AN APPROACH FOR DESIGNING OF ENTERPRISE IT LANDSCAPES TO PERFORM QUANTITAVE INFORMATION SECURITY RISK ASSESSMENT

Anton Romanov and Eiji Okamoto
Department of Risk Engineering, Graduate School of Information and Systems Engineering, University of Tsukuba
Tennodai 1-1-1, Tsukuba Science City, 305-8573, Ibaraki, Japan

Keywords: Information security, Risk assessment, IT landscape design.

Abstract: Nowadays most of enterprises must consider information security aspects as of the highest concern. It is caused not only by growing hacker's activity but also because of increasing legal requirements and compliance issues. One of required procedures to manage information security is regular performing of information security risk assessment. This article describes an approach for designing and managing of an enterprise IT landscapes which makes possible to perform quantitative information security risk assessment using already established methodologies which were previously inapplicable by some reasons. Moreover, application of the proposed framework allows transformation of any IT landscape to such state. Other relevant key features of the proposed approach are unification and reduction of maintenance cost.

1 INTRODUCTION

In the context of rapidly growing (Service Oriented Architecture) SOA development and enforcement of legal requirements (compliance) regular assessment of information security related risks becomes an important element of management of any IT infrastructure of an enterprise. At the current time there are two significantly different approaches to assess information security risks: based on qualitative decisions and based on quantitative estimations. The first group is already widely used in the industry even though the outcome sometimes could be quite doubtful and require so-called adjustment (Munteanu, 2006), but the second group is still mostly a subject to research. Later in this article we will consider only quantitative approaches and the preparations necessary to apply to a given IT landscape to make these approaches applicable to the real enterprise environments.

2 GENERAL WAYS TO REDUCE IS RISKS

From the theoretical point of view it is essential to consider two ways of providing security related (quality assurance service) QAS, see "Figure 1": perform formal verification (i.e. build a formal mathematical model of a given software entity and prove its effectiveness) or perform risk assessment.

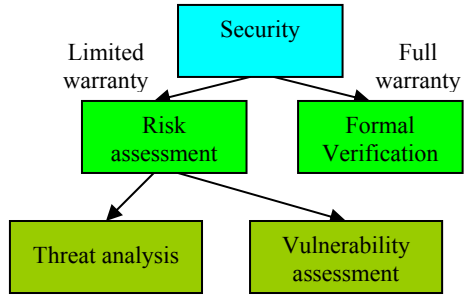

Figure 1: Ways to perform security quality assurance service.

As the first approach is based on mathematical equations, it allows achieving full warranty, though performing risk assessment is able to provide only limited warranty. Approaches to perform formal verification are out of scope of this article and for correct application require redesign of the whole software development life cycle (SDLC).

The way to calculate risk (Bodeaum, 1992) is provided in equation (1), where P_{threat} is a probability

Romanov A. and Okamoto E. (2009).
AN APPROACH FOR DESIGNING OF ENTERPRISE IT LANDSCAPES TO PERFORM QUANTITAVE INFORMATION SECURITY RISK ASSESSMENT.
In *Proceedings of the International Conference on Security and Cryptography*, pages 313-318
DOI: 10.5220/0002224803130318

of a given threat to occur, $P_{vulnerability}$ is a probability of a vulnerability to be exploited, AV is an asset value.

$$Risk = P_{threat} \times P_{vulnerability} \times AV \quad (1)$$

Usually evaluation of asset's value is out of scope of security team members and is performed by business owners of a given asset. So, if there is an asset with some given value, there must be a pair of a threat and relevant vulnerability for any risk to happen.

2.1 Limitation of Current Approaches

Though there are already plenty of methods to measure financial, legal and other non - operational risks, the assessment of operational risks is still a challenge. Up to the current time there were many attempts to create a universal framework to measure risks related to IS (information security) which are a sub group of operational risks, but all of the attempts finished without real success, because of their inapplicability to the real enterprises (Ekelhart, 2007), (Arora, 2004).

The main problem of all of these approaches was connected to superfluous rapid changes which generally occur in most of common IT landscapes used in the industry. For example, if to consider a real enterprise, it would have several types of servers (database, mail, application) and a quite big set of client worksites, which use huge variety of hardware and software solutions. As usually there will be a need to update, replace or repair some of the components both on the server and client side (for example, to apply operating system patches, antivirus updates, install new versions of business related applications to add new functionality or deploy a customer developed software), there is no way to have a stable set of software components for all applications or even just a fixed set of applications in the whole IT landscape even for a single day. A software component in this article is defined as a basic application module to which an application name is usually assigned (for example, Microsoft Windows XP SP3 build 2.6.2700) and all add-ons implemented (like hot fix KB1234567). A software component is defined by its vendor, name, version number and all implemented add-ons names and version numbers.

2.2 Approaches used in Industry

Thus, as a risk is defined by a pair of a threat and vulnerability exploited by that threat, it is essential to consider two ways to find possible risks, see "Figure 1". Ways of performing of threat analysis are usually based on previously obtained experience which is summed up in catalogs of best practice, for example (BSI, 2004). Vulnerability assessment is usually made by different tools, like penetration testing tools. To notice a potential threat there must always be a theoretically possible vulnerability to exploit for a given software or hardware component itself or a group it belongs to. So if to consider information security assurance for an enterprise, most likely a combination of threat analysis and vulnerability assessment would be performed. But as at the current moment tools for vulnerability assessment are still far from accomplishment (at least because different entities of software could have different set of vulnerabilities, so such tools must be updated for any new version of any software component) most of enterprises would mostly focus on threat analysis. Thus, if a potential vulnerability has not yet been discovered by intruders, it would not be possible to define it neither during common security incident response management process which is based on analysis of information from logs and audit trails nor risk management process, as vulnerability tools have very limited functionality and are commonly based on known signatures. As to threat analysis, an enterprise security team usually does not have enough technical knowledge in software and hardware engineering to predict weird problems (simplified information security risk management process is shown on "Figure 2").

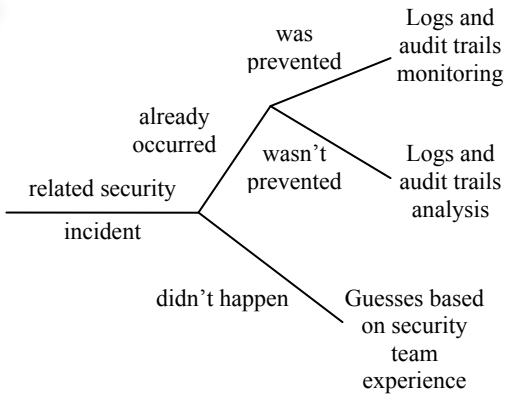

Figure 2: Simplified risk management process.

Thus it is possible to conclude that the problem of inapplicability of current quantitative approaches to measure information security risks is not a fundamental mathematical problem of building such framework, as there are many relevant approaches for financial and credit risks (Di Renzo, 2006), but a

technical problem, as there is no way to collect sufficient amount of statistics because of specifics of current (software development life cycle) SDLC and software life cycle (SLC) models.

3 A PROPOSED APPROACH

Prior to introduction of the proposed approach for designing of enterprise IT landscapes to perform quantitative information security risk assessment (QISRAP, where P stands for preparation) it is necessary to provide some relevant mathematical considerations.

3.1 Mathematical Considerations

As it was pointed out above, because of superfluous changes, if to consider a given IT landscape from the mathematic statistical point of view, it is not possible to assume that the state of landscape is not changing and thus there will be no way to collect any reasonable amount of statistics, related to occurred security incidents. Hence performing an approximation of a cumulative distribution function would also be unavailable. The main problem here is that as it was written above, for a risk to occur there must be a pair of threat and vulnerability. So, for a given enterprise without drastic changes in its organizational structure it is possible to assume that the distribution of threats is permanent. But if to consider vulnerabilities this would be an incorrect assumption as an entity of software is nothing more then a set of CPU instructions, like hardware is a set of primitive electronic elements, which have some given properties (let's call both of them trivial components). So vulnerability usually is not a property of a trivial component itself, but of a fixed set of such components. And it is quite clear that though software entities could have the same name or even version number but different add-ons installed, they could potentially consist of different sets of trivial components and only comparison of hash values can guarantee that these entities are really equal. Hence unequal software entities could potentially lead to different vulnerabilities. To conclude, a replacement of any software or even hardware component leads to potential changes of its vulnerability distribution function and hence changes CDF for security risks. So without some special preparation there would be several problems which ravel ISRA:

- There are no threat lists;
- There are no threat probabilities;
- There are no vulnerabilities lists;
- There are no vulnerabilities probabilities;
- There is no way to collect sufficient information about vulnerabilities;

And if it is still possible to collect information about threat distribution using data from different surveys in other companies from the same industry, which are often performed by different software vendors and audit companies, obtainment of information for vulnerabilities related to all software components would be impossible because of superfluous heterogeneity of IT landscapes of enterprises even within the same industry.

3.2 QISRAP Approach to Prepare for IS Risk Assessment

In the preceding paper (Romanov, 2009), the authors introduced a framework for securely building and managing ERP landscapes (landscapes which include Enterprise Resource Planning systems as the main component) where proposed unification of a set of typical software components and its fixation till the version number for all of the components as a way to reduce maintenance cost of a given ERP landscape and to increase the level of security confidence, because if a security incident happened for a single unified worksite, it would happen for all others under the same external conditions, as all worksites are equal from the hardware and software point of view.

Though previously the accent was made to the way of transference of major security investments from an enterprise to vendors by establishing a set of requirements, let's consider the enhancement of that approach for any random IT landscape from information security risk assessment point of view.

If to consider any IT landscape, it would consist of several types of servers (database, business application, service application servers, DNS or DHCP). Any of them could be represented as a set of abstract layers, see "Figure 3". Hence it is possible to state that amount of total technical vulnerabilities of a given workstation is the sum of vulnerabilities at each layer. As most of users need to perform very common set of business functions, it is possible to fix a suite of all applications needed for performing business functions and likewise there are several types of servers. Thus, it is possible to create a hardware and/or software configuration profiles for a client worksite, mail server, ERP server, database server etc. Of course, there could be some exceptions, but it is better to try to avoid them

as much as possible. Consequently in the context of risk assessment the proposed operation means that we fix all the set of vulnerabilities for the defined configuration profile. Hence observation of security incidents occurring in large number of such typified computers could be considered as a multiple realization of a random variable which has the same distribution of vulnerabilities relevant to this fixed configuration profile and the same distribution of threats from the complete set of all threats peculiar for the organization involved.

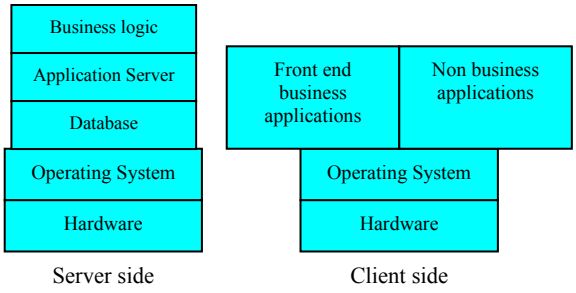

Figure 3: Vulnerabilities layers.

So it means that statistics collected from different samples of the same configuration profile would represent the result of multiple experiments with same probabilistic parameters. And as risk for a given asset is defined by multiplication of two probabilities and a constant asset value (1), and workstations are typified (hence relevant asset values are equal), distribution of threads is the same for the whole organization, and vulnerabilities are fixed for selected configuration profile, it is possible to conclude that gathered statistics could be used to approximate the cumulative distribution function (CDF) of security incidents and consequently losses.

Thus having calculated CDF by creation of fixed set of configuration profiles, further application of any other approaches to assess risks of any nature, like Value at Risk, (Ozcelik, 2005), (Wawrzyniak, 2006) can be made. Stages and outcomes of the proposed approach are presented on “Figure 4”.

It is necessary to note that the framework can be applied to a new enterprise without any IT infrastructure or to already existing enterprise which management is interested in making its current IT landscape more secure and needs extended level of information security maturity in terms of COBIT (ITGI, 2006), (which consequently leads to the need to perform extended assessment of information security risks). Simplified stages description is provided below.

3.2.1 Business Process Reengineering Stage

At this stage all business processes in a given enterprise are investigated. The aim of this stage is to define those business processes which would be or are already automated and possible places where fraud could occur. If controls in main application are unable to prevent all relevant fraud activities, another type of control (software, hardware or procedural) must be introduced.

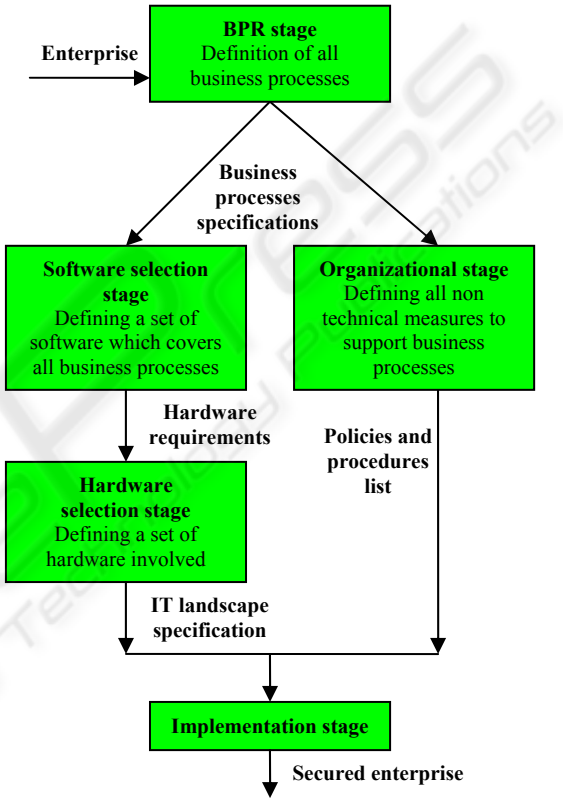

Figure 4: Stages of a proposed framework.

3.2.2 Software Selection Stage

At this stage software solutions which support automated business processes are selected and evaluated according to possibility to provide application controls to prevent potential fraud activities founded during the previous stage. The outcome of this stage is the set of typical configuration profiles to be used for client workstations and servers and hardware requirements in terms of reliability, performance and support for software security controls (for example, if users are allowed to use external memory devices, they can copy confidential data, so a set of controls to prohibit such operations must be introduced). All software components selected for a given profile

must be fixed in terms of vendor name, software name, version number, add-on names, add on version numbers. Unified installation distributives for each configuration profile must be prepared.

3.2.3 Hardware Selection Stage

At this stage relevant hardware is selected. It should be able to cover requirements caused by selected software profiles, but also should not introduce any new risks. If it causes any additional security related risks, appropriate solutions must also be selected. All hardware components selected for a given profile must be fixed in terms of vendor name, device model name, firmware version number.

3.2.4 Organizational Selection Stage

At this stage all non automated procedures are analyzed. According to potential fraud activities not covered by technical controls, a list of relevant policies and procedures to mitigate the risk must be created.

3.2.5 Implementation Stage

At this stage all solutions introduced in upper stages are implemented. If there is already built IT landscape, appropriate changes to it must be performed according to requirements form previous stages (for example, a set of worksites which has similar hardware configuration and requirements to software should be defined, a software image should be created and applied to these worksites). All relevant policies and procedures must be created.

3.2.6 Change Management Process

In case of need to perform an update for a sample of a given configuration package, all other samples of this package must be updated simultaneously or, if technically impossible, at least during the smallest possible period of time. All changes in configuration packages must be documented by the same way as previously all configuration packages content were documented.

3.3 Goals and Feature of Proposed Approach

If this approach would be supported by many companies and they would share their incident statistics (which perhaps would not happen without a relevant law enforcement) or if there would be one single company which has large amount of samples of a given configuration profile, then hypothetically it would be possible to achieve a situation when all the vulnerabilities of a selected configuration profile are iteratively defined, enumerated and covered by defined countermeasures, see “Figure 5”.

As stated in (Arbaugh, 2000), the time to discover a given vulnerability is finite, see “Figure 6”, so if there will be no changes in configuration profile, state with complete mitigation of all vulnerabilities for a given threat distribution is achievable.

Moreover, a proposed framework allows to reduce maintenance cost and increase security assurance level, as it is essential that the more software is used the more potential vulnerabilities it could contain and the more different applications are installed the higher would be the maintenance cost, as, for example, it would lead either to demand for qualified staff who would be able to configure all these systems or to huge budget for external consulting. Thus it is possible to conclude that superfluous heterogeneity is beneficial to intruders and unbeneficial to security team as it is much more difficult to manage an IT landscape with huge amount of different software and hardware components, apply critical security updates and even perform backup and restore.

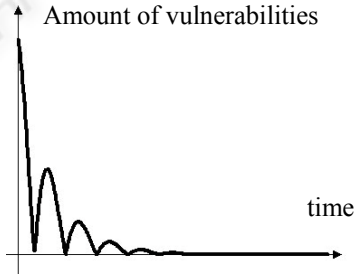

Figure 5: Vulnerabilities mitigation process.

The last question to consider here is the question related to application of different patches and critical updates from variety of vendors, as it is clear that installation of such patches could potentially change vulnerabilities distribution and disallow collecting of sufficient amount of statistical data. The authors consider two possible ways to deal with this problem: either trying to cover problems resolved in such patches by external solutions (which for sure is not always possible) or applying special acquisition procedure which must include deep functions testing (based on source code or disassembling) or certification by authorized third party laboratory for ISO 115408 with Evaluation Assurance Level (EAL) higher then 4 (as it includes source code

testing). Though this requirement is quite strong and could be considered as a potential limitation of this study.

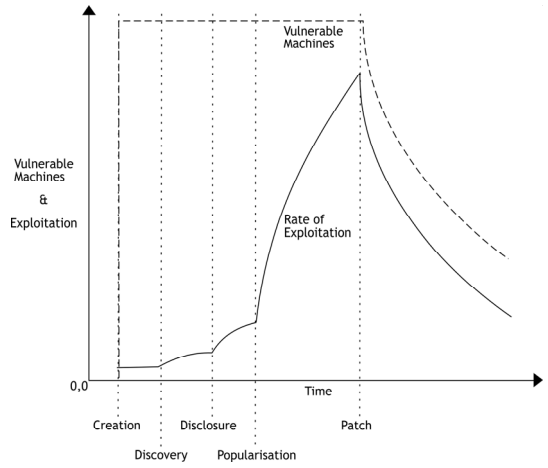

Figure 6: Vulnerabilities life cycle process.

4 CONCLUSIONS

This paper has presented an approach for designing and managing of enterprise IT landscapes which allows performing quantitative information security risk assessment by introducing configuration profiles which fix vulnerabilities distribution for large sets of workstations and thus stabilize CDF related to IS risks. Application of this approach to a given IT landscape would help not only to perform ISRA using any of already available methodologies to evaluate other types of non operational risks, but also to increase level of security assurance and to decrease maintenance cost.

Further research needs to be performed to test the proposed model on huge IT landscapes and build recommended configuration packages for typical client worksite and server workstations. The time required to gather sufficient amount of IS incidents statistics needs to be estimated and reduced by all possible ways. The correctness of combination of practical results obtained after application of the proposed model with already developed RA approaches also needs to be performed.

REFERENCES

Arbaugh, W.A, Fithen, W.L., and McHugh, J., 2000. Windows of Vulnerability: A Case Study Analysis. In *Computer, volume 33, issue 12*, 52-59.

Arora, A., Hall, D., Pinto, A., Ramsey, D., and Telang R., 2004. An ounce of prevention vs. a pound of cure: How can we measure the value of IT security solutions? In *Lawrence Berkeley National Laboratory.* Paper LBNL-54549. http://repositories.cdlib.org/lbnl/LBNL-54549

Bodeaum, D.J., 1992. A Conceptual Model for Computer Security Risk Analysis. In *Proceedings of Eighth Annual Computer Security Applications Conference*, San Antonio, TX, 56-63.

Bundesamt fur Sicherheit in der Informationstechnik (BSI), 2004. Threat catalogue for IT Grundschutz Manual.

Di Renzo, B., Hillairet, M., Picard, M., Rifaut, A., Bernard, C., Hagen, D., Maar, P., and Reinard, D., 2007. Operational risk management in financial institutions: Process assessment in concordance with Basel II. In *Software Process: Improvement and Practice volume 12, issue 4*, 321-330.

Ekelhart, A., Fenz, S., Klemen, M., and Weippl, E., 2007. Security Ontologies: Improving Quantitative Risk Analysis. In *Proceedings of the 40th Annual HICSS*. IEEE Computer Society, Washington, DC, 156a.

IT Governance Institute, 2006. Control Objectives for Information and Related Technology (COBIT).

Munteanu, A., Ioan, A., 2006. Information Security Risk Assessment: The Qualitative Versus Quantitative Dilemma. In *Proceedings of 6th IBIMA*, Bonn, Germany, 227-232.

Ozcelik, Y., Rees, J., 2005. A New Approach for Information Security Risk Assessment: Value at Risk, from http://ssrn.com/abstract=1104264

Romanov, A., Okamoto, E., 2009. A Framework for Building and Managing Secured ERP Landscape. In *Proceedings of the 2009 International Conference on Security and Management,* Las Vegas, NV (being printed).

Wawrzyniak, D., 2006. Information security risk assessment model risk management. *LNCS 4086*, Springer-Verlag Berlin Heidelberg, 21-30.