Applying the SecRAM Methodology in a Cloud-based ATM Environment

Antonio Marotta[(2)], Gabriella Carrozza[(1)], Luigi Battaglia[(1)], Patrizia Montefusco[(1)], Vittorio Manetti[(1)]
[(1)]SESM S.C.A.R.L, Via Circumvallazione Esterna di Napoli, Zona ASI, 80014 Giugliano (NA), Italy
Phone: +39-02-503-30066, Fax: +39-02-503-30010, Email: {pmontefusco, lbattaglia, gcarrozza, vmanetti}@sesm.it
[(2)]University of Naples Federico II DIETI, Via Claudio 80125 Naples, Italy, antonio.marotta@unina.it

***Abstract* – The SESAR ATM Security Risk Assessment Methodology (SecRAM) aims at providing a methodology to be applied by the SESAR Operational Focus Areas (OFAs). To give effectiveness to the evaluation of SecRAM, Air Traffic Management (ATM) operative scenarios are greatly required. In this paper we leverage a Cloud-based approach to build up a virtualized replica of a real Air Control Centre (ACC) in order to realize a vulnerability analysis and to find some possible points of attacks. Then we applied the SecRAM methodology on our test-bed and we built a real threat scenario for which a risk treatment is properly designed.**

***Keywords* – SESAR SecRAM, ATM testbed, Cloud Computing, quality assessment, risk mitigation**.

I. INTRODUCTION

Classified as Critical Infrastructure, the Air Traffic Management (ATM) system represents a suitable example of complex System of Systems: it really consists in a large number of heterogeneous HW/SW systems that are typically spread over different Air Traffic Control (ATC) centres within a single country. A national ICT Service Provider is usually responsible for guaranteeing Confidentiality, Integrity and Availability (CIA) of ATM data exchanged across a Wide Area Network (WAN), whereas the Air National Service Provider (ANSP) is responsible for both safety and security of ATM functionalities (as foreseen in the regulation EC 1035/2011 [1]). To improve the robustness of the whole ATM system against possible threats, such kinds of systems are often built up in redundant configuration over a distributed infrastructure.

Due to the lack of shared risk assessment methodologies in the whole ATM community, the Single European Sky ATM Research (SESAR) SWP16.2 [2] defined a new methodology, namely the SESAR ATM Security Risk Assessment Methodology (SecRAM) [3]. Nowadays SecRAM represents the foundation for the application of cost-effective, proportionate and reliable security measures within each part of the ATM system, and it aims at providing a methodology to be applied by the SESAR Operational Focus Areas (OFAs).

In order to realize a vulnerability assessment a real ATM scenario is required, but this process could obviously lead to troubles when you use the real system. With the aim to overcome the aforementioned obstacle, we propose the adoption of a Private Cloud Infrastructure implementing the IaaS (Infrastructure as a Service) model [4] to build up a full Air Control Centre (ACC) that is a replica of a real and operating system, and then to apply on this latter the SecRAM methodology, after assessing the vulnerabilities of the system.

Nowadays Cloud Computing is a key technology on which both academia and industry focus their research interests. The aim of the IaaS Cloud paradigm is to provide IT resources as services delivered through the network, by hiding in such a way the sophistication of the underlying infrastructure, and to guarantee the dynamic allocation of such resources against the current load. In the scenario we are depicting, we leverage the use of the Cloud technology to reproduce real world scenarios encompassing distributed systems, e.g., several ATC centres belonging to the same system and deployed over different cities in a given country, and to set up test-bed platforms for security assessment, namely to perform all the stages suggested by the SecRAM methodology: (i) risk identification, (ii) risk evaluation, (iii) risk treatment.

Furthermore, concerning the latter aforementioned step, we properly designed and realized a Cloud-based mechanism allowing the secure and transparent migration of virtual resources (namely Virtual Machines) that host system components affected by recognized threats.

The paper is structured as follows. In Section II a brief overview on the SESAR SecRAM methodology is carried out; in Section III a description of the Private Cloud Computing infrastructure, hosting the virtualized ACC centre, is illustrated; Section IV describes the application of the SecRAM methodology on the selected use case scenario; Section V details the vulnerability assessment and the threat scenario; Section VI presents the strategy we intend to realize for the last step of the SecRAM, namely the risk treatment and we discuss about pros and cons; Section VII offers conclusion remarks.

II. SECRAM METHODOLOGY OVERVIEW

SecRAM represents the foundation for the application of cost-effective, proportionate and reliable security measures within each part of the ATM system. The

978-0-7695-5008-4/13 $26.00 © 2013 IEEE
DOI 10.1109/ARES.2013.108

SecRAM aims at performing risk identification, evaluation and treatment as shown in Figure 1.

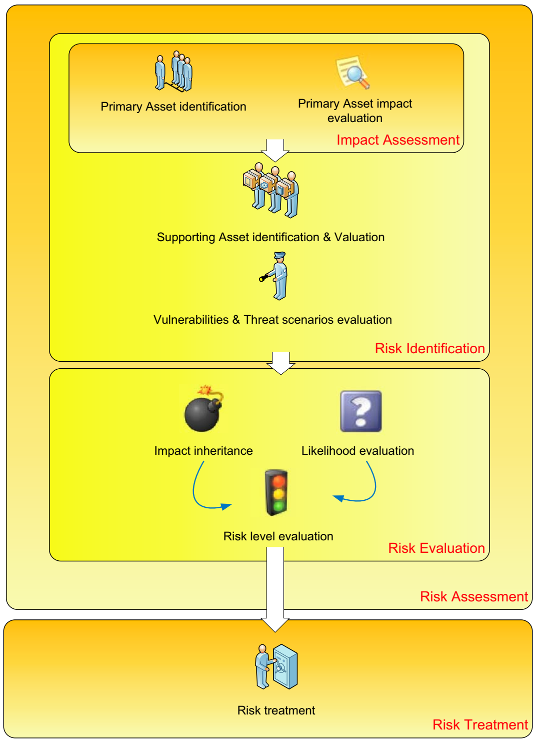


Figure 1 - SecRAM methodology

- The risk identification is the process of finding, listing and characterizing elements of risk. It consists in identifying and evaluating the assets to be protected (namely Primary and Supporting Assets), and in building the threat scenario defined as a combination of a threat over a supporting asset within the considered environment.

- The risk evaluation is the process of assigning values to the likelihood and impacts of a risk.

- The risk treatment is the process of selecting and implementing measures to modify risk.

There are two types of assets: primary assets and supporting assets. Primary assets are the intangible functions, processes, activities, information and services which need to be protected; supporting assets are entities which contain or encapsulate the primary assets. Supporting assets have vulnerabilities that are exploitable by threats aiming at impairing primary assets. After having identified them, all primary assets will be linked with at least one supporting asset, and all supporting assets will be linked with at least one primary asset. A practical example of how to distinguish the assets is: if a primary asset consists in sensitive information then the supporting asset could be the hard disk on which the information resides.

For each primary asset evaluated, it is needed to identify the level of Confidentiality (C), Integrity (I) and Availability (A) required. This evaluation is a number ranging from 1 to 5 to be associated to each of the CIA criteria related to each primary asset. To obtain this evaluation, the impact will be evaluated due to the loss of Confidentiality (C), Integrity (I) and Availability (A) for each of its primary assets on each of Impact Areas (IA) described in Table 1.

As it was specified before, supporting assets are those which have vulnerabilities that are exploitable by threats aiming to impair the primary assets within scope. The risk evaluation of the SESAR methodology is based on the impact and the likelihood of a threat scenario. The threat scenario is built by identifying:

- ▪ for each supporting asset the relevant threats;
- ▪ for each threat the targeted criteria (confidentiality, integrity and availability).

A threat scenario has a specific likelihood of occurrence and will have a specific impact (depending on the target criteria). The risk treatment consists in one of these decisions for the threat scenario:

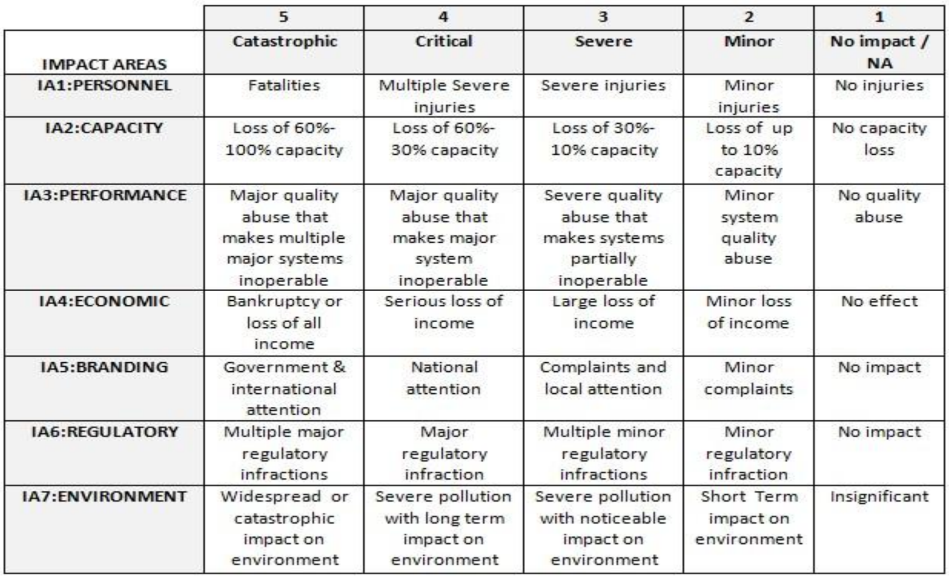
- ✓ accept (or tolerate) the risk, which means that no further action is needed. The risk level is considered low enough to be accepted.

- ✓ Reduce (or treat) the risk to a new level through the selection of controls so that the residual risk can be reassessed as being acceptable.

- ✓ Avoid (or terminate) the risk, which means that if the risk is considered too high and the counter-measures to reduce it too onerous, then the project can decide to withdraw the activity or change its nature so that the risk is not present anymore.

- ✓ Transfer the risk, which means that the project decides that the risk should be transferred to another party that can effectively manage it.

Once the risk treatment plan has been defined, residual risks need to be determined. This involves an update or re-iteration of the risk assessment, taking into account the expected effects of the proposed risk treatment. After this important activity (risk treatment), it is needed to consider the acceptance of the risk. In fact, the risk treatment plan is fundamental to assess the risk in order to meet the acceptance criteria.



	5	4	3	2	1
IMPACT AREAS	Catastrophic	Critical	Severe	Minor	No impact / NA
IA1:PERSONNEL	Fatalities	Multiple Severe injuries	Severe injuries	Minor injuries	No injuries
IA2:CAPACITY	Loss of 60%-100% capacity	Loss of 60%-30% capacity	Loss of 30%-10% capacity	Loss of up to 10% capacity	No capacity loss
IA3:PERFORMANCE	Major quality abuse that makes multiple major systems inoperable	Major quality abuse that makes major system inoperable	Severe quality abuse that makes systems partially inoperable	Minor system quality abuse	No quality abuse
IA4:ECONOMIC	Bankruptcy or loss of all income	Serious loss of income	Large loss of income	Minor loss of income	No effect
IA5:BRANDING	Government & international attention	National attention	Complaints and local attention	Minor complaints	No impact
IA6:REGULATORY	Multiple major regulatory infractions	Major regulatory infraction	Multiple minor regulatory infractions	Minor regulatory infraction	No impact
IA7:ENVIRONMENT	Widespread or catastrophic impact on environment	Severe pollution with long term impact on environment	Severe pollution with noticeable impact on environment	Short Term impact on environment	Insignificant

Table 1 Impact Areas

III. CLOUD-BASED ATM TESTBED IMPLEMENTATION

Cloud Computing is a technology that provides the chance to deliver ICT services by hiding the underlying complex infrastructure and the dynamic allocation of the resources composing it. Cloud infrastructures can be classified concerning the service and the deployment model they implement. From the service model perspective, they are classified as Software, Platform, or Infrastructure as a Service (SaaS, PaaS, IaaS), depending on the abstraction level through which resources are provided to the final user. IaaS, also referred to as Resource Clouds, represents the lowest level of abstraction: users have access rights to virtualized resources such as computational resources, networking, and storage. Instead, from the deployment model point of view, Cloud infrastructures can be classified as Public, Private, or Hybrid, depending on the level of exposure to external WAN connections (i.e. Internet). Private Cloud stands for a Cloud infrastructure hosted within the data center of a single organization, and used by local users only.

In this section we describe the implemented ATM test-bed, which relies on a Private Cloud Infrastructure properly customized to host a complex System of Systems. Such infrastructure implements the IaaS service model, and relies on the OpenNebula [8-9] and Open vSwitch [10] open source technologies. The realized test-bed consists in 30 ATM nodes, each of them is running on a well-defined Virtual Machine (VM). All VMs are interconnected by the means of 12 Virtual Local Area Networks (VLANs). The virtual switch allows the implementation of the aforementioned VLANs, which enable the virtualized ATM nodes to exchange ATM data (i.e. RADAR, flight data, and so on).

The whole ATM test-bed runs on a cluster of six Dell PowerEdge M610 Blade Servers, each of them are equipped with Quad-core Intel® Xeon® E5420 2.50GHz dual-processors, 16GB of RAM memory, and four Gigabit Ethernet adapters. On the top of the physical infrastructure the OpenNebula 3.8.3 platform is installed and properly configured. The Kernel-based Virtual Machine (KVM) [11] is adopted as the full virtualization hypervisor. Thanks to KVM, the platform is able to run multiple Virtual Machines, each of which has private virtualized hardware, namely: network cards, disks, graphics adapters, and so on.

As shown in Figure 2, our Cloud Infrastructure is organized on two different datacenters each equipped with a Storage Area Network (SAN), and connected through an emulated Private Enterprise Backbone. The backbone link emulation is pointed out by adopting the Dummynet Open Source software tool [12].

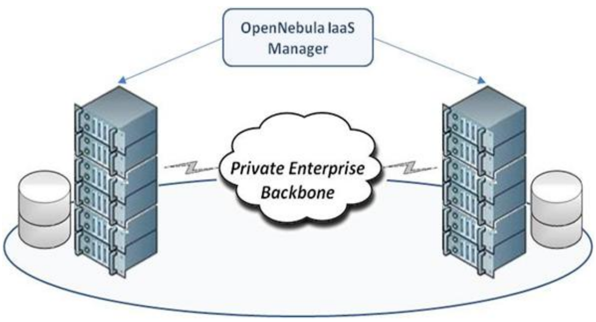
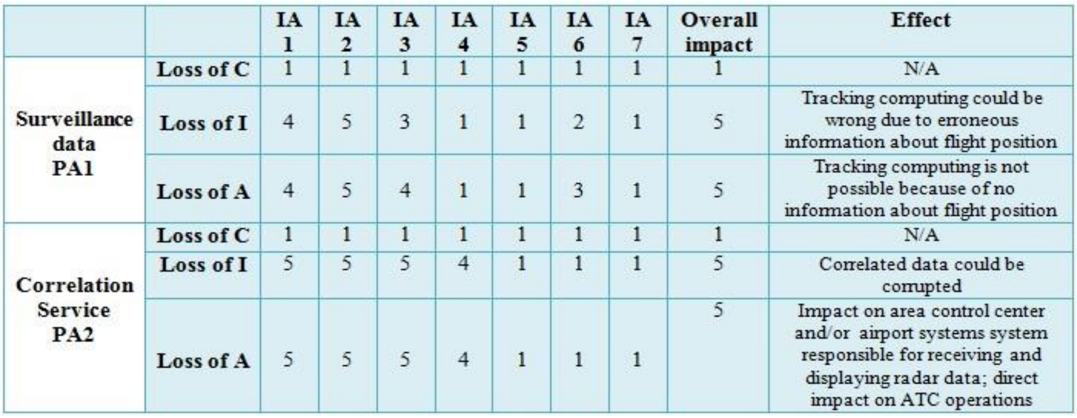


Figure 2 The overall Cloud infrastructure



		IA 1	IA 2	IA 3	IA 4	IA 5	IA 6	IA 7	Overall impact	Effect
Surveillance data PA1	**Loss of C**	1	1	1	1	1	1	1	1	N/A
	Loss of I	4	5	3	1	1	2	1	5	Tracking computing could be wrong due to erroneous information about flight position
	Loss of A	4	5	4	1	1	3	1	5	Tracking computing is not possible because of no information about flight position
Correlation Service PA2	**Loss of C**	1	1	1	1	1	1	1	1	N/A
	Loss of I	5	5	5	4	1	1	1	5	Correlated data could be corrupted
	Loss of A	5	5	5	4	1	1	1	5	Impact on area control center and/or airport systems system responsible for receiving and displaying radar data; direct impact on ATC operations

Table 2 Primary asset evaluation

IV. APPLICATION OF THE SECRAM METHODOLOGY

We present an example of application of the previously described SecRAM methodology exploited on the component of the ACC testbed responsible of receiving radar tracks from multiple sources and mixing them thanks to a correlation service. The information that comes from this correlation process is given as output to the presentation layer deployed on another Computer Software Component Interface.

Risk Identification

The first step of the risk identification is to list and evaluate the primary and supporting assets. We considered the component explained before and we listed its primary and supporting assets. Among them, we decided to carry on the application of the metodology with the most critical SAs and PAs. Our choice fell on two primary assets and one supporting asset, which are respectively:

- PA1: surveillance data;
- PA2: correlation service;
- SA: correlation manager (CSCI).

We chose as secondary asset the CSCI itself because of its fundamental functionality in the system and as primary assets the surveillance data and the correlation service, since their security pitfalls could bring to:

- excessive workload for the Air Traffic Control Officer;
- a wrong correlation process and subsequently to an erroneous procedure of the ATC controller, with catastrophic impacts.

Then for every primary asset we assessed the level of impact in terms of loss of Confidentiality (C), Integrity (I) and Availability (A) on each of the security impact areas that are shown in Table 1. The results of the impact assessment are shown in Table 2. For every impact area a value ranging from 1 (no impact) to 5 (catastrophic impact) is chosen to specify the severity of the impact: the overall impact is defined as the maximum impact level between all the impact areas. Next to overall impact value, an effect for each of the security principles is also given.

The next step is the identification of vulnerabilities, namely the security breaches that can be exploited with interest related to different impact areas. One or more vulnerabilities can be exploited by a threat scenario which can be defined as a combination of an attacker and his resources, motivation and objectives. As explained before, only supporting assets have vulnerabilities exploitable by threats with the aim of impairing the primary assets. In this phase for each supporting asset previously identified, we need to recognize relevant threats, and then for each threat the targeted criteria (C, I, A). We obtained the threat scenarios (for the unique supporting asset that we identified) from a preliminary vulnerability assessment, whose results are collected in the next section. The considered threats are:

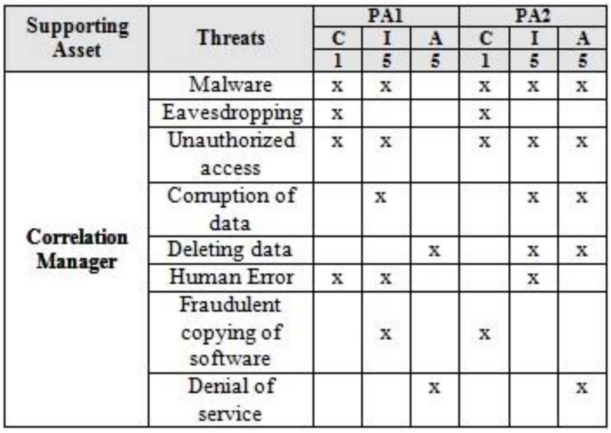
- ✓ Malware;
- ✓ Eavesdropping;
- ✓ Unauthorized access;
- ✓ Corruption of data;
- ✓ Deleting data;
- ✓ Human error;
- ✓ Denial of service;
- ✓ Fraudulent copying of software.

The overall link between primary and supporting assets, the relevant threats for the supporting asset and their impact on each criteria is shown in Table 3. The threat scenarios evaluation represents the last step for the risk identification: we identify the impact on the CIA criteria that is caused by the threat exploitation on the supporting asset.

Risk Assessment

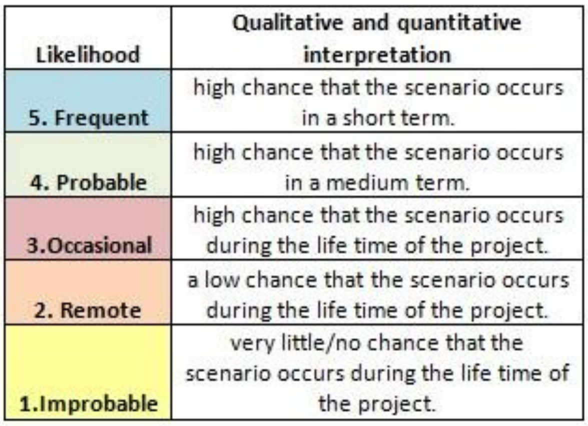
The risk evaluation consists in obtaining the impact and the likelihood of occurrence for each of the threat scenarios taken into account. We get the impact of the threat scenario from Table 3, by selecting the maximum impact of the targeted criteria. This value is the so-called "inherited impact". Then we computed a likelihood which is the evaluation of the chance of a threat scenario occurring, by considering the existing security countermeasures and security controls. It can be a value ranging from 1 to 5: its significance is explained in Table 4.

In order to accomplish this evaluation, we took into account the time and skills required to prepare the attack, the knowledge of the attack target, the skills needed by the attacker to leverage the threat and finally the time window in which the target needs to be available as explained in Table 5. The risk evaluation process is shown in Table 6.



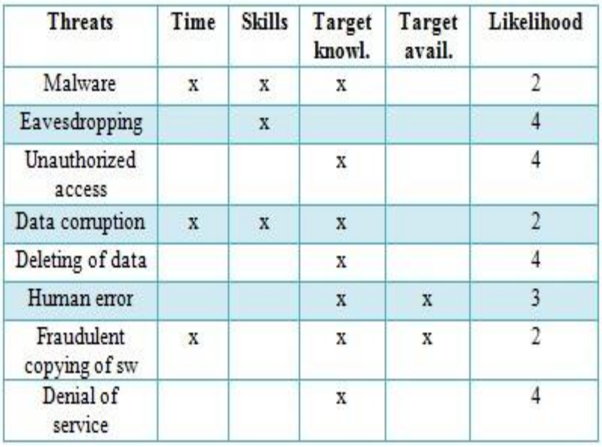
Supporting Asset	Threats	PA1			PA2		
		C	I	A	C	I	A
		1	5	5	1	5	5
Correlation Manager	Malware	x	x		x	x	x
	Eavesdropping	x			x		
	Unauthorized access	x	x		x	x	x
	Corruption of data		x			x	x
	Deleting data			x		x	x
	Human Error	x	x			x	
	Fraudulent copying of software		x		x		
	Denial of service			x			x

Table 3 Threat scenarios evaluation



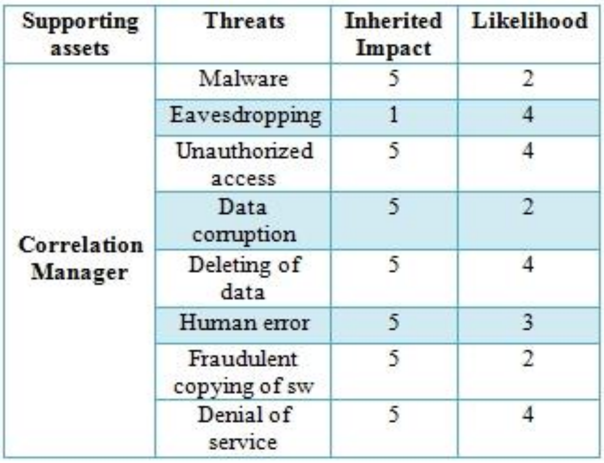
Likelihood	Qualitative and quantitative interpretation
5. Frequent	high chance that the scenario occurs in a short term.
4. Probable	high chance that the scenario occurs in a medium term.
3.Occasional	high chance that the scenario occurs during the life time of the project.
2. Remote	a low chance that the scenario occurs during the life time of the project.
1.Improbable	very little/no chance that the scenario occurs during the life time of the project.

Table 4 Likelihood significance



Threats	Time	Skills	Target knowl.	Target avail.	Likelihood
Malware	x	x	x		2
Eavesdropping		x			4
Unauthorized access			x		4
Data corruption	x	x	x		2
Deleting of data			x		4
Human error			x	x	3
Fraudulent copying of sw	x		x	x	2
Denial of service			x		4

Table 5 Likelihood values



Supporting assets	Threats	Inherited Impact	Likelihood
Correlation Manager	Malware	5	2
	Eavesdropping	1	4
	Unauthorized access	5	4
	Data corruption	5	2
	Deleting of data	5	4
	Human error	5	3
	Fraudulent copying of sw	5	2
	Denial of service	5	4

Table 6 Supporting Asset Evaluation

V. VULNERABILITY ANALISYS AND THREAT SCENARIO

Since the SecRAM methodology explained and applied in the previous sections doesn't deeply analyze vulnerabilities, we used the ACC test-bed to identify some vulnerabilities that can affect the entire system and in particular our supporting asset in order to build a real threat scenario. The first step was to perform a vulnerability analysis of the system itself with the objective to find the running services and eventual security breaches. To this aim, we used a penetration testing tool, namely Backtrack [13], which is equipped with a set of tools to perform well-known vulnerabilities scanning and to launch the selected exploits by taking advantage of the found security pitfalls. After launching the vulnerability scanning process, we collected all the found vulnerabilities, we drew the inherent possible threats and finally we computed the percentage of their occurrences in the overall system. Figure 3 shows the results.

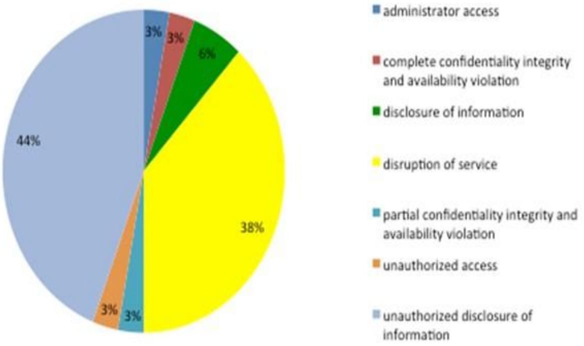


Figure 3 Threats distribution

One or more of these vulnerabilities can be exploited to create a threat scenario. For example if a remote login service is in execution on the machine that represents the CSCI (the supporting asset), an attacker could be able to intercept the credentials used to access the node itself and this situation could potentially bring to threats such as unauthorized access (impact on I and C), deleting data (impact on A) or fraudulent copying of sw (impact on I and C). The supporting asset we considered shows two main vulnerabilities that can impact on it in terms of:

- ✓ unsecured access control;
- ✓ flow in implementation (management of a big amount of data).

We decided to exploit the second kind of vulnerability that allows us to define a real threat scenario. So we used the found open ports and we flooded them with a great amount of data in order to have repercussion mainly on the supporting asset's availability.

VI. RISK TREATMENT AND DISCUSSION

For the last step of the methodology, namely the risk treatment, we implemented in our cloud test-bed an architecture [14] which is able to detect malicious attacks (e.g. an abnormal amount of data arriving to the attack target) and we also provided the cloud platform with the capability of reconfiguring itself to react against security alerts. The risk treatment we used, with regard to the threat model explained before, is the transfer one. The architecture we designed allows the IaaS infrastructure to reallocate a subset of ATM functionalities, e.g. the node under attack, by migrating virtual resources across geographically connected data centers. The connection between the two data centres is secured through the use of a MPLS-based splitting packets [15] mechanism. When a malicious activity is detected by the network sniffer, an alarm is sent to a correlator as illustrated in Figure 4. This component is in charge of detecting the severity level of the alarm and deciding which mitigation strategy is needed. We implemented a real threat scenario, in which a DoS attack was performed against the CSCI described in the previous sections. The risk treatment process is handled by the correlator, which decides that the virtual appliance under attack must be migrated in a more "secure" data centre, in order to mitigate this attack. The cloud infrastructure is also based on Software Defined Networking [16] mechanisms in order to easily spread security policies in the network (e.g. blocking the source of the attack) and to assure the VM's mobility after the migration process.

Our virtualized test-bed allowed to realize a vulnerability assessment that was useful to:

- find and list the vulnerabilities that affect our system;
- apply the SecRAM methodology to identify and then evaluate the supporting asset;
- to build a real threat scenario with the identified vulnerabilities;
- design a cloud based architecture to automatically realize risk treatment and mitigation when one of the discussed threat scenarios is identified.

The vulnerability analysis we conducted is not to be considered as an exhaustive solution, since it mainly focus on application-based vulnerabilities but it can be used as a good start point for the methodology. The SecRAM methodology applied in the context of our virtualized test-bed allowed us to evaluate the risk affecting our systems and also to manage it, without having effects on the real operational one.

VII. CONCLUSION AND FUTURE WORK

In this work we described and applied a general methodology for ATM domain risk assessment and treatment in a cloud-based test-bed which represents a real ACC, Air Control Centre. It basically consists in risk identification for finding and listing the system's primary and supporting assets. The primary assets are then evaluated in terms of loss of confidentiality, availability and integrity and in relation to determined impact areas. Subsequently there is a phase in which the primary assets are evaluated and threat scenarios are built. The second step, namely the risk evaluation, allows to compute the likelihood and the inherited impact on each considered threat scenario. The risk treatment is the process of reducing, transferring or accepting the level of the risk itself.

After the application of the methodology, we used our test-bed to conduct a preliminary vulnerability assessment in order to build a real threat scenario that was then implemented. Finally we described the mitigation

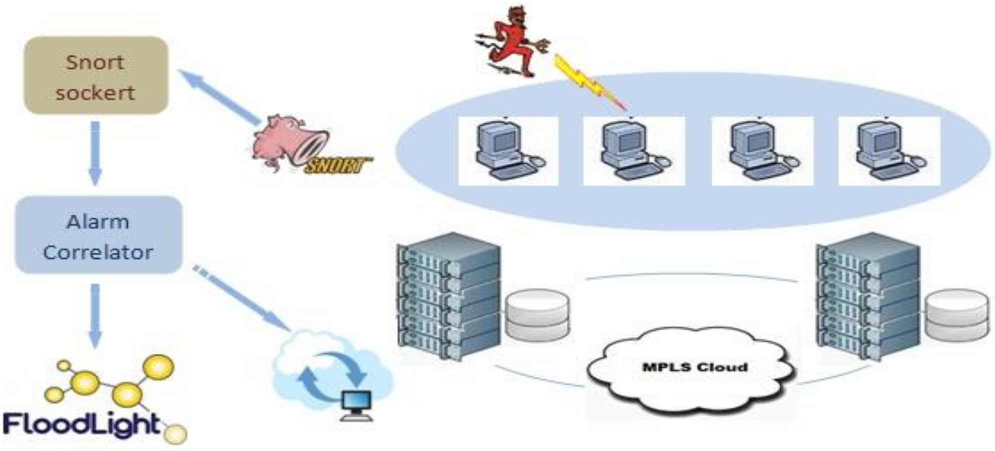


Figure 4 Components'interaction

procedure we use to realize the transfer risk treatment. Our main contribution is the adoption of Cloud Computing to realize a vulnerability assessment and a risk evaluation by applying the SecRAM methodology. As future work, we aim at implementing other threat scenarios, applying the methodology to different target scopes as well as investigating different treatment procedures.

REFERENCES

[1] Commission implementing Regulation (EU) No 1035/2011, Official Journal of the European Union, 17 October 2011.

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

[3] Deliverable 16.02.03 – SESAR ATM Security Risk Assessment Methodology ; SESAR WP16.2 – ATM Security.

[4] Micheal Armbrust et al., A View of Cloud Computing, Communications of the ACM, Volume 53 Issue 4, April 2010. pp 50-58.

[5] EUROCONTROL ATM Security Risk Management Toolkit – Guidance material v1.0

[6] ISO/IEC 27005:2008, Information technology – Security techniques – Information security risk management

[7] Commission of the European Communities, Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM (2006) 786 final, Brussels, 12 December 2006.

[8] Giovanni Toraldo, “OpenNebula 3 Cloud Computing”, PAKT Publishing, May 2012.

[9] OpenNebula official web site: http://www.opennebula.org/

[10] Open vSwitch official web site: http://openvswitch.org/

[11] Kernel Based Virtual Machine, http://www.linux-kvm.org/page/Main_Page

[12] Dummynet web-site, http://info.iet.unipi.it/~luigi/dummynet/

[13] Backtrack official web site: www.backtrack-linux.org

[14] G. Carrozza, V. Manetti, A. Marotta, R. Canonico, and S. Avallone, “Exploiting SDN Approach to Tackle Cloud Computing Security Issues in the ATC Scenario”. I Dependable Computing Lecture Notes in Computer Science Volume 7869, 2013, pp 54-60. EWDC 2013, Coimbra 15-16th May 2013.

[15] Avallone Stefano et al., A Splitting Infrastructure For Load Balancing And Security in an MPLS Network. 3rd International Conference on Testbeds and Research Infrastructure for the Development of Networks and Communities, 21-23 May 2007. Pages: 1 – 6

[16] Open Network Foundation, https://www.opennetworking.org/