International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-3, Issue-5, May 2015

A Model for Cryptography in Information Security

Hayfaa Abdulzahra Atee

***Abstract*— No matter how well designed and implemented a security system is, the crucial factor is the trustworthiness and reliability of people handling a system. The fact that human factors play a crucial role in most accidents is a worrying feature of the "safety" factors in modern expertise. Appropriate technical solutions can be implemented but the human factor cannot yet be managed. Our research project aims to better understand the role of human factors in information security systems. We have developed a model system to explore the dynamic simulation of complex security problems. We use a mere fiction to illustrate how system dynamics can offer ideas on the "problems of the safety of persons" and assist in the robust case design of security policies. To move forward, collaborations with businesses or organizations are needed in order to gather the necessary studies.**

***Index Terms*— Safety, Instrumental Conditioning, Part of Cryptography.**

I. INTRODUCTION

The World Wide Web has experienced phenomenal growth in recent years. Individuals, businesses and governments have extensively used web applications that can provide efficient and reliable communication solutions to challenges, management and direction of trade in this century. However, these Web applications have many entry points that can endanger databases. Recently, the number of reported data breaches involving sensitive private information of government levels, organizations and companies have grown at an alarming rate. In some extreme cases, confidential information belonging to millions of people were revealed. For example, security providers of researchers discovered a server containing sensitive e-mails and Web data of thousands of people, including health information, credit card numbers and documents with needed security (containing information that involves both technology and people). Technological advancements are indeed impressive tools, but it is increasingly evident that the human factor is the Achilles heel of information security. In is interesting to note that, you can replace "organizational accident" to "security concerns"[1]. Human performance should be considered in an integrated work environment subtly shaped by technology and human behavior. Improved safety (and security) require improved understanding of evaluations: The dynamics of the problem, namely, the contagion effects linked by causal mechanisms is essential[2;3].

Improving our understanding of this dynamic way is the grounding for analysis of empirical studies, distillation behavior of them, and the development of models for putative causal structures, dynamic performance and validation of dynamic simulation of these models by comparing simulation of empirical behavior-based models.

Hayfaa Abdulzahra Atee, Foundation of Technical Education, Iraq

II. METHODOLOGY

The interaction of technology, work environment and human behavior in the security development is an essential system with feedbacks, the time evolution (nonlinear dynamics), delays, soft factors and interdisciplinary aspects. Obviously, the ultimate practical reason for studying these systems is to achieve the desired goals and to prevent unwanted performance. In other words, the safety systems must be managed. A discipline explicitly designed to manage systems are characterized by the prior factors mentioned (feedbacks, dynamics, delays, intangible factors, interdisciplinary aspects) are the dynamics of the system [3].

A basic principle of the system dynamics is that you should not model a "system" - but rather a problem: The specification problem - clearly defined in terms of time and structure, and is characterized by behavior patterns problem and the desired behavior, called "reference patterns of behavior" - used Occam's razor to cut the relevant aspects of the system, keeping only what is essential for the problem at hand. Believing that the system dynamic studies of safety systems provide useful additional information to information safety, we present a dynamic model of the system of which, a crucial aspect of the problem is the "people problem" - ie factors that determine compliance [4; 5]. Pertaining to 'security measures', our aim is to discuss the model itself and the policy proposed by the suggested model. The truth is preliminary - the dynamic system model is the treatment with respect to risk perceptions, and can serve as example of what can be done with the modest methodology (generic) empirical information, and as a sample for the organizations[6; 7]. They might be tempted to undertake a collaboration in identifying the behavior of reference methods for the integrated system dynamics modeling.

III. DYNAMICS COMPLIANCE

1.1. Factors Shaping Compliance

Many factors can affect the performance of the security measures, for example, the implementation of exerted pressure (performance pressure) by the imposition of a higher priority towards production and on security; Cost-benefit factors, include the perception of personal gains and losses [2;8]; conflicts between personal and organizational goals [4;5;9] - both are detrimental to security objectives. And finally, risk or perceived risk in time.

The role of risk perception is particularly interesting [10]:

(1) While other potential influences (eg the performance pressure) may or may not be present, there is always some impact (change) on the perception of risk.

(2) In addition, the perception of risk is very volatile and orientate the inclination of direct and indirect circumstances (eg, clean and experiments reported), and have a remarkable impact on the volatility.

(3) A powerful psychological mechanism - to learn. Instrumental conditioning - imply that vigilance on risks has a positive impact on compliance.

(4) An unfortunate aspect of instrumental conditioning - i.e. the extinction of the conditioned behavior is likely to be a major reason for the tendency of performance standards to deteriorate and diminish over time.

A. 3.2 The theory of controlled behavior

1) 3.2.1 Introduction

The theory of the regulation of behavior operating conditioning is posited on a continuum from quite simple to dynamic models of compliance [5;11] However, the dependence of the compliance risk perception should be a good initiating point for studying the dynamics of information security systems.

Operant conditioning is learning through consequences: the behavior of the object that produced positive results (high "instrumental response") is strengthened, and the negative effects that result in (on "instrumental response") is weakened. Two aspects are essential: (1) Introduction of a contingency between one stimulus ("booster") and the highly desirable event perceived by the subject as less desirable ("instrumental response") (2) contiguity between the instrumental responses and reinforce[7].

The theory of control behavior is a relatively recent phenomenon that addresses two key questions regarding the operant conditioning, i.e. making something effective as a reinforce/reinforcement and how–it triggers and operates its activating effect [11-13]. The Behavioral Bliss Point (BBP) - defined as the preferred distribution of the object of activity in the absence of procedural restrictions - is a key concept here.

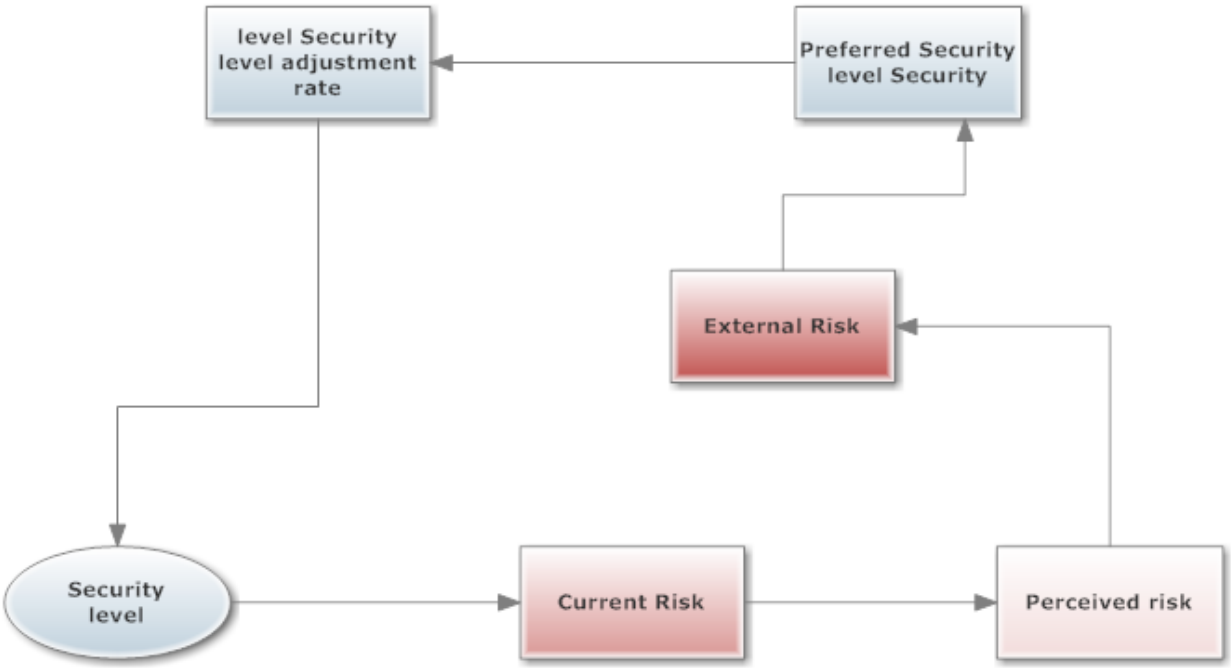

Figure 1: the proposed model

IV. REFERENCE MODES FOR REAL-LIFE SECURITY SYSTEMS

Information security systems therefore need a consistent management policy dealing with human nature. Unfortunately, too often it is based solely on technical issues. In which case, the human factors in security systems are treated as "obvious" or considered unmanageable, hoping that technological solutions will automate security marginalities. Such an approach is useless: the literature emphasizes error in "ironies of automation" where humans can execute technologically trivial tasks, leaving more people demanding tasks [12-14]. As for the interactions between people, [1] provides that the technology "this interaction is the biggest security risk of all."

To improve the robustness of the safety systems of modern information, further understanding of the role of human factors - particularly its dynamics - is essential. The perception of the intrinsic interactions among people, technology and the working environment in the security systems is the primary goal of our research [15; 16]. The problem requires an interdisciplinary approach involving the relevant knowledge of technology, information science, psychology and management. To understand the dynamics is to understand the causal structure of problems and the opening of channels or ways for the most effective policies (eg, the use of system dynamics).

Thus far, the research focused on exploring theoretical aspects. Having acquired an initial theoretical understanding of the problem, we are now ready to expand our objectives, including research applications. We are interested in collaborating with organizations in order to obtain data on the performance of information security systems (technology, environment and people) [16]. These "reference patterns of behavior" would guide the development and validation of comprehensive models of dynamic systems and their implementation in terms of specific recommendations to improve security policies. We hope that this paper encourages collaborations between organizations and us.

V. CONCLUSION

The proposed model is to enhance the information security of data transferred in its lifecycle in different level of risk and the future work is to find an algorithm to connect the proposed model with artificial intelligent to have an integrated sustainable security of data could help both sender and receiver to secure their data.

VI. REFERENCES

[1] B. Schneier, “Schneier on Security,” Wwwschneiercom, p. 336, 2008.
[2] H. Kadhem, T. Amagasa, and H. Kitagawa, “A Novel Framework for Database Security Based on Mixed Cryptography,” 2009 Fourth Int. Conf. Internet Web Appl. Serv., 2009.
[3] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, et al., "Position-based quantum cryptography: Impossibility and constructions," SIAM Journal on Computing, vol. 43, pp. 150-178, 2014.
[4] M. M. Jaber, M. K. A. Ghani, N. Suryana, M. A. Mohammed, and T. Abbas, “Flexible Data Warehouse Parameters: Toward Building an Integrated Architecture,” Int. J. Comput. Theory Eng., vol. 7, no. 5, pp. 349–353, 2015. DOI: 10.7763/IJCTE.2015.V7.984
[5] K. M. A. Ghani, M. M. Jaber, and N. Suryana, “Telemedicine supported by data warehouse architecture,” ARPN J. Eng. Appl. Sci., vol. 10, no. 2, pp. 415–417, 2015.
[5] M. K. A. Ghani, M. M. Jaber, and N. Suryana, “Barriers Faces Telemedicine Implementation in the Developing Countries : Toward Building Iraqi Telemedicine Framework,” ARPN J. Eng. Appl. Sci., vol. 10, no. 4, pp. 1562–1567, 2015.
[7] A. W. Naji, S. A. Hameed, W. F. Al-khateeb, O. O. Khalifa, and T. S. Gunawan, “Executable File Using Computation between Advanced Encryption Standard and Distortion Techniques,” vol. 3, no. 1, pp. 1–6, 2009.
[8] J. J. Gonzalez and A. Sawicka, “A Framework for Human Factors in Information Security,” Int. Conf. Inf. Secur., pp. 1–6, 2002.
[9] J. Katz and Y. Lindell, Introduction to modern cryptography: CRC Press, 2014.
[10] T. J. Abaas, A. S. Shibghatullah, and M. M. Jaber, “Use Information Sharing Environment Concept to Design Electronic Intelligence Framework for Support E-Government : Iraq as Case Study,” Sci. Int., vol. 4, no. 1, pp. 22–24, 2014.
[11] N. Ferguson, B. Schneier, and T. Kohno, Cryptography Engineering: Design Principles and Practical Applications: Design Principles and Practical Applications: John Wiley & Sons, 2011.
[12] M. A. Fengou, G. Mantas, D. Lymberopoulos, N. Komninos, S. Fengos, and N. Lazarou, “A new framework architecture for next generation e-health services,” IEEE J. Biomed. Heal. Informatics, vol. 17, no. 1, pp. 9–18, 2013.
[13] J. Nazario, “DDoS attack evolution,” Netw. Secur., vol. 2008, no. 7, pp. 7–10, 2008.
[14] M. H. Ali and M. A. Othman, "Towards a Exceptional Distributed Database Model for Multi DBMS," in Advanced Computer and Communication Engineering Technology, ed: Springer, 2015, pp. 553-560.
[15] M. M. Jaber, M. K. A. Ghani, and N. S. Herman, “a Review of Adoption of Telemedicine in Middle East Countries : Toward Building Iraqi Telemedicine Framework,” Sci. Int., vol. 26, no. 5, pp. 1795–1800, 2014.
[16] M. A. Mohammed, M. H. Kadhim, A. Fuad, and M. M. Jaber, "Follow up System for Directorate of Scholarship and Cultural Relations in Iraq," in International Conference on Computer, Communications, and Control Technology (I4CT), 2014, pp. 182-187.