Poster : Security Quotient - Defined

Naga Sushma Devarapalli
Student,Software Engineering
Santa Clara University
ndevarapalli@scu.edu

***Abstract*— The impact of the human element on the security of a system is undeniable. Until now the naïve users who are considered as the weakest link in security are perceived to be the sole human component. The other human elements that shape and affect the security in positive or negative direction are often viewed in isolation. The human elements range from the management who make the decisions to the designers, developers and testers of the system. As we identify Intelligence Quotient (IQ) and Emotional Quotient (EQ) to humans, we identify Security Quotient to the human elements involved in shaping the security of the system. The Security Quotient aggregated from these human elements is in direct relation to the security of the developed product.**

Keywords— Security Quotient; Security awareness; Users

I. INTRODUCTION

Humans are an integral part of a system. A system exists for humans, developed by humans, managed by humans and used by humans. The Microsoft SDL methodology [1] focuses on the secure software development practices and the dynamic capability maturity model [2] views the security from management dimension. In this paper, we view the different human elements involved in the system in coalition to understand their influence on the security of a system. The strength of this concept is that it is not restricted to cyber security but can be customized and extended to other areas as well.The human elements include users of the system, management who make crucial decisions in development and deployment of system, designers who shape the system, developers who code the system and testers who verify and assure the system. While academics describe and attribute individuals with IQ score and management with EQ score, so can security experts attribute Security Quotient(SQ) to the humans involved in a system. The aggregated Security quotient of the human elements is the Security Quotient of the entire system and is used as a measure for the security of a system as shown in Figure 1.

II. DESCRIPTION

The first human element in the system is the User. Historically, user is labeled as the weakest link in the security of a system. With the advent of technology, the user base has increased to mass markets, including naïve users to sophisticated users. This has further complicated the security increasing the users' position in the security of a system to a greater length. Though user education has been argued as a myth [3], the importance of users' impact on the security of a system has its own significance [4]. These research studies point out that through studying human-computer interaction, more can be understood about user's behavior and that user education is not a panacea. The security quotient of the user is the security awareness and the tools available to them to achieve their security goal.

$$SQ_{SYSTEM} = SQ_{USERS} + SQ_{MANAGEMENT} + SQ_{DESIGNERS} + SQ_{DEVELOPERS} + SQ_{TESTERS}$$

FIGURE 1 SECURITY QUOTIENT OF A SYSTEM

The Management who is responsible for taking the key decisions in shaping the security of a system is a core human component. The management needs to be conscious about the security of the products that are developed and the impact it has on the reputation of the organization. They have to acknowledge the importance of security and create a security aware organization through their security awareness programs [5]. Management has to make a continuous and consistent effort to "reach out" to all the employees in the organization. To achieve this, management has to objectively evaluate the current status of security in the organization and has to take necessary measures to move towards the organization's security goal [6]. The security quotient of the management is the security consciousness on their part and the efforts made to achieve it.

The next human component is the designers who make the key architectural decisions in the system. The programming languages and the operating environment chosen by these key players will impact the security of a system to a greater extent. There are studies which prove that usability is a key factor and that it needs to be considered deeply during the design phase [7,8]. The security quotient of the designers is the design considerations made by them to achieve better usability and better user interfaces which have a direct correlation on the security of a system.

The other human component that impacts the security of a system to a greater extent is the developers. The programming languages such as C and C++ have historically proven to have higher vulnerabilities like Stack Overflow and Heap Overflow. The web development has brought with it a higher chance of vulnerabilities in the form of Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF). With more and more API's being used for ease and portability, the need for security awareness has gone to the next dimension. Developers should use the available tools [9,10] to know about the secure coding practices which are independent of the programming languages. The security quotient of the developers is the awareness to the vulnerabilities that can exist and the secure coding practices to reduce the attack surface vectors.

Testers are our last human component in the security of the system. There has been more consideration of this phase than ever with the increasing threats and attacks to the systems. The highly needed assurance [11] for a system heavily relies on testers. Testers these days have more responsibility than other human components in exposing the vulnerabilities of the system. To achieve the desired results, testers have to be aware of the possible threats and the attack surfaces to perform their job efficiently. Penetration testing [11] has been a specialized area in the security aspect of a system and its automation has become a key concept. The security quotient of a tester is the exposure to possible threats and ability to locate the vulnerabilities in the system.

The human components in a system do not exist in solitude but rather depend on each other to a greater extent. The Usability plays a major role in designer's decisions, which in turn impacts developers and testers. The management decisions heavily influence the other human components – designers, developers, testers and in fact users. Considering the security quotient of each human element in a system, the security quotient of the entire system can be arrived at by aggregating the individual security quotients.

III. CONCLUSION

While the other methodologies and processes view the security from technical or management or user dimension, this concept presents an integrated view. The human components involved in using and shaping the system should not be viewed in isolation but rather in coalition. This consideration helps in measuring the security of the system from end to end right from its inception to its deployment and use. This paper highlights the key human players in the system and their individual security quotients which when aggregated provide the security quotient of the entire product.

REFERENCES

[1] http://www.microsoft.com/en-us/download/confirmation.aspx?id=12379

[2] Adler, Richard M. "A dynamic capability maturity model for improving cyber security." Technologies for Homeland Security (HST), 2013 IEEE International Conference on. IEEE, 2013.

[3] S. Gorling, "The Myth of User Education," in ¨ Virus Conference, Oct. 2006

[4] Adams, A., & Sasse, M.A. (1999). Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures. Communications of the ACM, 42, 41–46

[5] McCoy C, Thurmond Fowler R. 'You are the key to security': Establishing a Successful Security Awareness Program. SIGUCCS'04; 2004.

[6] Davis K. Saving Users From Themselves:Creating an Effective Student-Oriented Anti-VirusIntervention. SIGUCCS'01; 2001

[7] J.Nielsen,"Ten Usability Heuristics," 2005, http://www.useit.com/papers/heuristic/heuristic list.html.

[8] B. Shneiderman and C Plaisant "Designing the user interface:strategies for effective human-computer interaction" 5th ed

[9] R. Seacord, "Secure Coding Standards," in Proceedings of the Static Analysis Summit, NIST Special Publication 500-262, July 2006. Available: http://samate.nist.gov/docs/NIST_Special_Publication_500-262.pdf

[10] CERT, "Secure Coding," Software Engineering Institute: Carnegie Mellon. [Online]. Available: https://www.cert.org/secure-coding. [Accessed: February, 16, 2008].

[11] B. Snow, We need assurance!, Proc. 21st AnnualComputer Security Applications Conference, IEEEComputer Society, 2005

[12] Kolodgy, C. & Pintal, G. (2007, January). *White Paper: Automated Penetration Testing: Can IT Afford Not To?* Retrieved March 5, 2007, fromhttp://www.coresecurity.com/files/attachments/WP_IDC_Auto_Pen Test_0107.pdf