Application of Security Metrics in a Metropolitan Network : A Case Study

Rodrigo Sanches Miani*, Bruno Bogaz Zarpelão*, Leonardo de Souza Mendes*
*School of Electrical and Computer Engineering
University of Campinas (UNICAMP)
Campinas, Brazil
Email: {rsmiani,bzarpe,lmendes}@decom.fee.unicamp.br

***Abstract*— The information security issues in the current communication networks demand the development of efficient methods to find security vulnerabilities and facilitate the decision making process. Security metric is a widely used concept in this area. The metrics can indicate the actual level of a specific security target and may determine the actions that should be taken. This work presents a case study about the security metrics implementation in the Open Access MAN (Metropolitan Area Network) of Pedreira, a city located on southeast of Brazil. The paper also presents a methodology for data gathering and analysis to support the security metrics implementation, the security metrics that were used in the case study, the metrics program results and some discussions about the benefits and disadvantages of the security metrics usage.**

Keywords*— *Communication systems, Computer network management, Computer network security, Security metrics, Open access metropolitan area network

I. Introduction

In order to deal with the great diversity of security issues, it is necessary to invest in implementation of security controls. The characteristics of these investments must be carefully accounted for and can be defined from measures and analysis of the overall information security structure. This process may be formalized using security metrics [1].

Metrics can be defined as a set of measures that can generate a quantitative approach about a problem [2]. Security metrics may support the development of a common approach to standardize the security controls and methods. Typical examples of security metrics are: patches applied per period, rate of host uptime and workstations covered by antivirus software.

Our case study target, the Open Access MAN also known as Open Access Network (OAN) can be defined as the convergence of services, applications and infrastructure to create a community communications network of a city [3]. The Open Access MAN is characterized by a variety of services that intend to reach every sector of the society, providing information access to the citizens. The need for data privacy and the high number of users, create new challenges related to information security in such networks.

A security metrics model for Open Access MANs was proposed in our previous work [4] and [5]. The attributes of a metric and a simple approach for defining the metrics formula were showed in [4]. In [5], it was defined an alternative approach for the security metrics formula, including a new component, called intersection component. In this paper, we address the problem of security metrics implementation by using a case study performed in the Open Access MAN of Pedreira. Moreover, the security metrics used in the case study will follow the guidelines described in [4] and [5].

The focus of this work is to define a methodology for data gathering and analysis to assist the security metrics implementation and to present the main challenges in the development of a security metrics program using a case study performed in the Open Access MAN of Pedreira, a city located on the state of São Paulo, Brazil.

This paper is organized as follows. Section 2 presents some related work associated to security metrics. Section 3 shows the proposed methodology for data gathering and analysis that was applied in the case study. Section 4 describes and discusses the case study. In section 5 we present the final considerations and future work.

II. Related Work

Jansen [6] provides an overview of the security metrics area and look at possible avenues of research that could be pursued to advance the state of the art. The author states that much of what has been written about security metrics is definitional, aimed at providing guidelines for defining a security metric and specifying criteria for which to achieve. However, relatively little has been reported on actual metrics that have been proven useful in practice.

Some examples of security metrics applications are presented by Savola [7]: risk management activities in order to mitigate security risks, comparison of different security controls or solutions, obtaining information about the security posture of an organization and a process, certification and evaluation of a product or an organization.

In this paper, we will propose a methodology for security metrics implementation. Iversen and Kautz [8] describe ten principles that may be valuable to a metrics implementation effort. The principles are: 1) use improvement knowledge, 2) use organizational knowledge, 3) establish a project, 4) establish incentive structures, 5) start by determining goals, 6) start simple, 7) publish objectives and collected data widely, 8) facilitate debate, 9) use the data and 10) evaluate the metrics program to further improve. These principles are general and can be used in any metrics program. Our aim is to propose a specific methodology for security metrics implementation.

Swanson et al. [9] proposes a security metrics development process composed by seven steps: 1) stakeholder interest identification, 2) goals and objective definition, 3) information security policies, guidelines, and procedures review, 4) information security program implementation review, 5) metrics development and selection, 6) metrics development template and 7) feedback within the measures development process.

Payne [10] also proposes seven steps that could be used to guide the process of establishing a security metrics program: 1) define the metrics program goal(s) and objectives, 2) decide which metrics to generate, 3) develop strategies for generating the metrics, 4) establish benchmarks and targets, 5) determine how the metrics will be reported, 6) create an action plan and act on it, and 7) establish a formal program review/refinement cycle.

The methodologies presented ([9], [8], [10]) does not propose well defined steps to assist the implementation and analysis of security metrics. They only describe some important tasks required for the use of security metrics.

Based on this facts, our proposal consists in a concise and efficient methodology to support the security metrics implementation and analysis of the obtained results.

III. Proposed Methodology

Before the metrics application, it is necessary to work on some issues such as: which metrics will be applied, how and where to gather information and how to analyze the obtained data. The proposed methodology aims to support the solution of such issues. The eight steps that define the methodology to support the security metrics implementation and analysis are:

1) Define which metrics will be applied

The metrics that will be applied must be chosen together with the IT department, considering the organization priorities. The decision can be made using several conditions as: financial issues, metrics simplicity, security aims predefined, availability and capability of human resources and others.

2) Prepare the environment for data gathering

The environment adequacy for the data gathering starts with an organization reconnaissance. Information about: network topology, network diagrams, hardware and software description, IP addresses, number of servers/workstations, personnel information and security policies should be obtained. Moreover, the gathering tools that will be used must be defined, according to the chosen metrics and the organization requirements.

3) Automate the data gathering tools

The automation of data gathering tools can provide the following major benefits: standardization, accuracy, repeatability, increased measurement frequency, reliability, transparency and auditability [11]. Besides, the generated data can be used as input data for the development of an integrated gathering tool.

4) Data gathering

Basically, there are four ways to make data gathering: using specific audit tools, log analysis, technical reports and interviews. The data gathering process should not be intrusive for the network operation.

The data gathered should be stored in information databases. This repository is important to make comparisons between the measurements enabling the before-and-after process [11].

5) Formula calculation for each metric

Every metric result is expressed by a formula. From the result of the formula, the metric value or indicator is obtained, and it is usually expressed in percentage terms.

6) Organize the metrics according to the results

A simple approach for the establishment of the security controls priorities is to organize the metrics according to the results, in a descending way.

7) Aggregate the metrics results according to its classification

Proposing a reorganization of the results, according to the metrics classification, may provide a better view about the sources of the security issues. In our study, the metrics will be classified according to the Open Access MAN layers [4]: network structure, interconnection node or services. The network structure of the Open Access MAN can be based on four technologies: optical fiber, wireless, dedicated access or hybrid. The Open Access MAN can also be classified according to the nodes: public buildings, private buildings and residences. Once the infrastructure is ready, several services can be made available for the citizens.

8) Metrics data analysis

The aim of the analysis is to identify the gap between the actual and the desired performance of the security controls and discover the vulnerable areas. Some tools that can be used to make data analysis are the generation of security indicators by ordering and grouping metric results, grouping the measures within a particular scope of analysis, aggregating the data, using statistics and analyzing the data behavior over the time.

IV. Case Study - Open Access MAN of Pedreira

The Open Access MAN of Pedreira is a project that has being developed by the University of Campinas (UNICAMP) and by the government of Pedreira. The project started in 2005 and officially launched in 2007. The network infrastructure is constituted by an optical backbone, which links the city schools, health centers and other important buildings, forming the main network core. There are also wireless access points, assembled in the form of wireless microcells, offering free Internet access for the citizens.

According to the proposed methodology, the first step is to define which metrics will be applied. The following nine metrics were chosen together with the Pedreira's network management. The critical factors for the metrics definition were: choice of metrics with low impact on the network performance, usability of softwares already installed and preference of metrics with data that could be collected remotely.

It is important to note that this set of metrics are not sufficient to express the security state of the entire network.

This is an open issue in security metrics field, and some discussions about this subject can be found in [6]. Here, we would like to know the security degree of the components measured by the choosen metrics.

Due to space limitations, we will only describe the objective, classification and the measures of the choosen metrics. The gathering frequency of all metrics was ranged from one to four months, and the data source included network administrators interviews, system logs, auditing and tracking tools.

1) Security between nodes connections

This metric goal is the analysis of the security level between the node connections. The measures are: number of buildings, number of buildings that has firewall resources or logical access control among the connections, number of buildings using cryptography and number of buildings with firewall and cryptography. Also, the cryptography component will receive different weights depending on the key size. The metric classification is Network Structure.

2) VoIP security requirements

This metric goal is the security level study of the VoIP network. The attributes are: number of VoIP branches, number of VoIP calls in a period, number of ciphered VoIP branches, number of VoIP branches that are in segregated networks, different from the data network, number of VoIP calls not completed and number of ciphered VoIP branches and number of ciphered branches in segregated networks. The metric classification is Services.

3) Users account management

The metric aim is to evaluate the users account management in the Open Access MAN nodes. The measures are: number of users account, number of workstations, number of users with administrator privileges and number of workstations using the adminstrator account as the work account. The metric classification is Interconnection nodes.

4) Wireless network security

The measured attributes are: number of AP's (Access Points), number of AP's with enabled security protocols (excluding WEP), number of AP's with default passwords, number of AP's with default Service Set Identifier (SSID), number of AP's with obsolete versions of software and number of AP's with open authentication. The metric classification is Network structure.

5) Availability and reliability of servers

The aim here is to evaluate the impact of the unplanned downtime and the servers availability. The attributes are: number of servers, number of hours, number of servers with redundancy resources, number of servers that are in the backup program, number of servers that store the backups in security offsite, uptime mean of servers and number of servers with redundancy that are in the backup program. The metric classification is Services.

6) Internet link management

This metric goal is to measure the Internet link usage, allowing the development of baselines for analysis of historical data, link capacity and abusive usage. The measured attributes are: Internet bandwidth in Mbits/s, number of nodes with Internet access, Internet average bandwidth (upload and download), number of workstations with external Internet access. The metric classification is Service.

7) Security patch application in servers

This metric goal is to measure the efficiency of the security patch application in the Open Access MAN servers. Therefore, the vulnerability indicator of each server will be measured using the CVSS (Common Vulnerability Score System) [12]. The CVSS score is ranged from 0 to 10 for each vulnerability, with 10 for the higher severity.

The formula will be expressed by the mean among the CVSS scores found in each server. The final result must be divided per 10, to preserve the scale previously defined. The metric classification is Interconnection nodes.

8) Password complexity

The aim here is to measure the password complexity of the Open Access MAN servers, routers and access points. The password complexity is calculated using the Password Strength Meter, [13]. The software output is a complexity password score ranged from 0 to 1, with $0 =$ low complexity and $1 =$high complexity. The measures are: number of servers, number of routers, number of access points, mean of complexity password scores of servers, routers and access points. The metric classification is Network structure.

9) Open Access MAN segmentation

The metric goal is to evaluate the network segmentation level of the network. This metric is important because the nodes that do not have the same interest domain, should be logically or physically segregated from the others. This can be made using VLANs (Virtual Local Area Networks) or Firewalls in the application level, or creating other physical sub-networks. The attributes are: number of domains and the number of domains that access other domains that aren't defined by the internal security policies. The metric classification is Network structure.

In the second step of methodology we need to collect some general information about the network in order to support the gathering tools definitions. Until October 2009, the Open Access MAN of Pedreira had: 17 buildings (10 connected by optical fiber and 7 by wireless link), 60 VoIP branches, 5 Access Points used both for internal access and for the citizen access, 5 servers, 214 workstations, 13 radios for the wireless link, 14 network domains, a single 2Mbits Internet link, 2 routers and 19 switches.

According to the chosen metrics and the information collected it was possible to select the following gathering tools: RemoteAssetTracker [14] to audit the workstations, shell-scripts to measure the uptime in the servers, MRTG (Multi Router Traffic Grapher) [15] to monitor SNMP network devices and gather information about the Internet bandwidth, Nessus Vulnerability Scanner [16] and Ping tools to test the network access. We also retrieve information by making interviews with network managers and auditing the network equipments.

Considering the third step of methodology, we only achieved good levels of automation using the RemoteAssetTracker tool, shell-scripts and MRTG.

TABLE I
RESULTS - GOOD AND BAD POINTS

Metric	Result	Good	Bad
1) Security between node connections	0.3271	i) Access List implemented in all buildings.	i) Lack of cryptography in 10 of 17 buildings; ii) DES usage, 64 bits cryptography; iii) Lack of cryptography in the Municipal Hall.
3) User account management	0.3678	i) 0.02% of Municipal Hall PCs uses the "Administrator" as work account.	i) Lack of domain controller; ii) 92% of all users accounts has administrative privileges.
7) Security patch application in servers	0.389	i) Few vulnerabilities in the VoIP server.	i) Firewall: 136 security vulnerabilities found and CVSS average score of 0.5877; ii) Mail Server: 75 security vulnerabilities found and CVSS average score of 0.5681; iii) VoIP: CVSS average score of 0.6841.
4) Wireless network security	0.5	i) Security policies implemented for default passwords, SSID and open authentication in all AP's.	i) WEP usage.
2) VoIP security	0.6046	i) The whole VoIP network is isolated from the data network; ii) 4% of missing calls.	i) Lack of cryptography .
5) Availability and reliability of servers	0.7217	i) All servers are in the backup program; ii) 99.86% of average availability; iii) 2/3 of servers has remote backup.	i) Only the Mail server has redundancy services.
8) Password complexity	0.7666	i) Servers: 0.71 of complexity password rate; ii) Routers: 0.8 of complexity password rate; iii) Access Points: 0.79 of complexity password rate.	i) One password found with 0.38 of complexity rate.
6) Internet link management	0.8756	i) 99% of PCs uses the Internet provide by the government; ii) 26.52% of average download link usage; iii) 8.07% of average upload link usage.	
9) Open Access MAN segmentation	0.9285	i) 92.85% of networks were correctly segmented.	

After that, it was started the security metrics application, in the period between February and October of 2009. The next subsection will show the results of the case study and how the steps 5 to 8 of the proposed methodology were executed.

A. Results and Analysis

The result of each metric is presented in Table I. The column "Results" is related to the metric quantification. The quantification was made using the model proposed by Miani et al. [5]. The model consists in calculating the arithmetic and weighted mean of the metrics attributes, generating a single value for each metric. This value or indicator varies between 0 and 1, with 0 for the lowest secure level and 1 for the highest security level.

The results, in general, can be considered satisfactory, since if we consider that this was the first security test applied to the network. The Table I also represents the steps 5 and 6 of the methodology.

In particular, two results caught our attention. The first one was the bad performance of the security patch application program in the servers. And the second one was the use of WEP on all access points. Another bad result, related to the users account management metric, occurred as expected, due to lack of human resources to manage more than 200 computers.

The results of Table I can also be sorted according to the metric classification, as proposed in the seventh step of the methodology. Thus, it is possible to visualize the areas of the Open Access MAN that had the best performances. By grouping the metrics according to its classification and calculating the mean, we will have the following results: Network structure $= 0.6305$, Services $= 0.7339$ and Interconnection nodes $= 0.3784$.

The entire IT (Information Technology) infrastructure of the public buildings such as workstations and human resources belongs to the municipality and so far has not been part of the Open Access MAN project. The lack of resources, security policies definition and investments were crucial for the results of the metrics 3 and 7 and consequently for the Interconnection node layer.

The data analysis (last step of methodology) revealed interesting information such as the possibility of unauthorized access from a particular network domain to another network domain, the high password complexity of servers, routers and switches, the reliability of the VoIP network, the high rate of users with administrators privileges, the high latency in the distribution of security patches for servers and others.

The analysis also show some deficiencies in the metrics applications. One of them is the requirement of lots of input data, which can turn the security metrics implementation into a big problem for the IT managers. For an accurate analysis, a large set of metrics should be applied, which consequently implies in a lot of data gathering. The data extraction, which will feed the metrics, often depends on adequate software, updated hardware, well-defined computational infrastructure and qualified network administrators. However, for managers, these factors may imply in high financial costs.

Another difficulty that should be mentioned is the lack of specific tools for the implementation of security metrics. A typical tool to support the implementation of security metrics could be developed using the flow: automating the data gathering, writing the data in a database and performing data analysis. The development of such a tool would contribute to the development of security metrics, specifically for their usage in several sectors like private companies, universities, government and large scale networks.

The selection of appropriated metrics proved to be complex. The decisions taken by the network management was based on two factors: financial costs and the metrics simplicity. Metrics with a higher level of complexity, which would require a great effort to gather, were discarded. Similarly for the metrics that required high investments for its application.

Despite the deficiences and difficults found, the metrics application brought some benefits to the Open Access MAN of Pedreira such as: beginning of studies for application of cryptography in the VoIP branches, development of a domain controller for the workstations, deployment of backups in security offsite, increase of Internet link bandwidth, revision of access control policies and implementation of *Access Control Lists*, deployment of a server used to manage the bandwidth destined for the citizens and awareness of chiefs and managers about information security risks.

The implementation of security metrics in a large-scale and heterogeneous network such as the Open Access MAN of Pedreira showed good results. It was very effective in the visualization of issues and also for the development of a knowledge base on network security. Metrics also have been useful for the evaluation of the IT investments. However, in order to ensure the continued success of security metrics, the implementation should be continuously evaluated and improved [8]. In doing so, new metrics and gathering tools can be added, data sources can be changed and analysis on historical data can be made.

The case study revealed some important questions, which, if properly treated, may increase the efficiency of the security metrics implementation. We can highlight the following issues: i) security team trained to work with metrics, ii) a simple and well defined methodology for the metrics application, iii) development of suitable methods to support the selection of appropriated metrics and iv) development of specific and automated tools to assist the data gathering and analysis.

V. Conclusion and Future Work

The methodology proved to be useful and easy to apply. It can be considered a good starting point to assist the implementation of a security metrics program. However, the security metrics depend on the context in which they are applied. Each company may develop their own way of defining and using metrics. Therefore, the mere application of steps is no guarantee for success, as observed by Iversen and Kautz [8]. Our goal here was to create a simple, but formal process to support the hard task of security metrics implementation.

Besides the relevance of results and the benefits, the case study proved to be a rich field experience due to the direct interaction with several technologies and also by the diversity of real problems faced. The possibilities in a scenario where a security metrics program is regularly applied are many and include: detailed knowledge of the solutions adopted and its related impacts, prediction of possible security issues, development of an information security database and application of financial investments in information security area with high level of accuracy.

The studies presented in this work also opened up several possibilities for future work, such as: application of the proposed models in other case studies, development of software for efficient storage of collected data in order to enable historical queries, regression analysis and simulations, development of new security metrics for Open Access MANs, and also studies about the efficient selection of metrics, according to the specific characteristics of an organization.

Acknowledgment

The authors would like to thank the State of São Paulo Research Foundation (FAPESP) that supports this work.

References

[1] S. Weiss, O. Weissmann, and F. Dressler, “A comprehensive and comparative metric for information security,” in *Proceedings of IFIP International Conference on Telecommunication Systems, Modeling and Analysis (ICTSM2005)*, nov 2005, pp. 1–10.

[2] P. W. Lowans, “Implementing a network security metrics program,” SANS, Tech. Rep., 2002.

[3] L. S. Mendes, A. C. G. Inocencio, A. Panhan, and M. Tilli, “Bringing together digital cities and open acess mans,” in *Annals of The 2008 Networking and Electronic Commerce Research Conference*, 2008.

[4] R. S. Miani, B. B. Zarpelão, L. de Souza Mendes, and M. L. P. Jr., “Metrics application in metropolitan broadband access network security analysis,” in *SECRYPT 2008 - International Conference on Security and Cryptography*, 2008, pp. 473–476.

[5] R. S. Miani, F. M. Pires, and L. de Souza Mendes, “An alternative approach for formula modelling in security metrics,” in *SECRYPT 2009 - International Conference on Security and Cryptography*, 2009, pp. 381–386.

[6] W. Jansen, “Directions in security metrics research,” National Institute of Standards and Technology (NIST), Tech. Rep., 2009.

[7] R. Savola, “Towards a security metrics taxonomy for the information and communication technology industry,” in *Software Engineering Advances, 2007. ICSEA 2007. International Conference on*, 25-31 Aug. 2007, pp. 60–60.

[8] J. H. Iversen and K. Kautz, “The challenge of metrics implementation,” in *Proceedings of the 23nd Information Systems Research Seminar in Scandinavia (IRIS 23)*, 2000.

[9] M. Swanson, N. Bartol, J. Sabato, J. Hash, and L. Graffo, “Security metrics guide for information technology systems.” NIST Special Publication 800-55, Tech. Rep., 2003.

[10] S. C. Payne, “A guide to security metrics,” SANS Security Essentials GSEC Practical Assignment Version 1.2e, June 2006.

[11] A. Jaquith, *Security Metrics - Replacing Fear, Uncertainty and Doubt*. Addison-Wesley, 2007.

[12] P. Mell and K. Scarfone, “A complete guide to the common vulnerability scoring system version 2.0,” http://www.first.org/cvss/cvss-guide.html, June 2007.

[13] J. Todnem, “Password metter,” http://www.passwordmeter.com/.

[14] AdminPCTools, “Remote asset tracker,” http://www.adminpctools.com/asset-tracker/.

[15] T. Oetiker, “Mrtg - the multi router traffic grapher,” http://oss.oetiker.ch/mrtg/.

[16] Tenable, “Nessus: The network vulnerability scanner,” http://www.nessus.org/nessus/.