METRICS APPLICATION IN METROPOLITAN BROADBAND ACCESS NETWORK SECURITY ANALYSIS

Rodrigo S. Miani, Bruno B. Zarpelão, Leonardo de Souza Mendes and Mario L. Proença Jr.
School of Electrical and Computer Engineering (FEEC), University of Campinas, Campinas, Brazil
Computer Science Departament, State University of Londrina, Londrina, Brazil

Keywords: Metropolitan networks, Security metrics, Security Analysis, Network Security.

Abstract: This work proposes the development and application of specific security metrics for metropolitan broadband access networks that aim to measure the efficiency of security programs and support action planning against detected problems. The approach presented in this work show metrics developed for these networks and parameters for metrics definition. This paper also presents results achieved from application of the metrics reported here in the metropolitan broadband access network of Pedreira, a city located in São Paulo, Brazil.

1 INTRODUCTION

Metropolitan broadband access networks (MBAN) can be defined as the convergence of services, applications and infrastructure to create a community communications network of a city.

The MBAN is characterized by a variety of services that intend to reach every sector of the society in an universalization process of information access. The need for data manipulation privacy and the high number of users create new challenges related to information security in this network's paradigm. Our work proposes the utilization of security metrics as an important tool for the solution of the questions involving the presented scenario. CERT (2006) recommends the usage of security metrics for dealing with the security vulnerabilities that may occur in MBANs.

Through a combination of pre-defined objectives, collection and data analysis, security metrics can indicate the actual level of security we must aim at, directing the actions that network administrators must take to secure the network (Patriciu et al 2006).

Weiss et. al. (2005) proposes a technique to measure organizations security. This technique consists in identifying several scenarios of threats that have the same function of the metrics here proposed, and the creation of a security index for these scenarios. The index is calculated using the percentage of lost assets with possible attack scenarios. Our proposal consists in the creation of indexes considering the current state of security components of a metric.

The contributions of this work are: i) definition of a security metrics model for MBANs, ii) creation of a generic model for formulas calculation of security metrics and standardization of names and terms related to security metrics, iii) presentation of five security metrics for MBANs.

This paper is organized as follows. On section 2, we define classification concepts of MBANs. In Section 3, we show how to build security metrics for MBANs and the mathematical model for metric indicator calculation. Section 4 brings a general view of a MBAN developed in Pedreira, Brazil, and preliminary results related to proposed metrics utilization. In Section 5 we present the final considerations.

2 MBAN CLASSIFICATION

A MBAN can be classified according to the three layers model, composed by: i) Network structure, ii) Interconnection points and iii) Services (Alexiou et al. 2006).

The network structure of a MBAN can be based on four technologies: optic, wireless, dedicated access (e.g. ADSL, cable network) or hybrid.

A MBAN can also be classified according to the type of the points connected. There are three categories of connections: public buildings (schools, hospitals, etc); private buildings (industries); and

S. Miani R., B. Zarpelão B., de Souza Mendes L. and L. Proença Jr. M. (2008).
METRICS APPLICATION IN METROPOLITAN BROADBAND ACCESS NETWORK SECURITY ANALYSIS.
In *Proceedings of the International Conference on Security and Cryptography*, pages 473-476
DOI: 10.5220/0001924204730476

residences. Once the infrastructure is ready, several services can be made available for the MBAN users, as shown in (Ford & Koutsky, 2005). Some of these are: Internet distribution, VoIP, E-gov systems, information programs for education departments, and video sharing systems.

This classification allows the treatment of security problems separately in each of the layers of the MBAN model. This procedure permits a better understanding about security within each layer and, consequently, the analysis of the respective potential problems.

3 SECURITY METRICS APPLIED TO MBANS

Here, we present an approach for definition and application of security metrics that unite methodology concepts proposed by (Payne, 2006), (Swanson et al. 2003) and (Jaquith, 2007). The set of attributes defined for the MBAN security metrics are the following.

Objectives: The metrics proposed in this work were developed to attain the following general objective: *the metrics must be able to allow an efficient analysis of the security risks and respective counter measures at the three levels of MBAN.* This generic objective could be used for development of other security metrics for MBANs.

Besides the main objective above mentioned, specific objectives for each metric may be defined.

Metrics and measures: Identification of metrics and measures are realized from the acknowledgment of the essential security objectives inside a MBAN that must lead to accomplishment of these goals. The metrics are obtained from the analysis of data measured over the operation of the network.

Data source and frequency: The data source includes network administrators interviews, system logs, auditing, and tracking tools (Swanson et al. 2003). Frequency defines the periods of time that data shall will be gathered.

Metrics classification: A metric can be classified accordingly to the MBAN layers presented in section 2. It means that each metric will be related with one ore more MBAN components

Formula: Formula (Swanson et al. 2003) describes the calculus that must be done for metric quantification in a numeric expression. Formula's input data is obtained from realized measures. From the result of the formula, it is obtained a value or indicator for the metric that varies between 0 and 1, with 0 for the lowest and 1 for the higher value.

3.1 Formula Modeling

Despite some interpretation flaws (Box et al. 1978), we define the formula using the arithmetic mean. Our goal is the creation of a indicative that represents the security level of a metric.

Consider a metric *M*, which is composed by components denoted by a_1, a_2, ..., a_n and $a_i \in \Re^*$, being $\Re^*$ the non-negative real numbers set. The formula *F* of a metric can be defined as a relationship between the components a_1, a_2, ..., a_n satisfying the condition $0 \leq F \leq 1$.

Take the set of the components a_1, a_2, ..., a_n. For each a_i, let a_t be the maximum value that this measure assumes. For example, if a_1 represents the number of infected computers, the respective maximum value a_t will be the total number of computers.

Definition 1: *a component a_n is said insecure if, when its value increases, the risks of security problems of the correspondent metric objectives increases too.*

Definition 2: *a component a_n is said secure if, when its value increases, the risks of security problems of the metric objectives decrease.*

Consider an insecure component a_i. Let a_t be its maximum value. We denominate $CI = \left(\frac{\frac{a_i}{a_t} \cdot 100}{100} \right)$ as *normalized insecure component.* Analogously, for a secure component a_i with a_t as its maximum value, we can define *CS* as *normalized secure component*.

Let *X* be a set of normalized secure components, *Y* a set of normalized insecure component and a metric *M*. Consider the possible cases about *M*:

Case 1 – *M* is composed only by secure components.

The formula of *M* will be given by the mean of normalized secure components:

$$F_M = \overline{X}$$

Case 2 – *M* is composed only by insecure components.

The same as the case 1, but to preserve the relationship 0 = *low security* and 1 = *high security*, the formula will be modified as:

$$F_M = \left(1 - \overline{Y}\right)$$

Case 3 – M is composed by insecure and secure components.

In this case, the formula will be given by the mean between the secure and insecure components.

3.2 Metrics Description

Next, we present five security metrics for MBANs.

1) Metric: Buildings connected using information security technologies.

Objective: To analyze and to increase security level among MBAN buildings.

Data source: Interviews with network administrators and network equipment auditing.

Frequency: Monthly or every two months.

Classification: Network structure.

Measures: a_t = total number of buildings, a_1 = number of buildings with firewall resources, a_2 = number of buildings with secure connections.

Formula:

$$F_1 = \overline{X} \text{ with } X = \left\{ \frac{a_1}{a_t}, \frac{a_2}{a_t}, \right\} \quad (1)$$

2) Metric: Ratio between administrator users and desktops.

Objective: To reduce the number of desktop users with administrative privileges in the MBAN.

Data source: Auditing tools such as Network Management Suite (2008).

Frequency: Monthly for baseline establishment; then, every three months.

Classification: Interconnection point.

Measures: a_t = total number of users and a_1 = total number of administrative users.

Formula:

$$F_2 = \left(1 - \overline{Y}\right) \text{ with } Y = \left\{ \frac{a_1}{a_t} \right\} \quad (2)$$

3) Metric: Ratio of wireless connections with security protocols enabled.

Objective: To increase security level of wireless connections.

.**Data source:** Equipment auditing, scanner tools like AirSnort (2004).

Frequency: Monthly.

Classification: Network structure.

Measures: a_t = total number of APs (Access Points), a_1 = number of APs without security protocols, including WEP, a_2 = number of APs with default passwords

Formula:

$$F_3 = \left(1 - \overline{Y}\right) \text{ with } Y = \left\{ \frac{a_1}{a_t}, \frac{a_2}{a_t} \right\} \quad (3)$$

4) Metric: Ratio of servers with backup and redundancy services. Servers' ratio uptime.

Objective: To increase availability and reliability of MBAN servers.

Data source: Monitoring and auditing in the servers.

Frequency: Monthly.

Metric classification: Services.

Measures: a_{t1} = number of servers, a_{t2} = number of hours, a_1 = number of servers with redundancy, a_2 = number of servers in the backup program, a_3 = number of servers with remote backup, a_4 = mean of servers uptime.

Formula:

$$F_4 = \overline{X} \text{ with } X = \left\{ \frac{a_1}{a_{t1}}, \frac{a_2}{a_{t1}}, \frac{a_3}{a_{t1}}, \frac{a_4}{a_{t2}} \right\} \quad (4)$$

5) Metric: Internet utilization rate of MBAN.

Objective: Baseline creation for helping the detection of: traffic, abusive use and outliers.

Data source: Traffic and bandwidth analysis tool and auditing in the network management.

Frequency: monthly.

Metric classification: Network structure and Services.

Measures: a_{t1} = Internet access bandwidth size, a_{t2} = number of desktops that access Internet, a_1 = Internet access average bandwidth and a_2 = number of desktops that access Internet through external links to the MBAN.

Formula:

$$F_5 = \left(1 - \overline{Y}\right) \text{ with } Y = \left\{ \frac{a_1}{a_{t1}}, \frac{a_2}{a_{t2}} \right\} \quad (5)$$

4 CASE STUDY: MBAN OF PEDREIRA

The MBAN of Pedreira is a project that has being developed by the University of Campinas (UNICAMP) and by the government of the city of Pedreira. The project started in 2005 and officially launched in 2007. The network infrastructure is constituted by an optical backbone and wireless access points, assembled in the form of wireless microcells. The current available services running over the MBAN are: Internet distribution, VoIP, E-mail and City surveillance.

The application of the security metrics presented in section 3.2 to the MBAN of Pedreira was executed in the period between January and April of 2008. Table 1 summarizes some results, such as components and formula of each metric.

In metric 1, all the buildings have logical access control between the connections (access lists).

However, the WEP protocol is used by the eight buildings with secure connections.

Table 1: Components and Formula.

Metric	Components	Formula
1)	a_t=18; a_1=18; a_2=8	$F_1 = 0.7222$
2)	a_t = 116; a_1 = 111	$F_2 = 0.0431$
3)	a_t=18; a_1=18; a_2 = 0	$F_3 = 0.5$
4)	a_{t1} = 3; a_{t2} = 768 hours; a_1 = 0; a_2 = 3; a_3 = 2; a_4 = 767 hours and 34 minutes.	F_4 = 0.66652
5)	a_{t1}=8 mbits/s; a_{t2}=214; a_1=0.87844; a_2 = 6	F_5 = 0.93107

The low indicator of metric 2 shows that there is not a defined policy for users creation in Pedreira's network. In metric 3, no default password was found, but all APs use WEP.

In metric 4, the final result was affected by the lack of redundancy component. The metric 5 result reveals that the use of Internet was not abusive because, on the average only 0.1098% of download bandwidth and 0.06915% of upload bandwidth is in use.

The proposed security controls from the results of security metrics application are: design of a test suite for the switches access lists, cryptography implementation in the connections, deployment of a Domain Controller, to change WEP by WPA, passwords auditing in the APs, RAID implementation for data redundancy and Heartbeat (Hearbeat, 2007) for services.

5 CONCLUSIONS

The successful deployment of MBANs it depends on the reliability of the systems that constitute them. Warranty of this reliability can be obtained through well formed criteria of information security. The security metrics are tools that can accomplish such objectives when properly developed and applied.

The metrics applications presented in this work allow the visualization of security critical areas on the MBAN of Pedreira. Security controls were proposed, following the obtained results for this network. It is important to note that for a complete network analysis, a larger set of security metrics must be developed and implemented.

Future work includes the development of new security metrics for MBANs using the template proposed here. Another topic is the development of a framework for data analysis in security metrics.

ACKNOWLEDGEMENTS

The work presented here has been developed under the umbrella of the projects "Municipal Infovia – An Open Access Network for Cities" and "SIGM – An Integrated e-Gov Environment for Cities". These projects have been supported in part by the governments of the cities of São José do Rio Preto, Pedreira, Penápolis, and Campinas, São Paulo State, Brazil.

Bruno Bogaz Zarpelão's work is supported by the State of São Paulo Research Foundation (FAPESP).

REFERENCES

AirSnort. 2004. [online] [Accessed 15th April 2008] Available from World Wide Web <http://airsnort.shmoo.com/>

Alexiou, A., Bouras, C., Primpas, D., 2006. Design Aspects of open municipal broadband networks. *In Access Nets '06, Proceedings of the 1st international conference on Access networks*. ACM Press.

Box, G., Hunter, W., Hunter, J., 1978. *Statistcs for Experimenters*. Wiley Series in Probability and Mathematical Statistics.

CERT. (Unpublished, 2006). *Potential Vulnerabilities in Municipal Communications Network.* Report dated May 2006.

Ford, G., Koutsky, T., 2005. *Broadband and economic development: a municipal case study from Florida.* Review of Urban & Regional Development Studies.

HeartBeat. 2008. [online] [Accessed 15th April 2008] Available from World Wide Web http://www.linux-ha.org/Heartbeat

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

Network Management Suite. 2008. [online] [Accessed 5th April 2008] Available from World Wide Web: <http://www.mishelpers.com/network_management/>

Patriciu, V., Priescu, I., Nicolaescu, S., 2006. *Security metrics for enterprise information systems*. Journal of Applied Quantitative Methods.

Payne, S., 2006. A Guide to Security Metrics. *SANS Security Essentials Version 1.2e.*

Swanson, M., Bartol N., Sabato, J., Hash., J. Graffo, L., 2003. *Security Metrics Guide for Information Technology Systems.* NIST Special Publication 800-5.

Weiss, S., Weissmann, O., Dressler, F., 2005. A Comprehensive and Comparative Metric for Information Security. In *ICTSM2005, Proceedings of IFIP International Conference on Telecommunication Systems, Modeling and Analysis*