

# Adaptive Security Metrics for Computer Systems

Gregory L. Vert Satish Baddelpeli  
Computer Science and Engineering Department  
University of Nevada  
Reno NV, US  
gvert@cs.unr.edu

**Abstract—** The major concern for a computer system is its security and integrity. It is necessary to check the security level of your system and keep it updated. This can be best achieved by using a metric system. At present, there is no standard metric to measure the integrity and security of a computer system. Defining a standard metric that suits all the systems is difficult, considering the fact that every system is built according to the functions it is used for. The Computer systems are used for millions of different functions. In this work we develop an adaptive metric system for measuring security and integrity level of a computer system. To define the metric system we have used a matrix called Security Matrix. We call this matrix adaptive because users can introduce or delete columns in the matrix according to their requirements. The idea behind this is to allow the user to have a metric system that suits his or her system best. Each dimension in the matrix represents one influential factor of the system security and integrity. The factors can vary from the software used in the system to the mediums of attack on the system. In this thesis we refer the system for a single computer or multiple computers connected in a network infrastructure using routers and switches.

**Keywords:** Security Matrix, Penetration Testing, and Security Threats

## I. INTRODUCTION

Computers are the integral part of modern society. Intrusion of computers is seen in all the fields. Computers have become, by far the most preferable way to store and manipulate data. Due to this reason, maintaining security and privacy of data finds an important place in system administrator's priority list. However, with the availability of simple and numerous hacking tools over the World Wide Web, it has become more difficult to stop the hackers. In fact, there is seldom a place or time when any network can be considered completely secure [1]. When trying to improve security care should be taken because increasing security can sometimes degrade the performance or functionality of the network. The balance between required security and the functionality has to be carefully found. For a server used for commercial purposes it is even more critical to find a correct balance. The ability to conduct business for any organization increases with an increase in functionality, but a lack of security can put an organization out of business. Therefore the balance between the functionality

and security needs to be carefully considered. It is critical to reduce the security risk while protecting the functionality [1].

The security of a computer system can be affected in many ways. Therefore the measure of the security of a system needs to be based a metric that represents the wide range of variables found in a system that can affect security. Currently there has been little work done in ways to quantitatively measure security of a system. By developing a quantitative measure of a system, one can use the results to compare with previous measurements and determine whether there is decrease or increase in security. Such a metric can be based on tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data [2].

There are some defined metric systems to measure the security of a system. However they are typically built to suit a particular system. Because of this, there is a need to create metrics that are portable adaptable to any particular type of system In order to develop a portable metrics our research has developed the following general guidelines based on a consensus from several sources [cites]

- define goals and objectives for system security through policy
- decide what objects of the system are to be measured. (Ex: programs, Departments etc.)
- develop methods to collect data and to analyze it.
- determine the method to report the results.
- develop actions based on collected information.

Since the objects found in a computer system differ from one system to another it can be difficult to develop a standard metric system that suits all the computer systems. Because of this, it is easier to create meta descriptions of system objects via equations.

In this our initial research we have developed and present a mathematically based model for evaluating the security metrics of a computer system. This is referred to as an adaptive security metric method. In this method we develop a security matrix where factors affecting the security of a system are stored in columns and systems that are being tested as rows. This matrix model allows security managers to select

their own factors for a security matrix thus tailoring security evaluation to the unique factors found in their own systems. This method can also be used to compare various factors of two or more systems. It can also be used to study the reasons for vulnerabilities and risks of the system.

## II. SECURITY MATRIX

For this research we designed an adaptive metric for security level of a computer. The metric is adaptive in the sense that users of the technique select and tailor the evaluation of the metric to their own systems. For example, users can add or delete rows or columns in the matrix depending on the kind of data he wants to collect and the components of his system to be measure. This can be done by determining the factors that affect the system and using them as the components of the matrix can do this. This helps a great deal in determining the security of a system a little more precisely. The main reason behind this is the fact that all the computer systems are not identical. A security threat for one system need not be a security threat for the other. This matrix can also be adopted in decision-making process. For example Table 1 shows a model of a security matrix. This matrix can be used to measure the security of a system with different operating systems.

The matrix in table 1 has factors as columns and systems as rows. Data for this matrix is collected in several different ways. One method of data collection is by physical inspection of the system. The second method is by penetration testing. By assessing the data collected from both methods, weights are assigned to each column in the security matrix. Using these weights the security factor of a system can be calculated from the equation we developed to measure security of a system given as:

$$SF = (\sum W) / NF \quad (1)$$

where:

SF - security factor

W - represents weight of factors in columns

NF - is number of factors utilized in calculation

There were two stages in the design of our method. The first of these was is developing the concept of the matrix called the Security Matrix. The second one is determining the weights for values to be included in the matrix. The security matrix was developed using the factors that can affect the security and integrity of a system. These factors were compiled from a background research on a multitude of authors [cites]. The first column of the matrix contains the names of the systems under testing. The last column is the Security Factor (SF) of the respective system. SF is the overall metric by which we measure and compare the security systems. The larger the value of SF the more secure the system is thought to be. The

rest of the columns in the matrix represents various factors affecting the security of system and utilized in the calculation of SF.

Factors in the matrix can be added or deleted according to user's requirements. Changes to matrix are carried out depending on what factors the user wants to use to measure the security of his system. Relevant factors can vary from system to system depending on various such as consideration as the function of a system and the nature and state of the system. For example a public system set up just to provide internet access to the general public may not to use encryption. Whereas a system found in a corporate office probably needs to have an encryption process in place to protect sensitive business information. To measure security of a public system we can eliminate encryption factor from the matrix but we need to weigh the encryption factor for a corporate system.

Table1: Sample Security Matrix

O.S. / Factors	Type of Network	Physical Security	Open ports	Bios Security	Security factor
Win 1	$W_n$	$W_{ps}$	$W_p$	$W_b$	SF of Win1
Win2	$W_n$	$W_{ps}$	$W_p$	$W_b$	SF of Win2
Unix1	$W_n$	$W_{ps}$	$W_p$	$W_b$	SF of Unix1
Unix2	$W_n$	$W_{ps}$	$W_p$	$W_b$	SF of Unix2

### Algoritim

The process of developing and measuring security of a system can be described with the following algorithm which represents the guidelines presented earlier.

- Step 1:** Define the system to be measured
- Step 2:** Determine the factors to be measured
- Step 3:** Select the tools to be used to test the system
- Step 4:** Data collection
- Step 5:** Data Analysis
- Step 6:** Compare the two systems
- Step 7:** Generate the report for the results.

Figure 1 illustrates the various steps involved in forming the matrix and calculating the weights to measure the security of the system.

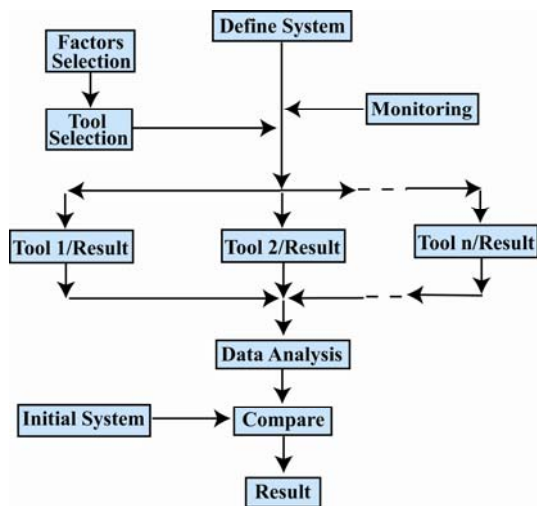


Figure 1 Algorithm for security metric development

The general parts of Figure 1 are described as:

#### *Define the system to be measured*

In this step we define the system we want to measure. We define the specifications, requirements and functions of the system. We examine purposes the system is used for and what kind of users are working on the system e.g. employees, students. This information is useful in forming security matrix. For example it can suggest what level of tolerance should be shown towards security violation of the system. This information also helps in deciding what kind of processes or tools need to be used in determining weights of factors in the matrix utilized for the calculation of SF.

#### *Determine the factors to be measures*

In this step we determine what factors are to be used to measure the security of the system. This is a very important step in measuring the security of a system. Care should be taken to list all the factors that can affect the system or part of system you are trying to measure. In this step we actually decide what factors have to be considered in measuring the security of the system. For this we use the information gathered from first step. Depending on what we want to measure, we list all measurable factors that affect that system. By measurable we mean the factors that can be quantitatively determined by security managers or security tools. The more factors we have the more precisely security of a system can be measured.

#### *Selection of tools*

After developing list of measurable factors we need to select tools that can give complete information about the

factors selected in the previous steps. Listing all measurable factors does not help in measuring a system's security unless we have tools that can gather complete information about those factors. There are some factors that should to be considered in selection of a tool:

- ease to use
- ease of automation
- correctness and accuracy
- amount of reporting information

For this research we felt that the foremost thing to be considered while selecting a tool is its preciseness and accuracy. One should check whether the results produced by that tool are dependable, precise and correct or not. There are many tools available in the market that have very good algorithms and technology but are very poor in reporting. An ideal tool is the one that is precise, simple to use, has automated processes and has good reporting technology.

#### *Data collection*

This is the process where we actually collect data using the tools selected in previous step. The collected data should represent the system's current state. This is where the reporting capabilities of tools will become very important.

#### *Data analysis*

This is the phase where we analyze the data collected in previous step. This data is used to calculate the weights of various factors for the matrix presented in the following sections. From these weights the SF is calculated. The SF gives a quantitative measure of system's security relative to other systems..

#### *System comparison and report generation*

This step is carried out only if more than one system is being evaluated. If this is the case we compare weights and other quantitative data derived from previous steps to conclude the security state of each system and how each system is better or worse from others. The results from this step can be very useful for decision making in terms of determining trust relationships among computers and information sharing. Finally reports are generated based on what has been found. These reports typically are textual and tabular but in future research we would like to examine how to visualize the SF data.

## II COMPONENTS OF MATRIX

The mathematical components of security matrix depend on the system specific information and can be different from one system to another. In this section we define the key factors in the generation of the SF metric. Multiple factors can contribute to a security metric. We selected factors based on the general subsystems found in a typical computer system. The categories include network, physical security, software patches and auditing.

### Type of Network

the type and use of the network connected to a system can affect its security; lots of security factors depend on this category. For example an unmonitored network is more risky than a monitored network. In an unmonitored network you cannot study the trend of users or cannot track their activities. Prevention of malicious activities is more difficult in an unmonitored network. The weight for the network security category is calculated from

$$W_n = (NV + UT + NM + NP) / 4 \quad (5.1)$$

where:

$W_n$  - weight for type of network

NV - variety of network {0 for public; 1 for private}

UT - training for users

NM - network monitoring {1 if true; 0 if false}

NP - network protection {1 if true; 0 if false}

In the above a public network is open for general public to use. It is difficult to monitor and secure a public system. A public network has a large number and variety of users with different skill levels. Due to the large number of users a public network can be hard to monitor. In contrast a private network often has fewer users and thus can be managed better than public networks. We assign Boolean values for variety of network. A system belonging to public network gets a value of 0 where as system in a private network gets a value of 1. Training of users is another important factor in network security therefore we include it as a term in the network weighting factor. We calculate the value for trained users as:

$$UT = (U - U_{ut}) / U \quad (5.2)$$

$U_{ut}$  - number of untrained users

$U$  - number of total users

Systems with more trained users has a higher value from the above equation. System with more untrained users has lower value.

Another part of this  $W_n$  factor is the network protection (NP). We assign values for this depending on what kind of protection they is utilized. The most commonly used protection techniques for a network are firewall, intrusion detection, intrusion prevention, and antivirus. We assign a value of 0.25 each for above mentioned methods. NP gets a value of 1 if all four methods are used. If they use only two of them then they will get only 0.5.

### Physical security

This is one of the most neglected areas in a system's security. Without first implementing physical security, all other security measures may be meaningless [3]. Perimeter security is very important. Care should be taken that no unauthorized person

can get in to facility with out anybody's knowledge. Included in this category is perimeter security, protection from fire hazards, and protection from water hazards.

Physical or perimeter security includes such considerations as users locking their computers and keeping access to servers and wiring closets to a limited number of persons. The logic is that if a company invests thousands of dollars to implement Intrusion Detections Systems (IDS) and does not restrict the physical access to the server then, resources spent on IDS are ineffective. The physical security factor for the SF is calculated as:

$$W_{ps} = (P_p + F_p + S_p + T_p + E_p) / 5 \quad (5.3)$$

where:

$W_{ps}$  - weight for physical security

$P_p$  - perimeter Security

$F_p$  - protection from fire

$S_p$  - protection from sprinklers and water leaks

$T_p$  - protection from temperature

$E_p$  - protection from electrical hazards e.g. surge

When these issues are addressed in a computer system we calculated the  $W_{ps}$  by assigning each factor a weight of 0.2. For example if all the factors are addressed; we calculate 1 as the corresponding weight. If only two of them are addressed properly we assign 0.4.

### Software and Security Patches

This is one of the simple and most effective factors that can influence the security of a system. It is very important to keep a system up-to-date. Unfortunately there are very few products that have no new vulnerabilities discovered after their release. In practice these patches are released after the vulnerability is found out in a real time environment. Hackers try to exploit these vulnerabilities before they are patched [4]. If there is a patch released then probability that a product can be exploited can be high. If one machine in a system is infected, the time taken for all the machines get infected can be as little as a few minutes. To avoid this, systems should be patched in a timely manner. To calculate weight of software security patch factor we use:

$$W_{sp} = (P_a - P_{ti}) / P_a \quad (5.6)$$

where:

$W_{sp}$  - Weight for Security patches

$P_a$  - patches available

$P_{ti}$  -Patches to be installed

Here we assign weight for security patches ( $W_{sp}$ ) by using number of patches available and number of patches installed. The more number of patches installed from what is available, the higher this weight will be.

### Auditing and Log Files

Log files are very important for achieving system security. The more comprehensive auditing is the more effectively systems can be monitored for security. The combination of log files and monitoring tools help you get an exact picture of your network [6]. Log files should be set up to log all the activities taking place in that system. For a given system there will be multiple log files needed. Each network device and system has its own log files. All these log files should be studied and all the issues recorded in these log files should be addressed. By studying these log files one can determine any unwanted or unauthorized activities taking place in a system.

Many critical systems come with the logging turned on by default, but some have logging turned off by default. Some times logging all the activity can lead to network slowdown. In this case it is better to avoid logging unwanted devices and services. Logging when paired up with network monitoring tools can form a good tool to fight with factors affecting system security. We calculate weight of this factor from

$$W_1 = LU / LP \quad (5.8)$$

where:

$W_1$  - weight for log files

LU - number of log files activated

LP - number of log files possible to be activated

We calculate weight using logs used against number of logs that can be used in a system.

### Security Factor (SF)

Equation (5.21) is the final equation to calculate Security factor (SF). This equation is derived by previous weighting factors into the equation and is given as:

$$SF = (((NV + ((U - U_{ur}) / U) + NM + NP) / 4) + (1 - (((0.75P_l) + (0.25P_{nl}) + (P_{nr}) + (0.5P_{nrl})) / P_o))) + (LU / LP)) / NF \quad (5.21)$$

where:

NF - number of factors

The values of all the factors should be in the range [0, 1]. This leads to the possible values of SF being in the range [0, 1]. The system with a SF value 0 is considered to be a less secured system, whereas system with SF value of 1 is more secured system. The success of a realistic calculation of SF can depend greatly on how well the method presented early, factors, tools, techniques of data collection and analysis are chosen and executed.

### III. RESULTS AND DISCUSSIONS

This initial work has started the development of a model that can be useful in administering, comparing and securing computers in a diverse system. Among some of the benefits of this approach are:

- because of its adaptive nature, users can manipulate list of factors to choose only those factors against which they want to test their system.
- this approach can be used to measure the security of a system quantitatively, which helps in studying security of a system more effectively than a qualitative measurement.
- the approach can be also used to compare the security of various systems with in an organization or between different organizations.
- the method is useful in decision making between software, hardware or methods of system setup.
- it can be used to study and evaluate resources for system's security with in a system.

To date, we have tested a small trail run of our method on different computers used for different needs and by various users. We selected three systems with Windows XP operating system. We named these systems as Win1, Win2, and Win3. Each belongs to a different user group. First PC is of a home user (Win1), second is a public PC used by general public (Win2) and third PC is of a system administrator (Win3). In general the equations appear to rank the computers according to what one would expect their SF factors should be. However, it is clear that much more work needs to be done to develop the SF matrix and factors that should be included in it.

### REFERENCES

- [1] Eric.C, and Jeff.R, Hackers Beware: The ultimate guide to network security, Pearson Education, 2001.
- [2] netsec website, Using metrics to improve security, accessed April 20, 2005 at [http://www1.netsec.net/content/securitybrief/archive/2004-09\\_Metrics.pdf](http://www1.netsec.net/content/securitybrief/archive/2004-09_Metrics.pdf)
- [3] Bob Pagoria - Implementing Robust Physical Security A Lord of the ring, SANS Infosec Reading Room, july 2004
- [4] Sans website, SANS Top 20 Vulnerabilities – The Experts Consensus, accessed Jan 25, 2005 at <http://www.sans.org/top20/>
- [5] foundstone website, Information Security Metrics, accessed April 15, 2005 at <http://www.foundstone.com/resources/whitepapers/>

wp\_securitymetrics.pdf

[6] Seham Mohamed GadAllah, The Importance of Logging and Traffic Monitoring for Information Security, SANS reading room, December, 2003.

[7] Canavan, J. *Fundamentals of Network Security* .Artech House Publishers, 2001

[8] Tricia Olsson , Strengthening Authentication with Biometric Technology, SANS Infosec Reading Room, August 2003.

[9] Lon D. Gowen, The MITRE Corporation - Predicting Staffing Sizes for Maintaining Computer-Networking Infrastructures, The MITRE Corporation, September 2005.

[10] Microsoft website, Create a Chart, accessed November 15, 2005 at <http://office.microsoft.com/en-us/assistance/HP051994911033.aspx>