International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:3, No:6, 2009

Security Risk Analysis Based on the Policy Formalization and the Modeling of Big Systems

Luc CESSIEUX, French NAVY and Adrien DEROCK, DCNS/IMATH

***Abstract*— Security risk models have been successful in estimating the likelihood of attack for simple security threats. However, modeling complex system and their security risk is even a challenge. Many methods have been proposed to face this problem. Often difficult to manipulate, and not enough all-embracing they are not as famous as they should with administrators and deciders. We propose in this paper a new tool to model big systems on purpose. The software, takes into account attack threats and security strength.**

***Keywords*—Security, risk management, threat, modelization.**

I. Notion of security policy

SECURITY policy is a document that states in writing how the compagny plans to protect the compagny's physical and information technology assets. This contains the set of laws, rules and practices to manage, protect and distribute sensitive information. Let see the main concept about modeling security policy.

A. A security policy based on access control

Most often, notably in the military domain, system security is based on the concept of information access.

1) Biba and Bell-LaPadula concept: Biba's model and Bell-LaPadulla's one[8], [1], [2], [5] is an access control model using Mandatory Access Control (MAC) which spreads the discretionary model of matrix access control. The main goal of this model is to express the multi-level security policy for confidentiality and integrity management. This control mechanism of information access cannot be broken. Now, the information is mobile and receives in a given time, diverse means of protection, more or less vulnerable. This information can be ciphered for privacy but its mechanism is potentially vulnerable and cannot be 100% trustable. We lose then the guarantee on the author of the message and the information becomes accessible to whomever. This model also relies on mechanisms which are under control. Unfortunately our systems are more and more complex and depend on third part systems which are potentially dangerous (bugs or backdoors), leading to a bad application of the access policy.

2) Or-Bac Model: The Model Or-Bac[3] allows to adapt rules according to the context and also takes into account the negative access control, allowing banning. This model, more complete, than the precedent one suffers nevertheless with the same weaknesses statements than the model presented in the previous paragraph. And if we take into account the notion of negative access, this one is not however equal to the notion of possible illegal access. We talk about here, the faculty of an aggressor to have access, since nothing was specified and because this one has means (technical, human and organizational) allowing to by-pass the established security policy.

Luc CESSIEUX is working for the french Navy. He is the Security Officer at DIRISI Toulon, France, cessieux@hotmail.fr

Adrien DEROCK is working in the information security department at DCNS, the french naval ship builder, Toulon, France, adrien.derock@dcnsgroup.com / He is also affiliated as researcher at ESIEA/IMATH laboratory, France

B. Behavior conformity observation

Vianney Darmaillacq and Nicolas Stouls[6] propose an interesting solution of approved communication formal modeling from a security policy. The main inconvenience of this methodology is its limitation and still does not take the security in its global nature.

C. A security policy based on safety

If the notion of safety exists since a long time[7], notably within the framework of the nuclear safety, it is necessary to admit that with the computerization of our environment, this one becomes very complex to model. It is also very delicate to apply this kind of model to predict environmental threats as earthquakes, floods or fires which can strike a blow at the system availability.

D. Security policy based on information system analysis

It is interesting to notice in the formalization of security policy that the notion of access right prevails[3] in analyses and proposed solutions, to the detriment of other elements of the security as the management of the quality of code or process of information circulation in its physical environment. We want to surround all the security problems and we want to be able to formalize a global security policy of an information system. It thus adorned us necessities to begin by modeling the information system in its global nature by taking into account either its logical than physical and human environment. Thus it is necessary to model at first the system before defining security policies and making the management of risk.

II. Exhibition of the model

We consider an object O as a material or immaterial entity of the information system which is provided with a set of property. For example: a computer, a person, a premises, a policy, an information system or even more an information. It is also possible to categorize certain objects following two criteria defined below:

Definition 1: The object O can be the composition of one or several objects. It is for example possible to consider an "information system" object as the association of several computers in a premises, accompanied with inverters and with means of air conditioning in the premises.
We designate with Ω all the objects O_n with $n \in \mathbb{N}$ with matching the definition above.

Definition 2: the object O can be also considered as "Essential" if it characterizes the security requirements of the other surrounding objects. For example, the confidentiality requirement of a server determines the requirement of "capacity hosting" of the premises in which the server is set up. In that case object will be qualified as "Essential by the person in charge of the model.

A. Properties of an object

An object O consists of a triplet (I, B, M) of a set of properties. These properties are cut in three big families:

- The properties of identity and operating
- The security properties.
  - With the properties of security requirements
  - The properties of threat

Definition 3: Let be O_i = (I, B, M) with:

- I all the properties of identity and operating
- B all the properties of security requirements
- M all the properties of threats

And I = (I_0,..., I_x) a finished set with $x \in \mathbb{N}$
And B = (B_0,..., B_y) a finished set with $y \in \mathbb{N}$
And M = (M_0,..., M_z) a finished set with $z \in \mathbb{N}$

1) The properties of identity and operating (PIO): Some of these properties are compulsory and necessary for the functioning of the posterior analysis. Other properties are free and in the just appreciation of the writer of the model. Whatever property we consider, it will always consist in couples of element:

- A title;
- A value.

Let us take the example of a software object, it can have for instance as couple:

- Manufacturer;
- Microsoft.

Definition 4: Let the couple I_k equal to (a, b) with a representing the identity and b the value. And I = (I_0,..., I_k,..., I_n) a finished set with n, $k \in \mathbb{N}$

To simplify the notation we note the access in one PIO of an object thanks to the symbol ".".

We thus obtain the following symbolism:

$$O_i.I_k$$

We also note the access to the value of this property in the following way: $O_i.I_k.b$

Example: $O_i.I_k.a$ = "Manufacturer"("Builder") $O_i.I_k.b$ = "Microsoft"

. The compulsory properties

To make easy the later possessing and define the relations between objects, it is necessary to categorize objects in the following way. A object can take one and the only one of these categories.

- The category "physical PHY (material object leading to the physical protection or having a direct action on the environment for a radar or a fire extinguisher);
- The category "geographical" GEO (a site, a premises, a zone);
- The category "software" SOF;
- The category "organizational" ORG (Policy, procedure);
- The category "computer hardware" COH;
- The category "information" INF (a paper or an purely immaterial notion of information);
- The category "function" FCT (bank transfer etc.);
- The category "staff" STF;
- The category "information system" (IS).

According to the level of detail we wish for our analysis, an object IS will be considered as an atomic object or as the grouping of several objects. We thus obtain as formal representation for some object of software type O_i:

$$O_i.I_0.a = "category"$$

and

$$O_i.I_0.b = "SOF"$$

We also suggest creating one subcategory allowing to refine the distribution of objects. Nevertheless, in order to simplify, we limit our description to the generic categories described above.

2) Security properties: . Properties of security requirements

Property 1: Let be the property B, the specification of security requirements in availability, integrity, confidentiality, the handling capacity, hosting information in confidentiality and integrity, as well as the specification of the lifetime for a security requirement in availability, integrity, confidentiality which are named respectively a, i, c, hc, hi, la, li, lc.

These requirements are each one estimated on a scale corresponding to the ISO 27005, here [0-9] with 0 for null requirement, and 9 for the maximal requirement. This estimation is excepted for the availability, where, it is specified a percentage rate PR(%) to refine calculations.

Definition 5: Let be B = (a, i, c, hc, hi, la, li, lc) with:

- "a" Representing the need in availability,
- "i" Representing the need in integrity,
- "c" Representing the need in confidentiality,
- "hc" representing the need of capacity in confidentiality,
- "hi" representing the need of capacity in integrity,
- "la" representing the need of lifetime in availability,
- "li" representing the need of lifetime in integrity,
- "lc" representing the need of lifetime in confidentiality,

we note the access to a requirement of an object with the symbol "." We thus obtain the following symbolism for the requirement in availability: $O_i.B_a$

Property 2: Let be the properties E, the evaluation of the security level in Availability, Integrity, Confidentiality and of the information handling capacity in confidentiality and integrity, as well as the evaluation of the properties of time

specified above. The set is respectively noted EBA, EBI, EBC, EBHC, EBHI, EBLC, EBLI.

This evaluation is calculated in a percentage rate and will correspond to the risk that a dreaded event occurs with regard to the security requirement affiliated to the object. The benefit of this evaluation is its similarity with the scale proposed above. This scale can easily widen to [0-10]. These properties of evaluation are necessary for the documentary production framework, but bring nothing to the formal aspect. Consequently, they will not be formalized.

Object	a,	i	c	hc	hi	la	li	lc
Requirement								
Evaluation								

Fig. 1. Table of evaluation property

. *Properties of threat management (risk management)*

Every object has a list of threats with which we associate various criteria allowing the evaluation of the risk for an object face to a threat.

Let be M_k = (v, a, d, p, t, c, s) with:

- "v" $\in$ [0-10] and representing the appropriate vulnerability of the object) in front of the threat (without any external protection). We can estimate this level as the opposite of the level of the aggressor, required for its achievement.
- "a" $\in$ [0-10] and representing the capacity of action of the object face to the threat.
- "d" $\in$ [0-10] and representing the capacity of the object to detect and to alert face to the threat.
- "p" $\in$ [0-10] and representing probability that the threat manages to. This probability has to take into account the context of opportunity in which is the object.
- "t" $\in$ (accidental and/or random) and representing the type of threat on the object). Is it a deliberate threat or not (accidental, random).
- "c" $\in$ (physical and/or logical) and representing the category of threat. Has the threat a physical or logical influence on the object.
- "s" $\in$ [0-1] and representing the capacity of the threat for the object to be a vector for an attack on another object. This kind of parameter is as a rule only valid for the deliberate threats.
- $M = M_0,..., M_k,..., M_z$ a finished set with $k \in \mathbb{N}$ the name or the number of the considered threat.

We note the access to a threat of an object by means of the symbol "." We thus obtain the following symbolism: $O_i.M_k$ and $O_i.M_kv$. Remark: it is advised to use the list of the EBIOS threats[4] or another one as one listed in the ISO 27005. The

Object	a	d	v	p	t	c	s
Threat 1							
...							
Threat n							

Fig. 2. Table of threat properties

foundations of information system modeling are explained, we can now see the problem of security policy.

B. An example: the laptop

We take here an example of object to give a concrete frame to our comments. A laptop will be defined as an elementary object (definition 1). It will be stored in the category COH and under "laptop" subcategory. Its others PIO will be:

- Function, what is it use for ?
- MAC adress.
- Organism in charge of the material.
- Serial number and reference number.
- Risk 1, theft of the material during travel.
- Risk 2, malware infection leading to information compromising.
- Security measure 1: complex password for login.
- Security measure 2: hard disk ciphered.
- Security measure 3: presence of at least two different antivirus.
- Security measure 4: presence of a firewall.
- Security measure 5: use of an account limited for the common usage.

The security requirements of this object are shown in figure 3.

Object	A	I	C	Hc	Hi	La	Ld	Lc
Requirement	90 % / year	2/9	2/9	4/9	5/9	1 year	1 year	6 months
Evaluation	50 %	10 %	10 %	40 %	10 %	90 %	90 %	90 %

Fig. 3. Table of security requirement for the laptop (example)

The threat associated to the laptop are shown in figure 4.

	a	d	v	p	t	c	s
Trapping of the material	4	4	4	1	Int	P/L	1
Trapping of the software	4	3	4	1	Int	P/L	1
Abuse of process	5	4	5	4	Int	P/L	1
Impersonation	5	5	4	2	Int	P/L	1
...							
Theft of materials	1	0	8	5	Int	P/L	1

Fig. 4. Table of threats

III. Inter object Connection

Now that we have defined the notion of object and its composition, it is important to be able to connect objects between them. Let be R the relation oriented or not between two objects O_1 and O_2. Let be $O_1\ R \rightarrow O_2$, the oriented relation from O_1 to O_2. The link realizing this relation between both objects is L_k. A connection owns in the same way as an object, properties of identity and operating (PIO). Quite as for an object, this one owns the compulsory property of category defined in the same way. It is then necessary to add a matrix, see figure 5 of association allowing specifying the category of the link between two objects of different categories.

O1 / O2	PHY	GEO	SOF	ORG	YES	COH	INF	STF
PHY	PHY	PHY		ORG	PHY	COH	INF	STF
GEO	PHY	GEO		ORG	GEO	GEO	INF	STF
SOF			SOF	ORG	SOF	SOF	INF	STF
ORG	ORG	ORG	ORG	ORG	ORG	ORG	ORG	STF
YES	PHY	GEO	SOF	ORG	COH	COH	INF	STF
COH	PHY	GEO	SOF	ORG	COH	COH	INF	STF
INF	INF	INF	INF	ORG	INF	INF	INF	INF
STF	STF	STF	STF	STF	STF	STF	INF	STF

Fig. 5. Table of category association matrix

IV. Example of application of the model

A. Availability

We propose in this part to make a focus on the rate calculation and the check of availability between two objects from the category "computer hardware" connected by a network link.

Formulae to calculate the rate of availability between 2 points are the following ones:

Let be $O_i.B_a$ and $O_j.B_a$ the rates of availability of objects Oi and Oj with i and $j \in \mathbb{N}$.

Objects in parallel:

$$PR = 1 - (1Oi - 1.B_a)x(1Oj.B_a)$$

Objets in series:

$$PR = (O_i - 1.B_a)x(Oj.B_a)$$

To be able to use these formulae on a complex model, it is necessary to consider all objects of the model in a combination of objects in parallel or in series. We put place here an algorithm allowing us to calculate the PR of availability on particularly big and complex networks thanks to a succession of combinationof object in series or in parallel but also thanks to a mechanism allowing us to removethe connections not influencing the PR of availability between two points.

B. Information disclosure calculation

It is possible to calculate the information disclosure between two objects with all the parameters introduced above.

Our process is divided in two. We begin to extract from the diagram all attack flows possible considering type of attack (logical, physical, deliberate, accidental). One this task accomplished we extract all the possible attack flow considering the level of the aggressor, the strenght of the object face to the threat used.

The level of strenght S corresponds to the inverse level of maximal vulnerability of the object.

$$S(O_i) = 10 - Max(O_i.M_v v, , O_i.M_z v)$$

We define also the function $P(R(O_i))$ wich return for the level of strenght, the level of occurrence probability.

In the example below, see figure 6, we choose a level of the aggressor of 7. The attack flow are the next ones :

We can notice that some object can block this attack (e13). We can calculate the probability of this attack. We can use numbers of techniques to calculate this probability. We choose here to use a markov chain associated with a stationnary law. This solution enable us to calculate the probability of

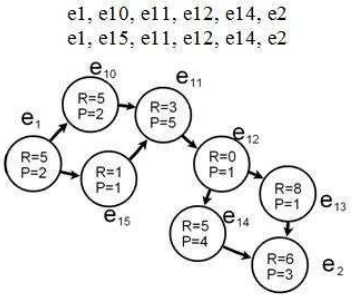

Fig. 6. Example of attack propagation calculation

an event bearing in mind the precedent event. We so obtain the following formula for a path between two objects O_i et O_j:

$$E = (P(R(O_i)) + ... + P(R(O_j)))/n$$

with n the number of objects between O_i et O_j. The risk probability is assimilated to the higher probability for an attack flow associated to this risk.

V. Example of use of the tool

The case proposed for our example carries on a naval ship in its global nature. To simplify our presentation we shall stay in a macroscopic scale of the diagram.

A. The environment

We begin here with the simplest part by defining the environment of the information system. We consider here the ship as a site. We connect then with the site "Ship" the various premises considered in our study (Central Operation, Telecommunication Center).

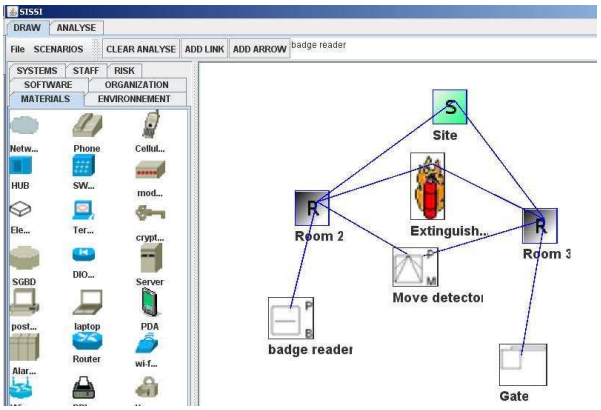

Fig. 7. Creating system environment

For every placed object, it is important to complete immediately the properties of the object as next.

Some properties are already proposed to the user, but he can add it at his convenience by clicking the button add a property.

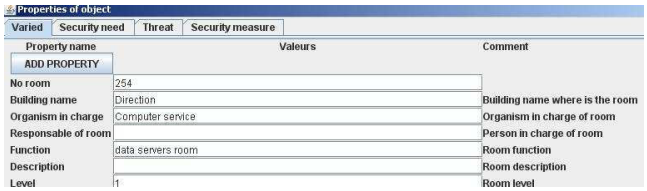

Fig. 8. Creating object properties

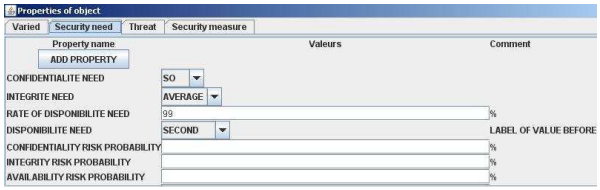

Fig. 9. Adding a new property

It is important to fill in a maximum of information about objects because the system is not linear. The modification of objects afterward can become boring and can generate a source of not unimportant error.

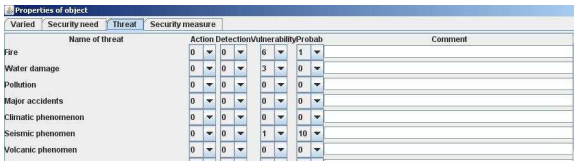

Fig. 10. Object property modification

The organization of the properties of the object allows in principle to ask the good questions as for requirements and security objectives of the object.

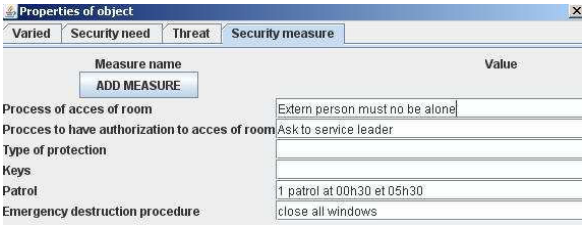

Fig. 11. Object security requirement

This step of filling in information is certainly boring but allows afterward to win a precious time on the design of the system on the diagram.

B. The staff

We place then on the diagram the various actors of the information system: users, administratorsvisitors etc. We connect them then in premises in which they have access as well as to the systems and the computer hardware in which they also have access. In the case of connections with a workpiece it will stipulate that the person has a physical access to the workpiece. The conditions have to be specified in the properties of the object. In the case of a connection with a computer hardware, it will imply the logical access.

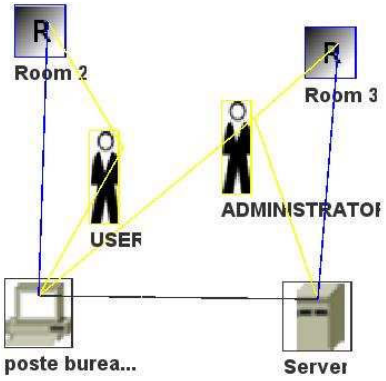

Fig. 12. Staff object creation

C. The materials and the software

We can now take a look in the heart of the system with the whole computer hardware set, the software which are installed on the materials) and the connections between them.

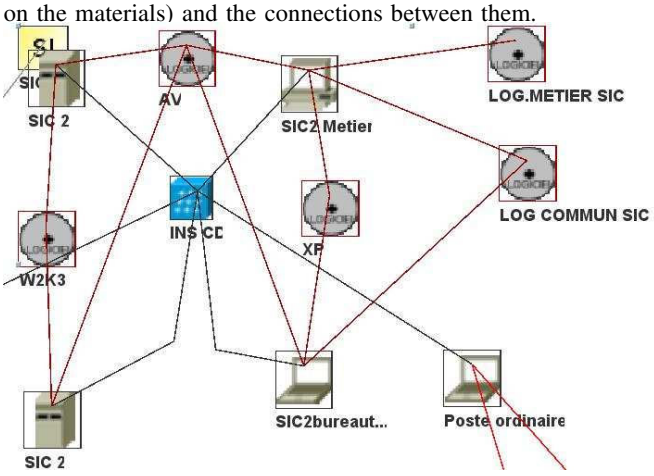

Fig. 13. Creating computer hardware and software object

It is advised to group together objects and software in subsystems as it is the case here. We grouped together in that case in the sub-system SIC21 all the servers and computing posts. We can so arrange more or less macroscopic sights on the systems and relieve the reading of the diagram according to the elements we wish to analyze. In this stage more than in the others, it is essential to complete as one goes along the properties of objects notably the part threatens.

D. Functions and information

We realized the material heart of the diagram, but all this does not allow expressing the stakes, the operating and the

major risks of the system. It is fundamental now to complete the diagram with the functions and the strategic information of the system, with the functions and the information allowing specifying the diagram execution.

We can also model as below a policy of back-up for example. The specifications of the policy of back-up are in the current objects.

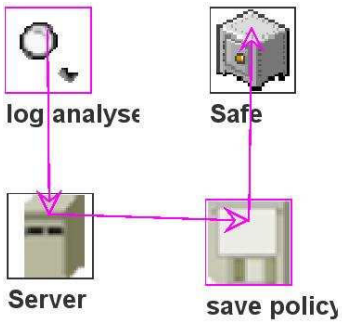

Fig. 14. Creating security policy : back up

But we can already see for example on the diagram that policy of back-up leaves the server to be stored in a safe. The server and the safe are possibly connected with two different local objects.

VI. Conclusion

We have proposed in our paper a model of an information system by taking into account the security risk pending on. The model has been implemented in a tool which is designed to help the administrators or even the deciders to make a decision in the measure to bring out to their system. The tool represent in a new way the system and the threat in a global view. Future works will complete the model with more calculations than those presented in this paper to complete the appreciation of risk in complex system.

References

[1] David Elliott Bell. Looking back at the bell-la padula model. *Computer Security Applications Conference, Annual*, 0:337–351, 2005.
[2] K. J. Biba. Integrity considerations for secure computer systems. Technical report, MITRE Corp., 04 1977.
[3] Fredéric Cuppens and Nora Cuppens-Boulahia. *Les modéles de sécurité*. Traité IC2, série réseaux et télécoms, Jun 2006.
[4] DCSSI. La méthode ebios,www.ssi.gouv.fr/fr/confiance/methodes.html.
[5] Len Lapadula, The Original, D. Elliott Bell, and Leonard J. Lapadula. titled secure computer systems: Mathematical foundations.
[6] Nicolas Stouls and Vianney Darmaillacq. Développement formel d'un moniteur détectant les violations de politiques de sécurité de réseaux. In S. Vignes and V. Viguié Donzeau-Gouge, editors, *Approches Formelles dans l'Assistance au Développement de Logiciels (AFADL'06)*, pages 179–193, March 2006.
[7] Xinwen Zhang, Ravi Sandhu, and Francesco Parisi-Presicce. Safety analysis of usage control authorization models. In *ASIACCS '06: Proceedings of the 2006 ACM Symposium on Information, computer and communications security*, pages 243–254, New York, NY, USA, 2006. ACM.
[8] Gansen Zhao and David W Chadwick. On the Modeling of Bell-LaPadula Security Policies using RBAC. In *Proceedings of 17th IEEE International workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE 2005), Rome*, June 2008.