) database [21]. These vulnerabilities can be relevant to design, implementation, protocol stack, Operating Systems (OS), etc;
- ***Network risk***: as a network is considered as a set of several nodes, the network risk is calculated as the sum of all individual risk per node.

However, in a computer network or an information system, nodes interconnection should be taken into account when the network risk for the global system is assessed. Indeed, nodes are connected physically (using an Ethernet connection for instance) and, more importantly, logically (for instance a server node offers different services to another client node). This implies that network security could be compromised by node communications. In the design of our methodology, we used the network risk propagation concept as the key component to assess the risk throughout the entire network. The idea is the following: when an attack occurs on a network node (*e.g.* an AeroMACS MS), it is highly likely that the intruder will try to attack the interconnected nodes when this is allowed by the network topology. The attacker would be able to do so if there were some system assets that could help him to break into a connected node. These assets could be applications, services (intruded on an associated port), user logins (*e.g.* root privilege access), or database access accounts. Furthermore, the dependency between these system facilities implies some kind of transitivity in the network risk propagation process: if a node *i* has some vulnerabilities, it might transmit its correlative risk to a connected node *j*. This risk will propagate to the different nodes connected with node *j*.

Figure1 shows a network security risk propagation example. An administrator user on node *A* is able to log on to a web server (node *B*) using the Secure SHell (SSH) [22] service. Users with root privileges on node *B* are allowed to access to a database (node *C*) in order to read stored confidential data. In order to control the access to node *C*, a firewall (node *D*) is deployed and filtering rules are configured to allow only root users from node *B* to access node *C*. However, if an intruder is able to exploit a vulnerability specific to node *A* (*e.g.* OS vulnerability) to get administrator privileges, he will probably also be able to log on node *B* and access the database without being intercepted.

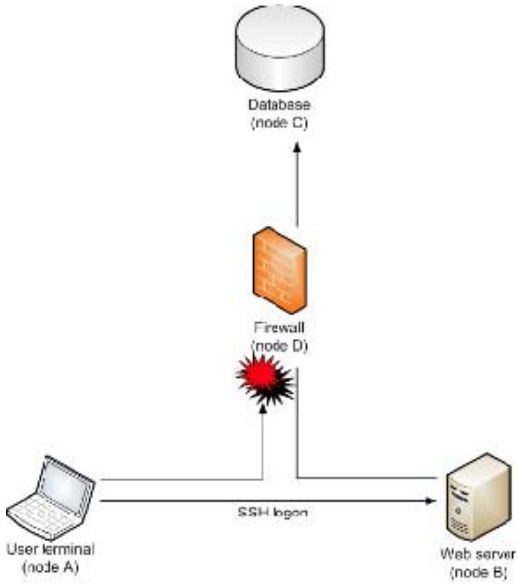

Figure 1. Network Security Risk Propagation Example

B. Propagation Based Risk Assessment Algorithm

We already published the basics of our quantitative network security risk assessment methodology used in SESAR in [23]. Thus, in this section, we only summarize the key components of our risk assessment algorithm. Please note that the different notations used in the following equations are developed in section VI.

The first step of our algorithm estimates the network risk for each node. As a node is connected to other nodes in the network, we evaluate the total risk for a given node i as the product of node value and the sum of individual and propagated risk:

$$Risk_i = Value_i * (Risk_i^{-} + Risk_i^{+}) \quad (1)$$

Considering that network nodes have not the same functionalities, we can assume their degree of importance (or value $Value_i$) in the network may vary. For instance, it is clear that a gateway or a firewall is more important than a simple host or a user terminal. For the aeronautical context, we have considered, besides the node functionality ($FunctionValue_i$ in (2)), the traffic generated by this node. In fact, for our purposes in SESAR there are mainly three traffic classes to consider: the Air Traffic Services (ATS) class for communications between for instance pilot and tower control, the Aeronautical Operational Communications (AOC) class which is relevant to airline information (aircraft maintenance messages for instance), and the Management Services class (e.g. the different control and signalization data exchanged to ensure the establishment of AeroMACS communication mechanisms). Thus, the value of a node i is given by:

$$Value_i = n_i * FunctionValue_i * ClassValu \quad (2)$$

Besides function and class values, we have also considered the total number of connected nodes n_i to node i. Indeed, the total value $Value_i$ increases when a node is logically connected to an important number of nodes in the network (for instance, a flight plan server or a AAA server).

The second parameter considered in equation (1) is the individual risk, namely the host risk specific to a node. The following formula is used to compute the individual risk for a node i:

$$Risk_i^{-} = \sum_{t=0}^{T_i} P_t(i) * I_t(i) \quad (3)$$

For each node, the total number of vulnerabilities T_i and the estimated impact I_t relative to a specific vulnerability t (namely, the t^{th} threat identified on that node) are gathered thanks to the NVD database. The number of vulnerabilities T_i is a simple addition of the existing vulnerabilities for that node.

The likelihood of occurrence of a specific vulnerability $P_t(i)$ represents the possibility that attacks associated with the vulnerability t are conducted. Thus, we use the likelihood of occurrence of a threat exploiting a given vulnerability on a node and its impact on that node. The likelihood of occurrence evaluation is driven by an existing threat analysis methodology [24] proposed by the European Telecommunications Standards Institute (ETSI). However, as the likelihood values are qualitative, we modified this part of the ETSI methodology slightly in order to quantify the parameters involved. Indeed, as described in [24], the evaluation of the likelihood is based on two factors: the technical difficulties that have to be resolved and the motivation for an attacker to carry out an attack.

The ETSI methodology assigns three values to the likelihood function: (1) *unlikely*, if the motivation for conducting an attack is *low* (e.g. no financial interest or technical challenges) and there are *strong*

technical difficulties to overcome (e.g. insufficient knowledge to conduct the attack); (2) *possible*, if the motivation is *moderate* (e.g. reasonable financial gains) and the technical difficulties are *solvable* (e.g. information required to exploit the vulnerability is available); and (3) *likely*, if there is a *high* attacker motivation (e.g. inducing a denial of service on the network, important financial gains) and technical difficulties are almost *non-existent* (e.g. no security protection). In our algorithm, we have made some modifications to the ETSI likelihood evaluation process to replace the qualitative values by quantitative values. First, the likelihood $P_t(i)$ is computed using the motivation and technical difficulties values as shown in equation (4):

$$P_t(i) = \frac{Motivation_t(i)}{TechnicalDifficulty_t(i)} \quad (4)$$

In fact, we think that likelihood of occurrence of a vulnerability t increases when the motivation also increases; otherwise, the likelihood decreases when the technical difficulties that must be overcome increase. The motivation for an attacker to exploit a vulnerability t on a node i is:

$$Motivation_t(i) = Value_i * T_t \quad (5)$$

The equation (5) shows that the motivation increases as the node value or the number of known vulnerabilities increases. Finally, technical difficulties become more significant when security features (e.g. Firewalls) are reinforced (e.g. increasing their number or enhancing the security policies) or when the amount of information required to exploit a vulnerability t is high:

$$TechnicalDifficulty_t(i) = S_t + B_t \quad (6)$$

In formule (6) $B_t > 0$ means that to exploit a vulnerability, some information must at least be available to conduct an attack. Indeed, we make the assumption that an attacker cannot do anything if a minimum of data is not available to start the attacking process (e.g. opened port IDs, user logins, target addresses, etc). Finally, the last parameter of formula (1), namely the propagated risk, is evaluated as the following:

$$Risk_i^+ = \sum_{j=0}^{n_i} \sum_{t=0}^{T_j} P_t(i,j) * I_t(i,j) \quad (7)$$

The idea is the same than the one used in equation (3), the main difference is that the propagated likelihood and impact are induced by all the vulnerable nodes connected with node i. The propagation likelihood of vulnerability t from a node j to a node i is given by:

$$P_t(i,j) = P_t(j) * P(i,j) \quad (8)$$

In fact, the propagation likelihood depends on the likelihood of vulnerability t on the issuing node j and the likelihood of correlation $P(i,j)$ between the two nodes, given by:

$$P(i,j) = \frac{f_{ij}}{F_{ij}} \quad (9)$$

The number of detected f_{ij} (relative to a service concerned by this vulnerability) and total data flows exchanged F_{ij} (which is basically an aggregation of all detected data flows) between two nodes i and j can be directly deduced using some network monitoring tools like NETSTAT[5] for instance. The propagated impact from a vulnerability t from node j to a node i is:

$$I_t(i,j) = Value_i * I_t(j) \quad (10)$$

The propagated impact depends on the affected node value, namely $Value_i$, and the impact of t on the issuing node j (cf. NVD database which provides CVSS[6] vulnerability scores). This CVSS score helps to quantify the impact of occurrence of a threat.

Then, the risk for a given node is the sum of its individual risk and propagated risk. Finally, we calculate the total risk as the sum of all the network risks relevant to each node in the network:

$$Risk_{net} = \sum_{i=0}^{N} Risk_i \quad (11)$$

[5] http://linux-ip.net/html/tools-netstat.html

[6] The Common Vulnerability Scoring System (CVSS) score [25] is provided by the NVD vulnerability database.

IV. Security Risk Assessment Simulation Campaign

A. Simulation Scenarios and Topology of Study

In order to apply our quantitative risk analysis methodology, we introduced the different additional network segments (Air Navigation Service Provider (ANSP), Airlines and Airport operator networks) that should be interconnected through the AeroMACS network. Nevertheless, this topology does not take into account additional network segments that can be consider for an real airport topology. This is why we consider our topology as an isolated scenario.

This scenario definition is also based on the different security options which can be foreseen for the AeroMACS (for instance RSA vs EAP authentication protocols). Nine AeroMACS base stations, twelve aircrafts and ten surface vehicles have been included in the network topology.

In this scenario, the AeroMACS (and the AAA server) is the only system supporting security features which prevent attacks and ensure the provision of ATS and AOC services. The AAA server will be directly reachable through a dedicated gateway between the AeroMACS network and the other Airport networks. The APC server refers to the AirPort Communications server (and not to the Airline Passenger Communication server as it may be the case in other publications [23]).

Figure 2 illustrates the AeroMACS topology relevant to the results presented in this paper.

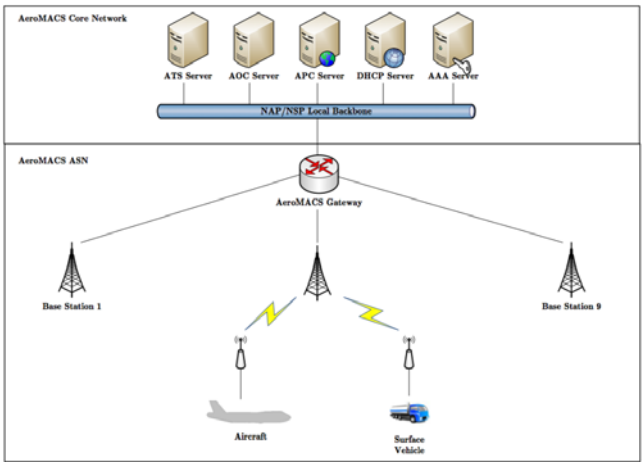

Figure 2. Network Topology (AeroMACS Isolated Scenario)

Table 1 provides interconnection details for this isolated scenario.

Table 1. Topology Details

Node ID	Number of connected nodes	Number of security protections	Number of vulnerabilities
Base Stations	**3/4/5**	**8**	**1**
Aircraft	**1**	**2**	**0**
Surface vehicles	**1**	**2**	**0**
AAA Server	**1**	**3**	**20**
DHCP Server	**1**	**1**	**64**
ASN Gateway	**14**	**2**	**1**
ATS Server	1	1	47
AOC Server	**1**	**1**	**47**
APC Server	**1**	**1**	**13**

Please note that, in a short future, an AeroMACS global configuration scenario will be defined within the scope of the WP 15.2.7. The AeroMACS (and the AAA server) will be integrated in a global network infrastructure including security features at other levels (firewall for instance) than link layer (eg AeroMACS security mechanisms). This approach will be based as far as possible on realistic network architecture (*e.g.* existing ACSP and ANSP interconnections). In this future scenario, the AAA server will be reachable through a dedicated gateway plus a dedicated Airport management network where the AAA server will be deployed. In this scenario, we will consider internal and external AeroMACS security issues with an end to end security management approach. However, the results of this end-to-end scenario are not yet finalized and consequently are not presented in this paper. Thus, the experimental results presented in the next section focus on the isolated scenario introduced at the beginning of this section.

B. Experimental Results

Figure 3 depicts the individual risks for all the network nodes.

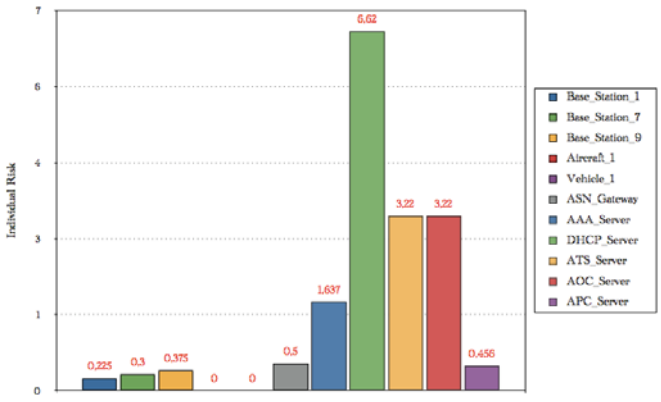

Figure 3. Individual Risks for all Network Nodes

As we can see, base stations and the ASN gateway individual risks are relatively low, because there is only a single vulnerability for these nodes. Despite having the same specific vulnerability (CVE-2008-1542[7]), there is a difference (evaluated from 0.07 to 0.15) between BS 8, BS 9 and individual risks for the first seven base stations. This difference is due to the fact that the first seven base stations are connected to three nodes (an aircraft, a surface vehicle, and the ASN gateway). BSs 8 and 9 are connected respectively to 4 and 5 nodes (plus one or two aircraft). Therefore, the base stations do not have the same node value as it increases when the number of connected nodes grows (see formula (2) in previous section for details).

The different function and traffic class values for each node used for this simulation are summarized in Table 2:

Table 2. Node Characteristics

Node ID	Function value	Class value
Base Stations	**1**	**1**
Aircraft	**0.7**	**1**
Surface vehicles	**0.7**	**1**
AAA Server	**0.3**	**1**
DHCP Server	**0.3**	**1**
ASN Gateway	**0.3**	**1**
ATS Server	**0.3**	**1**
AOC Server	**0.3**	**0.7**
APC Server	**0.3**	**0.1**

Another interesting result is that individual risks are very close for the APC server and the ASN gateway (respectively 0.46 and 0.5) despite a big difference in the number of intrinsic vulnerabilities on each of them (respectively 13 and 1).

As a result of this, we can expect a higher individual risk for the APC server node as it has more vulnerabilities. However, the ASN gateway compensates the gap with the highest node value in the network (equal to 14) whereas the APC server, giving it functionality and traffic class value, is the lowest one (equal to 0.03).

The DHCP server node is the most vulnerable node in the network, and consequently has the highest individual risk in this topology (assessed to 6.62). The FreeRadius server is the most vulnerable node in the network with 64 vulnerabilities and very high CVSS scores: 92% of these them have the top CVSS score (meaning 10, the highest score in the NVD database). Even the lowest CVSS score is relatively high (9.3) if we compare it to the vulnerability scores for base stations or ASN gateway (respectively 7.5 and 5.0). Finally the AAA, ATS and AOC servers, regarding the assumptions made in the inputs, show medium individual risk values.

Except for the ASN Gateway individual risk value which is affected by the high value of the node, all the individual risk values we have measured appear to grow with the number of exploitable vulnerabilities per node taken from the NVD database (according to the different vulnerabilities provided by the inputs) as shown in Figure 4.

[7] Vulnerability details as it appears in the NVD: base station has «topsecret» as its password for the root account, which allows remote attackers to obtain administrative access via a telnet login

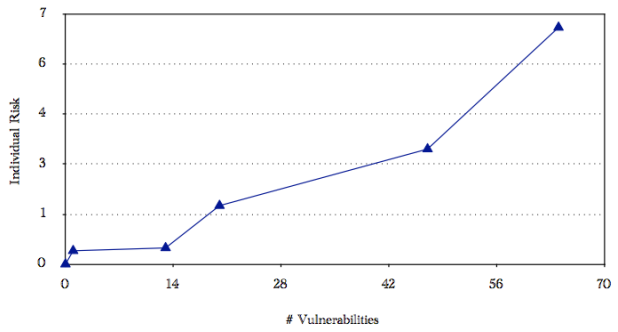

Figure 4. Individual Risk Evolution as a Function of Vulnerabilities

Regarding the assumptions made for the inputs of the current simulation, we can say that the individual risk depends on the number of vulnerabilities per node. Figure 5 illustrates the distribution of the CVSS score for each node in the network (please note that the terminology and taxonomy used in the NVD database has been respected):

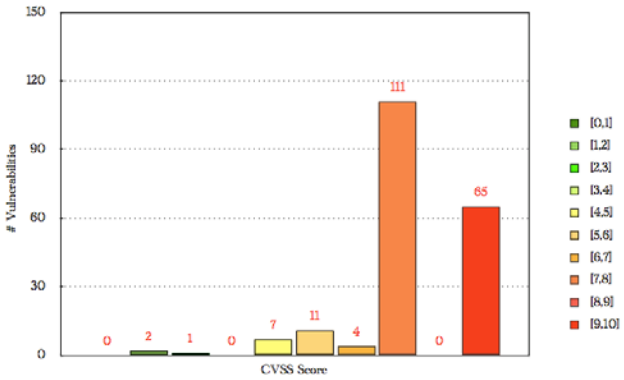

Figure 5. Vulnerability CVSS Statistics

The majority of the scores are ranked in the [7,8] NVD CVSS interval (and represent 55% of the total vulnerability scores). The maximum CVSS scores ranked between 9 and 10 are in most cases relative to the DHCP server node which explains why this node has the highest individual risk value among the network. The average CVSS score has been measured to 7.93.

Table 3 summarizes the propagated risk values for the different nodes in the network:

Table 3. Propagated Risks for All Network Nodes

Node ID	Propagated Risk
Base Stations (1 to 6)	**7. 47**
Base Stations 7 and 8	**9. 96**
Base Station 9	**12. 45**
Aircraft (1 to 6)	**0. 81**
Aircraft (7 to 12)	**1. 08**
Vehicle (1 to 6)	**0. 81**
Vehicle 7 and 8	**1. 08**
Vehicle 9 and 10	**1. 35**
ASN Gateway	**538. 99**
DHCP Server	**1. 20**
AAA Server	**1. 20**
ATS Server	**0. 39**
AOC Server	**0. 75**
APC Server	**0. 13**

The propagated risk results are mainly impacted by the importance of the connected node number parameter in the algorithm. For instance, we have made assumptions regarding the topology of this scenario for the base stations: the first 6 base stations are connected to three nodes (*i.e.* one aircraft, one vehicle, and the ASN gateway), base stations 7 and 8 are connected to four nodes (another vehicle plus) and the last base station to five nodes. The remaining parameters (security protection, offered service, exchanged data, number of NVD vulnerabilities) are always the same. However, the propagated risk values are slightly different (ranging from 7.47 to 12.45) because of different correlation density in the network.

The propagated risk for the aircraft also deserves to be deeply discussed. As we can see, it is not the same for the 6 first aircraft (equal to 0.81) as the 6 last ones (equal to 1.08). However, the justification does not lay in the connected node parameter this time as far as all aircraft are connected to a single base station. The difference between propagated risk for the aircraft (assessed to 0.27) is due to the individual risk specific to the base station to which the aircraft is connected to. DHCP, AAA, ATS, AOC, and APC servers have all low propagated risk values (ranging from 0.13 to 1.20) because all of them are connected to a single node (the ASN gateway) which has a very low individual risk (equal to 0.5).

As we can see, the most important result in this simulation is the propagated risk value of the ASN gateway which supersedes all the remaining nodes. This is likely due to a high node correlation for the

ASN gateway: as far as it is the 'corner stone' of the topology where all node exchanges have to pass through the gateway, it is logically impacted by the other nodes and their specific vulnerabilities. The concept of propagated risk relies in the importance of the connected node number parameter as shown in Figure 6.

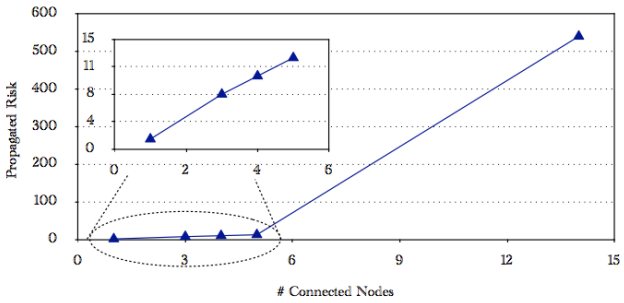

Figure 6. Propagated Risk Evolution as Function of Connected Nodes

The node risk of the ASN Gateway is hardly impacted by the high propagated risk of the node (cf. formula (1) of node risk evaluation). Besides, the high node value of the ASN Gateway plays a major role in the growth of the node risk value: even the highest node risk (which is relevant to the Base Station 9) is 117 times smaller than the ASN Gateway node risk. Consequently, as the network risk is given by the sum of the node risk, the network risk is mainly represented by the ASN Gateway node risk (96.12%) as we can see in Figure 7.

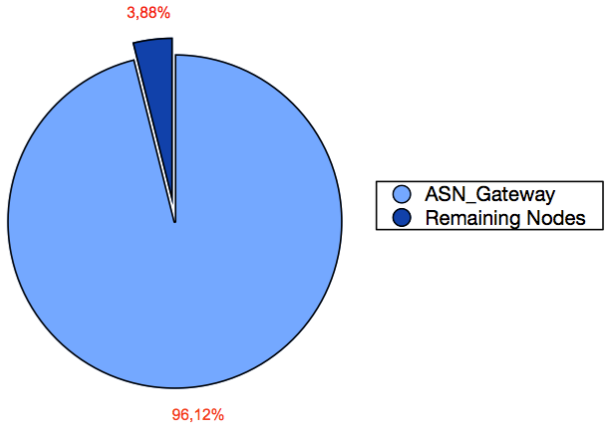

Figure 7. Percentage of Network Risk per Node Risk

Figure 8 shows the contribution (%) of each connected node with the ASN Gateway propagated risk.

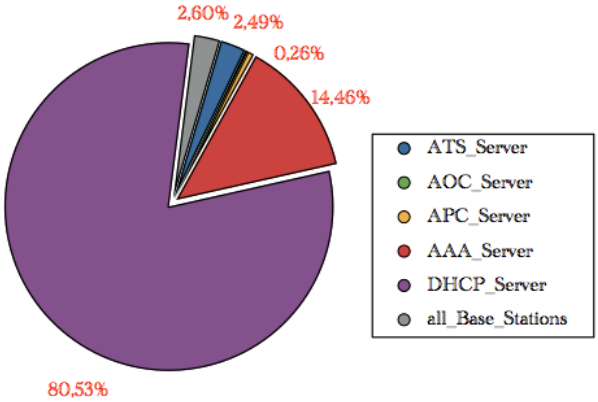

Figure 8. ASN Gateway Propagated Risk Contribution per Connected Node

It is clear that the DHCP server represents the biggest contribution in the propagated risk of the ASN gateway node and is the main actor of this high risk value. This means that if we want to get the ASN gateway node risk lower (and consequently the entire network risk) we should tweak two related parameters:

- The number of connected nodes is really important and should be limited per node as much as possible. This can be first done by some topological considerations that allows the network risk to be less high than in this first simulation ;
- The ASN gateway is the bottleneck of this risk analysis as we already saw in the previous results. Despite its high node connectivity, its high propagated risk value is not directly due to the number of interconnected nodes, but rather to the high individual DHCP server individual risk, the high correlation that exists between the two nodes (the ASN gateway is the only node connected with the DHCP server node) and the high node value of the ASN gateway.

As it has been previously mentioned, AeroMACS privacy sublayer is able to support both EAP and RSA for device and user authentication and authorization. Thus, we have slightly modified our initial scenario to introduce these two AeroMACS security mechanisms. The aim of this scenario is to compare the effects of these security options on the AeroMACS air interface on the global network. Currently, only one option can be chosen, which is

using RSA or EAP as authentication and authorization protocol. Much vulnerability has been found for both security mechanisms. It is worthy to notice that EAP has several methods defined in IETF RFCs (for instance EAP-TLS, EAP-AKA or EAP-SIM), however the NVD vulnerability database does not give much information on these methods: it is only mentioned that the vulnerability is relevant to the EAP protocol.

The NVD database clearly indicates a higher number of vulnerabilities for RSA (*i.e.* 33 vulnerabilities) compared to EAP (only 4 vulnerabilities). Indeed, RSA is much more known and used over all IT systems in the world. Then, it is quite logical to find more vulnerabilities inputs in the database compared to EAP. Nevertheless, the vulnerability statistics we made in this simulation shows that the number of vulnerabilities is not the only indicator on which security mechanism we should privilege.

Figure 9 shows the CVSS score distribution in both EAP and RSA security configurations.

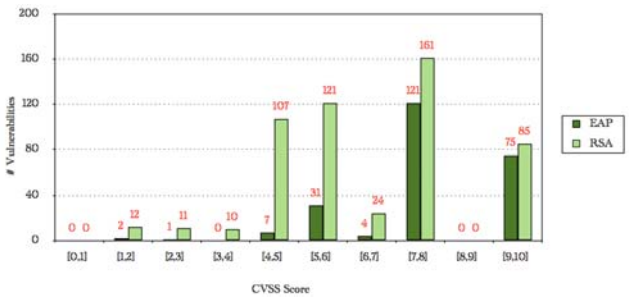

Figure 9. Vulnerability CVSS Score Distribution (EAP vs. RSA)

Indeed, despite a higher number of vulnerabilities (29 vulnerabilities more), RSA remains more secure than EAP: as we have seen in the initial simulation, the average CVSS score is a safer criteria if we want to compare two or more security mechanisms in the NVD database. The average CVSS score (on the total vulnerabilities in the AeroMACS network) has been evaluated to 6.32 for RSA and 7.79 for EAP.

However, the average CVSS score should be weighted accordingly to the individual risk values obtained after the simulation. Indeed, Fig. 10 shows the individual risk values updated for the base stations and the ASN Gateway (all the remaining nodes are not represented since there is no change to notice on them). The higher number of vulnerabilities for RSA makes naturally the individual risk higher than EAP for both base stations and the ASN Gateway (+16.35 and +14.8 respectively for RSA and EAP). These results suggest first that the number of vulnerabilities remains an important parameter because the individual risk is computed as a sum of likelihood of occurrence of a threat and its impact on the total number of vulnerabilities: since RSA has much more inputs in the NVD database, the individual risk relevant to EAP is lower.

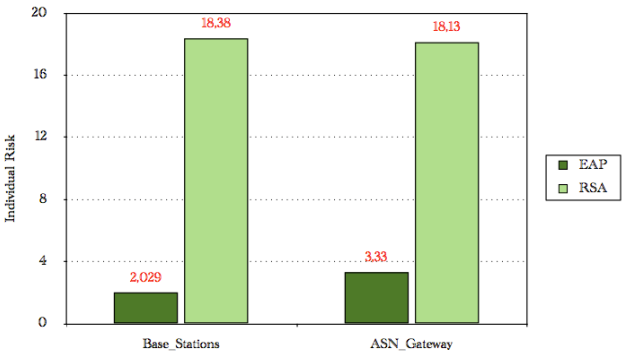

Figure 10. Base Stations and ASN Gateway Individual Risks (EAP vs. RSA)

As a conclusion, if we want to take the risk individually by node, it is clear that EAP should be used for authentication and authorization in the AeroMACS nodes. However, the propagated risk results should be also considered to effectively make final guidance on the use of EAP or RSA protocols. Figure 11 shows the propagated risk values using EAP or RSA protocols for all network nodes.

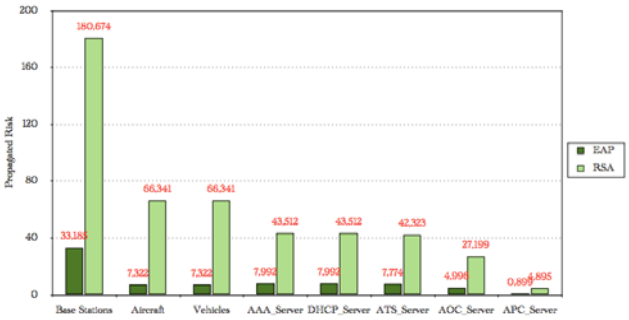

Figure 11. Propagated Risks for All Nodes (EAP vs. RSA)

The same comment for the individual risks remains true here: the EAP authentication protocol induces a lower propagated risk compared to the RSA protocol.

The ASN gateway is still the bottleneck in both sub-scenarios since it has the largest propagated risk among all the network nodes (1042.64 and 2499.87 respectively for EAP and RSA). We can notice that it still has the biggest contribution in the global network risk (either for EAP or RSA) as illustrated in Figure 12.

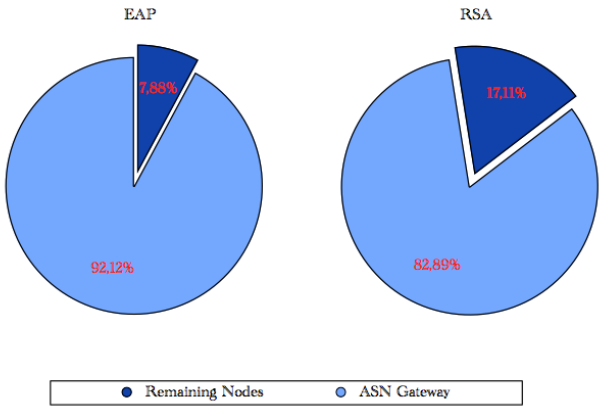

Figure 12. Percentage of Network Risk per Node Risk (EAP vs. RSA)

C. Security Profile and Guidance

Even if the results of this first scenario could be discussed again regarding the end-to-end AeroMACS topology simulation results, we can already draw up some guideline that will allow us to decrease the risk level for the different network nodes:

- *Implementation guidance*: network nodes should be chosen wisely with a minimum of intrinsic vulnerabilities. IP COTS nodes (AAA server, DHCP server) should be selected taking into account the number of the exploitable vulnerabilities and their respective CVSS scores. It would also help to establish a state-of-the-art of the potentially usable IP nodes (particularly the DHCP server node), classify them by number of vulnerabilities and CVSS scores and see how the individual risk per node is affected. The nodes to be preferred are obviously the nodes with the lowest individual risks. Also the simulations of the RSA vs. EAP scenario showed that EAP induces a lower risk (individual, propagated, and network risk) for the isolated AeroMACS topology.
- *Topological guidance*: as we have seen, the global network risk is increased primarily by the propagated risk values (more than the individual risk values) because the node connectivity is taken into account at this step of the risk assessment process. It is clear that the ASN gateway is the main issue in this topology and some countermeasures should be taken to avoid this problem. For instance, an important improvement would be to select two ASN gateways, each connected to a set of base stations and IP nodes as it appears in the AeroMACS network reference model. This is likely to provide less node correlation between the ASN gateway and highly impacted IP nodes (such as the DHCP server) and consequently to decrease the network risk.
- *Security guidance*: now that we have clearly identified the most constraining node in the network and their respective contribution to the global network risk, some security mechanisms ought to be deployed in order to limit the propagated risk. Particular attention should be given to the connectivity between the ASN gateway and the IP nodes such as the DHCP server. One of the best way to deal with this connectivity problem is the use of firewalls. The main advantage of firewalls is that they are able to limit the data exchanges between a highly vulnerable node and the ASN gateway. Also, maximizing security protections at a layer-2 (typically AeroMACS security) should also help the propagated node risk decrease for AeroMACS-based nodes (*i.e.* base stations and mobile stations).

V. Conclusion and Future Work

Network security evaluation is a critical process in network risk management. Nevertheless, most existing network security evaluation models do not provide a quantitative analysis. Another concern is they do not consider all risk aspects related to networks such as risk propagation. In order to address these concerns, we developed a new risk assessment method for network computer systems. Our approach

relies on quantitative measurements using risk propagation and node correlation principles. This network security risk assessment methodology has been applied in the scope of the SESAR 15.2.7 WP for airport communications. Some of the AeroMACS security features have been discussed regarding the results of the simulation campaign. The preliminary results obtained for the isolated AeroMACS topology show security features at higher layers of the protocol stack are needed in order to lower the network risk for the airport communications. The next phase of our work is to clearly define an end-to-end network topology (integrating firewalls, onboard nodes, other IP servers), and to compare the network risk results to the values presented in this paper. The security guidance could then be updated in order to assist future AeroMACS designers in their security and implementation strategy definition.

VI. Nomenclature

Table 4 details the different notations used in the different sections of this paper.

Table 4. Notations

Notation	Description
$FunctionValue_i$	**Function value of a node *i***
$ClassValue_i$	**Class value of a node *i***
$Value_i$	**Total value of a node *i***
$Risk_i^T$	**Individual risk evaluated on node *i***
$Risk_i^\dagger$	**Propagated risk evaluated on node *i***
$Risk_i$	**Total risk evaluated on node *i***
$Risk_{net}$	**Total network risk**
N	**Total number of nodes in the network**
n_i	**Number of nodes connected with a node *i***
T_i	**Total number of vulnerabilities detected on node *i***
$P_t(i)$	**Likelihood of occurrence of vulnerability *t* on node *i***
$I_t(i)$	**Impact induced by a vulnerability *t* on node *i***
$Motivation_t(i)$	**Motivation of an attacker to exploit a threat *t***
$TechnicalDifficulty_t(i)$	**Technical difficulty level to exploit vulnerability *t* on node *i***
S_t	**Number of security mechanisms used to protect a node *i***
B_t	**Number of information required to exploit vulnerability *t***
$I_t(i,j)$	**Propagated impact of *t* from node *i* to node *j***
F_{ij}	**Number of total flows between two correlated nodes *i* and *j***
f_{ij}	**Number of detected flows between two correlated nodes *i* and *j***
$P_t(i,j)$	**Propagation likelihood of *t* from node *i* to node *j***

References

[1] FAA official web site: http://www.faa.gov/

[2] EUROCONTROL official web site: http://www.eurocontrol.int/

[3] ICAO official web site: http://www.icao.int/

[4] SESAR official web site: http://www.sesarju.eu/

[5] EUROCONTROL, "Ieee 802.16e System Profile Analysis for Fci's Airport Surface Operation", Ed. 1.3, General release, 2009.

[6] IEEE Wimax official web site: http://standards.ieee.org/about/get/802/802.16.html

[7] Aeronautical Radio Inc. (ARINC), "Commercial Aircraft Information Security Concepts of Operation and Process Framework," ARINC Report 811, December 2005.

[8] EUROCONTROL, FAA, "Communications Operating Concept and Requirements for the Future Radio System", version 2, 2002.

[9] Wimax Forum official web site: http://www.wimaxforum.org/

[10] ARINC official web site: http://www.arinc.com/

[11] SITA official web site: http://www.sita.aero/

[12] RFC 6151, "HMAC: Keyed-Hashing for Message Authentication", February 2007.

[13] National Institute of Standards and Technology NIST, "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication", NIST Special Publication 800-38B, 2005.

[14] CRAMM official web site: http://www.cramm.com/

[15] Christopher J. Alberts and Audrey J. Dorofee, "Managing Information Security Risks: the OCTAVE Approach," Addison-Wesley, June 2002.

[16] ISO official web site: http://www.iso.org/

[17] ISO/IEC 27005:2008, "Information Technology, Information Security Techniques, Information Security Risk Management," International Standard, 2008.

[18] Aeronautical Radio Inc. (ARINC), "Commercial Aircraft Information Security Concepts of Operation and Process Framework," ARINC Report 811, December 2005.

[19] S. P. Bennett and M.P. Kailey, "An Application of Qualitative Risk Analysis to Computer Security for the Commercial Sector," in Proceedings of the 8th Computer Security Applications Conference, pp.64-73, November 1992.

[20] M.S. Ahmed, E. Alshaer, L. Khan, "A Novel Quantitative Approach for Measuring Network Security," IEEE International Conference on Computer Communications INFOCOM, 2008.

[21] NVD official web site: http://nvd.nist.gov/

[22] OpenSSH official web site: http://openssh.com/

[23] Ben Mahmoud M.S., N. Larrieu and A. Pirovano, " A Risk Propagation based Quantitative Assessment Methodology for Network Security – Aeronautical Network Case Study", 6th Conference on Network Architecture and Information Systems Security, May 2011.

[24] European Telecommunications Standards Institute (ETSI), "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis," Technical Specification ETSI TS 102 165-1 V4.1.1, 2003.

[25] M. Schiffman, "A Complete Guide to the Common Vulnerability Scoring System (CVSS)," in press, June 2005.

Email Addresses

Mohamed Slim Ben Mahmoud: slim.ben.mahmoud@recherche.enac.fr

Nicolas Larrieu: nicolas.larrieu@enac.fr

Alain Pirovano: alain.pirovano@enac.fr

2012 Integrated Communications Navigation and Surveillance (ICNS) Conference

April 24-26, 2012