Chapter 1.2
Social and Human Elements of Information Security:
A Case Study

Mahil Carr
Institute for Development and Research in Banking Technology, India

ABSTRACT

This chapter attempts to understand the human and social factors in information security by bringing together three different universes of discourse – philosophy, human behavior and cognitive science. When these elements are combined they unravel a new approach to the design, implementation and operation of secure information systems. A case study of the design of a technological solution to the problem of extension of banking services to remote rural regions is presented and elaborated to highlight human and social issues in information security. It identifies and examines the concept of the 'Other' in information security literature. The final objective is to prevent the 'Other' from emerging and damaging secure systems rather than introducing complex lock and key controls.

DOI: 10.4018/978-1-60566-036-3.ch008

AI can have two purposes. One is to use the power of computers to augment human thinking, just as we use motors to augment human or horse power. Robotics and expert systems are major branches of that. The other is to use a computer's artificial intelligence to understand how humans think. In a humanoid way. If you test your programs not merely by what they can accomplish, but how they accomplish it, they you're really doing cognitive science; you're using AI to understand the human mind.

-Herbert Simon

INTRODUCTION

Information security falls within the broad category of security. All the while when designing systems, designers employ an underlying model of the "human being" who is either an "attacker," "adversary," "eavesdropper," "enemy," or "opponent," apart from the normal user of a system who is a "beneficiary," "customer," or "user." For the sake of simplicity, let us call the human being who interacts with the information system in the normal, authenticated, and authorized user mode as a legitimate "user." Let us call a human being who interacts with the system performing some illicit operations not within the legitimate framework as the "other." It is important to understand that the same person may switch between different modes from user to the other depending on the context. Most security systems employ a model of the "other" in relation to which the security features of systems are designed.

This chapter focuses on fundamental underlying premises that are implicitly or explicitly employed while constructing secure information systems. This chapter attempts to open the door for a new approach to the study of information security. It examines the human and social factors in information security from the perspective of a model of human behavior and cognitive science. A real world case study is the basis from which insights are drawn from the process of its design (but not actual implementation). We attempt to outline three distinct universes of discourse and frames of reference and try to relate them together. First, we look at the underlying broad philosophical assumptions of security frameworks in general. Second, we choose a model of human behavior from a systems perspective and situate a cognitive science approach within it. Third, we analyze the technical fabrication of information security protocols in the context of human and social factors, drawing insights from a case study. We discuss and highlight issues in providing secure messaging.

The philosophy of security section discusses the reason why at all we need secure systems. Secure systems are products of a particular time, space, and the level of technology currently available in a society. From the nature of humanity we draw the conclusion that all human beings have the potential to create security hazards. However, whether a person is a legitimate user of the system or the "other" (at the individual level) is determined by his or her cognitive (rational) capacities, emotions (affective states), intent (will), spirituality (belief systems adhered to), and the overt behavior of the individual that is expected of him or her. This provides an explanatory framework to understand why individuals who are intelligent opt to undertake malicious activities (e.g., "hackers" and "terrorists"). The social setting in which the individual is embedded to a great extent determines his or her predisposition to choose act the role of "the user" or the "other." The expression of the "collective conscience" of the community to which he or she belong gives sustenance to the emotional basis, the formation of will, the spiritual basis, and specifies public action that is encouraged. Though these particular human and social factors are not treated in depth in this chapter, it points out that these factors have to be studied seriously and an approach should be taken to prevent the emergence and continued presence of the "other" in the social space. This probably is a more secure way of ensuring implementation of security features.

We look at a case study where information security is of key concern in a modern financial system. The case study outlines a design process for remote banking that offers several technical and managerial challenges. The challenge is to be able to extend banking to communities that hitherto have had no experience in banking and to those who are illiterate. This chapter outlines the technical issues that need to be addressed to make remote banking a reality. From this case study, we draw conclusions of how the "other" is present in the design of the project. We have only emphasized and dealt with the cognitive model of the "other" among the several human and social factors involved in providing a secure financial system. We conclude the chapter paving

Related Content