International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 2 Issue 1 January 2012

A METRIC MODEL FOR RANKING THE SECURITY STRENGTH OF A WEB PAGE

G. E. Okereke[*1], Prof. C. C. Osuagwu[2]*

*[*1] Computer Science Department, University of Nigeria, Nsukka*

george.okereke@unn.edu.ng[1]

okerekegeorge2000@yahoo.com[1]

[2] Department of Electronic Engineering, University of Nigeria, Nsukka

Abstract

It is common knowledge that any system or process that cannot be measured cannot be managed. This wisdom also applies to security as well. As much as the expansion of use of Information Technology (IT) in various processes is increasing, the question of security readily comes to mind often. Today we see various new ICT products and applications appearing in the market daily via web sites. Again, cases of Web security breaching are also on the increase since the Internet is accessible from any where. We see reports in the national dailies about the terms like hacking or other security breaching very common words. The concept of Computer Security in general is being heavily researched and this perfectly makes sense in a world where e-commerce and e-governance are becoming the standard. Security metrics are assuming tremendous importance as they are vital for assessing the current security status, to develop operational best practices and for guiding future security research. Security metrics is especially very important nowadays when organizations and enterprises are coming under increasing compliance pressure requiring them to demonstrate due diligence when protecting their data assets, products, services and their customers. In these circumstances metrics can enlighten organizations and enterprises to prioritize threats and vulnerabilities and the level of risks they pose to *enterprise information assets. Unfortunately, security metrics till date is taken as a qualitative measure. This paper surveys the various security metrics proposed in literature for information security and systems and develops a metric model for ranking the security status of a web page which is a common platform for modern business transactions in the globalized world.*

***Keywords**: computer security, security metrics, threats, vulnerabilities, security strength and ranking.*

1. **Introduction**

There are several methods of probing defences for weaknesses in security of a system. Popular ones include red teaming exercises, penetration testing, vulnerability scoring, e.t.c. which are currently being used for evaluating IT systems and network security. These strategies are inadequate in the present scenario considering the higher frequency these new vulnerabilities are discovered. Practice has shown that a set of good metrics would help organizations to determine the status of its IT security performance and to enhance it by minimizing the windows of exposure to the new vulnerabilities. Metrics monitor the effectiveness of goals and objectives established for IT security. They can measure the implementation of a security policy, the results of security services and the impact of security events on an enterprise's mission. IT security metrics can be collected at various levels and detailed metrics can be aggregated and rolled up to progressively higher levels depending on the size and complexity of the organization. It becomes essential to highlight the important difference between metrics and measurements. Measurements are instantaneous snap shots of particular measurable parameters, whereas metrics are more complete pictures, and typically comprised of several measurements, baselines and other supporting information that provide the context for interpreting the measurements. Metrics is usually discussed with respect to time.

2. **Related Work and Existing Methodologies**

Security measurement using metrics has attracted great interest in recent years with the help of guidelines, practices and standards accepted world wide and with the efforts of international organizations. Code of practices like BS7799, ISO17799,[1,2] NIST SP800-33 provide a good starting point for organizations in this context.[3] In 2004, Security Metrics Consortium (SECMET) was founded to define quantitative security risk metrics for industry, corporate and vendor adoption by top corporate security officers of the sector. The Metrics work group of International Systems Security Engineering Association (ISSEA) has lead another standardization effort in this area. This group develops metrics for System Security Engineering – Capability Maturity Model (SSE-CMM). One model used widely for conveying the vulnerability severity is the Common Vulnerability Scoring System (CVSS). This provides the end user with an overall composite score representing the severity and risk of a vulnerability. Score is derived from metrics and formulas. The metrics are in three distinct categories that can be quantitatively or qualitatively measured. Base metrics contain qualities that are intrinsic to any given vulnerability that do not change over time or in different environments. Temporal metrics contain vulnerability characteristics which evolve over the lifetime of vulnerability. Environmental metrics contain those vulnerability characteristics which are tied to an implementation in a specific user’s environment. The particular constituent metrics used in CVSS were identified as the best compromise between completeness, ease-of-use and accuracy. They represent the cumulative experience of the model’s authors as well as extensive testing of real-world vulnerabilities in end-user environments. There are seven base metrics that represent the most fundamental features of vulnerability. The environmental score (ES) is considered as the final score and used by organizations to prioritize responses within their own environments. CVSS differs from other scoring systems (e.g. Microsoft Threat Scoring System, Symantec Threat Scoring System, CERT Vulnerability Scoring or SANS Critical Vulnerability Analysis Scale Ratings) by offering an open framework that can be used to rank vulnerabilities in a consistent fashion while at the same time allowing for personalization within each user environment. As CVSS matures, these metrics may expand or adjust making it even more accurate, flexible and representative of modern vulnerabilities and their risks.

3. **Security Metrics**

The term security metrics is used often today, but with a range of meanings and interpretations. Metrics are tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. The purpose of measuring performance is to monitor the status of measured activities and facilitate improvement in those activities by applying corrective actions, based on observed measurements. While a case can be made for using different terms for more detailed and aggregated items, such as 'metrics' and 'measures,' this paper uses these terms interchangeably."[4, 5] "Measurements provide single-point-in-time views of specific, discrete factors, while metrics are derived by comparing to a predetermined baseline two or more measurements taken over time. Measurements are generated by counting; metrics are generated from analysis. In other words, measurements are objective raw data and metrics are either objective or subjective human interpretations of those data." [6] For information system security, the measures are concerned with aspects of the system that contribute to its security. That is, security metrics involve the application of a method of measurement to one or more entities of a system that possess an assessable security property to obtain a measured value.

The business logic associated with a metric follows a simple processing pattern: [5]

- Create: Obtain primary input data from one or more authoritative providers, including commercial products or home grown customer applications.
- Calculate: Apply a series of analytic operations (called actions) on the primary data to derive a result and store the result in the metric results database in the form of one or more rows in a table.
- Communicate: Communicate the metric results in any of the following formats: default visualization, email notification, email alert based upon detection of some policy violation.

4. **Basic indicator for security**

As described, none of the approaches above allows assessing the overall organization's information security. The most important problem seems to be the lack of an appropriate basic indicator allowing security expression of an entire organization.

A good starting point for this basic indicator seems to be the intuitive understanding of security. According to this, total security is reached if nothing is lost (over a long period of time). Moreover, an organization is regarded more secure than another if it possesses the same set of assets but lost less than a competitor. It is also regarded to be more secure if it possesses more assets but has lost the same.

Incorporating these aspects into one single formula, the indicator S for security of an organization can be calculated by

S = 100% - [percentage of lost assets] [7] (i)

This basic indicator is time-dependent. This means that it will be different if different time periods are analyzed. One year seems to be an appropriate period of time for security evaluations, but generally every other value may be taken from the concept level. As the term "percentage of lost assets" and the example given above suggest, the basic indicator is based on incidents. Thus, the losses of incidents are counted and summarized. It must be mentioned that S might possibly be negative. However, this indicates that more than assets available are expected to be lost during the given period of time. This is theoretically possible as assets can be repaired. However, it is probably unbearable for an organization, thus in reality it is rather unrealistic to occur.

Another way to look at metrics measurement is with respect to two parameters: one a parameter and second how much impact does this parameter have on the security. Since security is not just dependent on any one parameter, so we first have to decide on different parameters. These parameters may be fixed by an organization or may differ as per the project. Once the parameters have been identified the next task is to find ways to measure them. In other words, we have to map the qualitative parameters to some quantitative parameters, which can be used to calculate the security metrics. Thus we try and identify the measurable potential weak spots for the parameter. Depending on the project, these potential weak spots may be a continuous function dependent on some variable or it may simply be a discrete value, which can be measured, based on some criteria. Secondly the impact of every parameter will vary as per the project, so we need to assign some weighted value or impact factor to the parameter. Based on this a standard security metrics would be:

$$SM = \sum_{i=1} W_i X_i \quad [8] \qquad \text{(ii)}$$

Where
SM = Security Metrics
n = Number of parameters
W = Weight value or impact value
X = Measurable potential weak spots for a parameter

All research work done in this field moves around this metrics. The basic difference lies in which scenario the metrics is working. Based on the project what may differ is, the parameters of security, the weighted values and the method of calculating it. Whatever the case may be but the end result is that security metrics is nothing but the weighted sum of the number of potential weak spots identified within a project. An attempt has been made to map equation (ii) to the security of a web page which is a common platform for modern business transactions.

5. **Elements of a Web Page**

A web page, as an information set, can contain numerous types of information, which is able to be seen, heard or interact with by the end user: [www.en.wikipedia.org/wiki/web-page]

Perceived (rendered) information:

- Textual information: with diverse render variations.
- Non-textual information:
    - Static images may be raster graphics, typically GIF (graphics interchange format), JPEG (Joint Photographic Experts Group)

    or PNG (portable network graphics); or vector formats such as SVG (scalable vector graphics) or Flash - a multimedia platform used to add animation, video, and interactivity to web pages.

    - Animated images typically Animated GIF and SVG, but also may be Flash, Shockwave (a multimedia platform used to add animation and interactivity to web pages), or Java applet (a small application delivered to the users in the form of Java bytecode (Java bytecode is the form of instructions that the Java virtual machine executes).
    - Audio, typically MP3 (a common audio format for consumer audio storage).
    - Video, WMV (Windows), RM (Real Media), FLV (Flash Video), MPG, MOV (QuickTime)
- Interactive information:
    - For "on page" interaction:
        - Interactive text:
        - Interactive illustrations: ranging from "click to play" images to games, typically using script orchestration, Flash, Java applets, SVG, or Shockwave.
        - Buttons: forms providing alternative interface, typically for use with script orchestration.
    - For "between pages" interaction:
        - Hyperlinks: standard "change page" reactivity.
        - Forms: providing more interaction with the server and server-side databases.

Internal (hidden) information:

- Comments
- Linked Files through Hyperlink (Like DOC, XLS, PDF,etc).

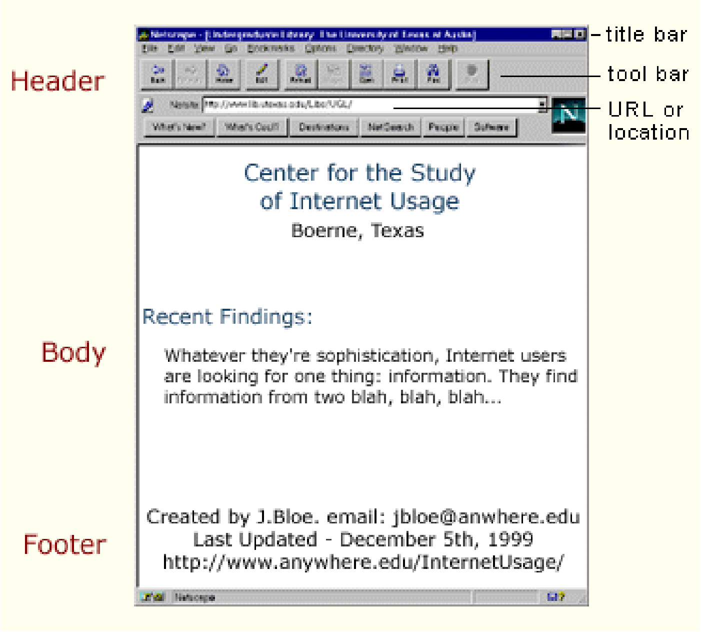
- Metadata with semantic meta-information, Charset information, Document Type Definition (DTD), etc.
- Diagramation and style information: information about rendered items (like image size attributes) and visual specifications, as Cascading Style Sheets (CSS).
- Scripts, usually JavaScript, complement interactivity and functionality.

The web page can also contain dynamically adapted information elements, dependent upon the rendering browser or end-user location (through the use of IP address tracking and/or "cookie" information).

From a more general/wide point of view, some information (grouped) elements, like a navigation bar, are uniform for all website pages, like a standard. These kind of "website standard information" are supplied by technologies like web template systems.

5.1 **Parts of a Web Page**

Figure 1 shows a typical web page and the various parts. Header is the top part of a Web document. The title of the page and the URL are usually found there. Title bar contains the title that the Web designer named the web page. Toolbar is where the buttons to navigate the Web are found. URL or Location is where the Web address for the page under view is found. This information is vital if one plans to cite Web documents in papers. Body is where the text or content of a Web page is found. Footer contains information about the page author or the sponsor. The last time the page was updated can be found in the footer.



Center for the Study
of Internet Usage
Boerne, Texas

Recent Findings:

Whatever they're sophistication, Internet users are looking for one thing: information. They find information from two blah, blah, blah...

Created by J.Bloe. email: jbloe@anwhere.edu
Last Updated - December 5th, 1999
http://www.anywhere.edu/InternetUsage/

Figure 1: parts of a web page

5.2 **Basic Web Page Layout**

Every web page create has four basic elements : the HTML Tags, the Head Tags, the Title Tags, and the Body Tags.

An example is shown below:

```
<html>
<head>
<title>This is My First Web Site</title>
</head>
<body>
This is my first web site.  I hope you enjoy the fun of it!
</body>
</html>
```

5.2.1 **The HTML Tags**

The <html> and </html> tags wrapped around the text shows that this is an HTML document. They signify the start of the web page and the end of the web page.

5.2.2 The Head Tags

The <head> and </head> tags wrapped around the title tags inform the web browser where it can get specific information about this page, and how it is displayed. The head tags must be at the top of the page, after the first HTML tag.

5.2.3 The Title Tag

The <title> and </title> tags tells the browser that what is in between here is the title for the web page. It is usually shown (in most browser) at the top of the menu and on the tab one is browsing from.

5.2.4 The Body Tags

The <body> and </body> tags wrapped around the text signifies the "body" of the web page, where the content are displayed in the browser.

Noticed that these tags come in pair. One of these tags is used to start the command to the web browser, and the other is used to end or close it. For example, the <title> tag, tells the web browser, "Hey, this is the web page's title here, pay attention!". The </title> tag tells the browser that we are done with the title.

Each web page is made up of four primary parts.

- The HTML tags which shows where the web page starts and ends.
- The head tags are used to display important information about the web page, that will not be seen by the end user.
- The title tags are used to tell the browser the title of the page.
- The body tags tell the web browser where the web page's content starts and ends.
- A tag started must be closed or ended.

6. Measurable Parameters of a Web page

Any web application contains the following vulnerabilities: [9]

- Cross-Site Scripting
- SQL Injection/ Blind SQL Injection
- File Inclusion
- Cookies poisoning

- Sessions Management problems
- Weak hash function
- Cross-Site Request Forgeries

A web application scanner looks for two major types of security problems in a web page - vulnerabilities and architectural weaknesses. The following list of problems to test was mostly extracted from the Web Application Security Consortium's Threat Classification version 2.0. [www.webappsec.org]. They include: Authentication, Authorization, Client-side Attacks, Command Execution, Information and Disclosure. The details of the examples of the various types of vulnerabilities and architectural weaknesses can be seen in the web site above.

No metrics test suite can handle all the possible vulnerabilities and architectural weaknesses in a modern and technology rich website as listed in [www.webappsec.org]. The choice of which ones to test depends on nature of the web application in consideration.

To apply equation (ii) to measure the strength of a web site, the evaluator decides the security parameters, vulnerabilities and architectural weaknesses to measure and the impact of each. The choice of higher impact for any security parameter, vulnerability or architectural weaknesses depends on the severity of the parameter and the number of them that are implemented in the web site.

8. **Web site Evaluation Model**

This evaluation model uses a common yardstick to measure and compare web sites [10]. Tables 1 and 2 show two evaluation models for measuring the security strength of three web sites. The measurable security parameters of each site are obtained from software which crawls through the sites to extract the security parameters and assign a specific value to each parameter. The first evaluation model (shown in table 1) simply lists the key security elements common to each of sites and scores them. The second evaluation model adds a weighted factor (impact factor). In this example, each evaluation parameter receives a rating based on its severity. Although the initial scores are the same in both models, notice that web site 1 has the highest total points in table 1, but web site 3 emerges as the most secured in the weighted model.

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 2 Issue 1 January 2012

Unweighted evaluation model for three web sites rates the sites on a scale from 1 (low) to 10 (high), and then adds the site's score to calculate total points.

	Web sites		
Security Parameters	**Site 1**	**Site 2**	**Site 3**
Authentication	6	5	9
Authorization	2	5	8
Client Side Attack	8	8	5
Command Execution	10	6	3
Total Points	**26**	**24**	**25**

Table 1: unweighted evaluation model for three web sites

Weighted evaluation model rates the same web sites on a scale from 1 (low) to 10 (high), then multiplies each site by the weighted (impact) factor and adds each site's score to get total points.

		Web sites		
Security Parameters	**weighted factor**	**Site 1**	**Site 2**	**Site 3**
Authentication	25	6*25=100	5*25=125	9*25=225
Authorization	25	2*25=50	5*25=125	8*25=200
Client Side Attack	35	8*35=280	8*35=280	5*35=175
Command Execution	15	10*15=150	6*15=90	3*15=45
Total Points	**100**	**630**	**620**	**645**

Table 1: Weighted evaluation model for three web sites

8. Result Interpretation

Tables 1 and 2 show security metrics parameters for three web sites to have the same initial ratings, but the two evaluation models produce different results. In the unweighted model, web site 1 has the highest total points and seems to be the most secured. However after applying weighted factors, web site 3 becomes the most secured.

9. Conclusion

Metrics can be an effective tool for security managers to discern the effectiveness of various components of their security programs, the security of a specific system, product or process, and the ability of staff or departments within an organization to address security issues for which they are responsible. Metrics can also help identify the level of risk in not taking a given action, and in that way provide guidance in prioritizing corrective actions. Additionally, they may be used to raise the level of security awareness within the organization. Finally, with knowledge gained through metrics, security managers can better answer hard questions from their executives and others, such as:

- Are we more secure today than we were last year?
- Are our competitors more secure than us in this regard?
- Are we secured enough to go online?

This way merchants engaging in e-business on the net can use this web page evaluation model to ascertain the status of their web site as well as compare their site with their competitors before engaging in business transaction on the Internet.

References

1. British Standard Institute (publisher). *Information Security Management. Specification for Information Security Management Systems (BS 7799-2).* British Standard Institute, London, 1999.
2. British Standard Institute (publisher). Information Security Management. Code of Practice for Information Security Management. (BS 7799-1). British Standard Institute, London, 1999.
3. Sree Ram Kumar, T, Alagarsamy K (2011). "A Stake Holder Based Model for Software Security Metrics*" International Journal of Computer Science issues*, Vol. 8, Issue 2, ISSN (Online): 1694-0814 www.IJCSI.org
4. Nielsen, Fran. "Approaches To Security Metrics." NIST and CSSPAB Workshop, Washington, D.C., 13-14 June 2000: 7. URL: http://csrc.nist.gov/csspab/june13- 15/metrics_report.pdf.
5. Deepti Juneja, Kavita Arora, Sonia Duggal (2011) "Developing Security Metrics for Information Security Measurement System", *International*

Journal of Enterprise Computing and Business Systems, ISSN (Online) : 2230-8849 http://www.ijecbs.com Vol. 1 Issue 2.

6. http://csrc.nist.gov/csspab/june13-15/Craft.pdf (10 July 2001)
7. Steffen Weiß, Oliver Weissmann, Falko Dressler (2006). "A Comprehensive and Comparative Metric for Information Security", Department of Computer Science, University of Erlangen, Germany.
8. Mukta Narang & Monica Mehrotra (2010). "Security Issue – A Metrics Perspective", *International Journal of Information Technology and Knowledge Management,* Volume 2, No. 2, pp. 567-571.
9. Elizabeth Fong, Romain Gaucher, Vadim Okun, Paul E. Black (2009). "Building a Test Suite for Web Application Scanners", *National Institute of Standards and Technology Gaithersburg, MD 20899-8970*
10. Gary B. Shelly, Thomas J. Cashman, Harry J Rosenblatt (2006). "System Analysis and Design", Thomson Course Technology, Boston MA.