Informatics Security Metrics Comparative Analysis

Ion IVAN, Bucharest, Romania, ionivan@ase.ro
Luckacs BREDA, Brasov, l.breda@yahoo.com

The informatics security concept is defined. For informatics applications which have a classical structure, the development, current use, maintenance, and reengineering particularities are described for distributed systems and m-applications.
Metrics are built for the security of open informatics applications and a method for their validation is proposed. To see when a metric is adequate a comparative analysis is made for each indicator using a representative diversity of data sets for the test.
***Keywords**: security, metrics informatics, evaluation.*

Informatics security

Informatics security is an incredibly vast research field. The informatics security problems are found in:

- the specific theories for encryption processes aimed at finding algorithms that have superior performance in raising the security level in the practical exploit of citizen orientated informatics systems;
- analysis and software design techniques, considering to include in he development cycle informatics security related elements;
- building the legislation regarding e-commerce, financial transactions, archiving, document circuit, electronic signature, transparency and the access guarantee to information in digital format;
- software quality management by including quality characteristics in strict connection to informatics security or which influence directly informatics security;
- the software products development which assist the testing of the software application, or which creates components that led to obtaining secure informatics systems.

Informatics security contains:

- software components that make specific processing, for a time interval they have to maintain these functions; if a program product is characterized by a contents in a moment T_0 at any next moment the product that is launching in execution should have the exact same contents; the security processes have the purpose of creating conditions that ensure the invariable character of the contents of a product program;
- the databases which describe after an established structure the traits of a collectivity and the relations between these elements; databases are characterized by their length, complexity and contents, it's very important that the levels of database characterization remain in the limits set by the developer, depending on the contributions of the users; to develop an application with the security characteristics of databases means creating the software components that offer resources to manage databases only to those that are privileged to have access, strictly between the limits given to each of them;
- communication processes, because the altering of the informational contents has to be maintained in the limit of identification and reversibility.

Informatics security is the domain which grows even more considering the development of distributed applications with a global character an the growth of the diversity of the means to complete the access to the resources of these applications, from the personal computer, to the public computer, from the mobile phone, from an iPod, from any other terminal. The growth of streams and specially the generalization of virtual financial transfers raises the stakes of ongoing processes that alter the contents of messages, thing that requires taking security measures, if the measures taken will not eliminate the risks of changes being made in the contents of the message or contents processing, at

least creates the premises of managing these risks, maintaining the efficiency of the application, for the owner and mostly for the users who are the every day beneficiaries of the application.

2. Traits of informatics applications

From the informatics security point of view there can de identified some traits for the applications designed to solve complex problems, especially network problems. The users of informatics applications are different, the majority will:

- use the resources of the informatics application, for the purpose it was developed, meaning: to solve problems defined as objective in the program specifications; considering an e-commerce application, the buyers identify products, select them, make payments and continue the cycle for which the application was developed; the access is unrestricted and restrictions are present only when the payment is made;
- update databases, such that they will reflect real aspects concerning the collectivity for which the application was created; for the e-commerce application, the administrator has the obligation to ensure the correctness of resource access, and the operators that have access to the data base update prices, stocks and stock structures in the supply process, selling process; the access is conditioned and has a well defined hierarchy;
- activate functions with an undesired role, which can access components of the application from outside it and can modify parts of it, or can modify the database these modifications are not reversible, and this generates reloading and updating procedures, if the modifications are reversible, the rebuilding process starts at application level; if the modifications are temporary and reversible, the visibility of the modifications has to be outlined through specific methods; if the modifications are temporary they will determine actions which ensure reversibility of the contents, the actions will be initiated by who activated the functions in the first place; these modifications are due to: the incomplete development of validation procedures, or access information obtainment, or because of unauthorized access; at design time there barriers have to be developed to permit the identification of this kind of typology of transformation in the application.

The traits are determined by the number of users, by the diversity of problems that need a solution, and especially financial resources involved in e-commerce transactions.

Applications are grouped regarding risk levels, the levels depend on the relaxation of policies defined by the owner of the application.

3. Informatics security metrics

The metrics of informatics security applications take in consideration the following aspects:

- the application's state of completion; component behavior estimation indicators are built when the necessary resources for the development of the entire application are planned; indicators are built to show the level of some security characteristics along the stages of the application development cycle; indicators are defined, that measure the effective behavior of the application when it is in use, the strict behavior considering insurance factors of informatics security;
- putting together an indicator system that contains the most diverse situation typologies in which the application will not be efficient, to identify the modules of the security component which need further insistent and augmented improvement;
- the takeover of elements from the security standards such that all who respect these standards, by measuring the indicators to obtain a clear image of the quality characteristics imposed by the standards;
- ensuring the compatibility of the newly created program components with the already existing ones, by using the same indicators, obtained using the same formulas; if the model circulation is restricted, the next step will be establishing

a correlation between the models, usually constants are obtained that used with values resulted from a known model, allow getting the level of an obtained quality characteristic if an unknown structure model will be used;

The indicator list for security quality takes refers to:

- the product program;
- the security process;
- the behavior of the software product in current exploration;
- the user behavior.

In all the cases a series of aspects comes up regarding the production rates calculation of a phenomenon and the weight of particular actions have in using the software application. In developing the indicator set the effort and duration necessary for collecting data have to be estimated such that indicators with realistic and credible levels are obtained.

Afterwards a stability analysis is required, and if a global model analysis of the security of software applications is needed the entire process becomes more complex.

4. Security metrics validation

Modeling the software application in risk conditions represents an important problem and more attention is given to the building of indicators with a growing degree of complexity, to contain more factors, to reflect as best as possible the application-user relation in their vast diversity of objectives. If refining models presumes the complexity reduction of the indicator included in an informatics security metric, the validation comes to establishing the proportion in which the indicators contained in the metric are representative or not, meaning the differences between the estimated levels and the effective ones is or isn't significant.

To perform a validation for an informatics security metric the next procedure is followed:

- establish the types of risks that the security components have to face from a multitude of software applications;
- define type of test data sets that will be used to test the software application to obtain the estimated security level for current use;
- make measurements of the behavior of software applications and calculate the indicators associated to each risk typology, also make measurements for the indicators regarding the behavior and the ones regarding the satisfaction degree of the users for whom the application has been developed; an estimation is made based on the efforts needed to complete the risky objectives by the complementary category of users in report to the objective; a complete matrix in obtained with values recorded for all the applications, for all data sets and all indicators
- record the real behavior of software applications, resulting in a matrix with the same structure as the one obtained in the previous step, following the same method, with the same indicators, totally comparable;
- determine the degree in which the differences between the estimated levels and the effective ones of the indicators are acceptable or not; the percent of the situations in which accepted indicators validate or invalidates the indicators, it validates or invalidates the metric as a whole, seen as a system of indicators.

The clarification of the risk situations for every application typology is of great importance. A metric for the security of an e-commerce application is defined using a different approach then the one used when defining a metric used for the security of a document management application and also the definition process behind the metric used for an electronic voting application is different from the rest.

The validation of each category of security metrics is presented as a volume, as a limit of acceptance and mostly as an effort to obtain the two matrixes

5. Indicator comparative analysis

The comparative analysis of the security metrics presumes a statistic approach, because the result must conclude if an indicator is more representative than another, that the accepted indicator is more suggestive there are

minor risks in having confidence in the indicator when a decision is being made.
If the vulnerability indicator is considered, it must be specified if it refers to the vulnerability of: the database, the communication processes or if the vulnerability refers to the whole software application.
Te comparative analysis presumes:

- using the same concepts concerning the contents, the type of interpretation, the influence factors and the degree of coverage in the security insurance processes regarding the methods and instruments used.
- using the same indicator classes; the indicators must be constructed using the same hypothesis classes; it is important when elaborating the indicator system to use hypotheses which have to be accepted, not to simplify beyond an reasonable acceptance limit the scope of the concepts; in the procedures of collecting data, the collectivities used for measuring must be precisely described to admit that they are representative; al the descriptions are made to permit the verification of the comparison;
- following consecrated hypothesis verification methods, determining the confidence interval.

The comparative analysis in necessary to filter the indicators used to measure the level of security in the software applications , such that, in time stabile indicators will be obtained, easy to calculate and their levels will have the same meaning for all the specialists in the application security typology domain. Further more, the effective levels measurements must be tied to the effort the software component developer is making to improve the security level when it is low, or to increase the degree of security, when its level is unsatisfactory and must become better or the best.

6. Conclusions

When a software application is developed, the security level is also designed, resource allocation planning is made and the measuring techniques are set. In software development there have been security classes defined and rigorous ways to determine the belonging of each product to a specific class. The use of metrics represents the only way to get a clear image concerning the favorable or unfavorable differences of real informatics security compared to the planned security level. Software developers for applications which have security characteristics use metrics to make comparisons to other existing software applications on the market or in use. The detailed results of this research are posted on www.ionivan.ro in the article METRICI ALE SECURITATII SISTEMELOR COLABORATIVE (METRICS FOR SECURITY OF COLLABORATIVE SYSTEMS)

References

[IVAN06] Ion IVAN, Cristian TOMA (coordonatori) – INFORMATICS SECURITY HANDBOOK, Editura ASE, Bucuresti, 2006

[PATR01] Victor Valeriu Patriciu, Ion Bica, Monica Ene-Pietrosanu–Securitatea comertului electronic, Editura ALL,Bucuresti, 2001

[PATR05] Victor Valeriu Patriciu, Ion Bica, Monica Pietrosanu, I. Priescu – Semnaturi electronice si securitate informatica, Editura ALL, Bucuresti, 2005

[IVAN02] Ion Ivan, Paul Pocatilu, Cristian Toma, Marius Popa – Semnatura electronica si securitatea datelor in comerul electronic, revista Informatica Economica , vol.6, nr. 3, 2002, pp 105-110

[PATR94] Victor Patriciu – Criptografia si securitatea retelelor de calculatoare cu aplicatii in C si Pascal, Editura Tehnica, Bucuresti, 1994