Chapter 7.6
A New Approach to Reducing Social Engineering Impact

Ghita Kouadri Mostefaoui
Oxford University Computing Laboratory, UK

Patrick Brézillon
LIP6, Paris 6, France

ABSTRACT

In recent years, the security research community has been very active in proposing different techniques and algorithms to face the proliferating security vulnerabilities. However, social engineering remains an alarming threat to the most secured networks. Security administrators are certainly aware of the gravity of the human factor, whatever is the strength of the technological measures. The human factor is still a difficult-to-surround notion and a difficult to quantify concept. It is rarely considered in the early stages of the development lifecycle of software, assuming traditional security considerations have been taken into account. In this chapter, we discuss the added-value of context as a way to deal with social engineering. Based on a case study describing a typical attack, we provide a first attempt to model this parameter.

DOI: 10.4018/978-1-60566-132-2.ch012

INTRODUCTION

Most of us have already been the target of social engineering attacks, whatever they succeeded or not. Emails asking for bank accounts passwords, grabbing user credentials by directing him to fake websites, or extracting passwords by false pretext phones are all examples of social engineering attacks. Kevin Mitnick in his book "*The art of deception: controlling the human element of security*" states that "*Social engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he isn't, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology.*" (Mitnick & Simon, 2003). Even if some application like medical systems and bank websites are more targeted than others to such attacks, social engineering is gaining ground in other fields. Curiosity, trust and intimidation are all examples of human weaknesses the social engineer takes advantage of. For example,

the well-known "ILoveYou" virus email exploited the weakness that curious people would click on an e-mail attachment with such an attractive subject was one of the factors that allowed this virus to have such a big impact (Edmead, 2002) even if it also used technological tools. A worsening factor for social engineering impact is the discrepancy with the technical dimension i.e. the evolution of ICT (Information and Communication Technology) often left an increasing number of persons on the side. The social-technical gap is the difference between social needs/expectations and computer system capability. It is the degree software fails to meet social requirements. Additionally, the fact that duration of work with others is limited, and the turnover is increasingly important and that on the Internet one is not always sure of the identity of the other (use of pseudo), trust becomes a key element in all transactions.

In this chapter, we discuss the added-value of context as a way to deal with social engineering. Two things are worth developing, the focus and its context of validity. Generally in security one is concerned by the focus only. Our claim is to learn how to recognize the context of the current focus, to identify it and to determine what the legal actions are authorized in relationships to the focus in the current context. For example, some attacks use URLs or Web pages very close from those of enterprises. One example is "BankOfAmerica" instead of "Bank_of_America". Another example is to write the real URL on a web page and hide another link when the user clicks.

As social engineering is now admitted to be the weakest link in the security chain, several efforts have been made in order to study its different ways of operation and to try finding defenses against this threat. From these contributions, users' awareness to information security and training emerge as the agreed upon ways for facing the attacks. Related work includes (Lafrance, 2004) which considers psychology as a valuable security tool. The author argues on the understanding of employees' psychology in order to be able to face their potential attacks. He proposes a set of 'psycho-security tips' and shows how they can apply to real situations. More focused on information security awareness, (Manjak, 2006) examines the various social engineering tactics targeting employees that an InfoSec Awareness campaign is designed to counter.

In this chapter, we will first define context and show how it can be considered as an operational factor for modeling the human element in security. Based on a case study of an attack preparation and execution, we show how the previous list of countermeasures (user's awareness, training) can be extended. A list of best practices is derived for the sake of reducing the impact of human element on information security. Then, a summary of previous contributions on the use of context in security is presented. Finally, the last section concludes the paper with a summary of future research.

BACKGROUND ON CONTEXT

This Section is intended to provide a summary of theoretical study of context.

The term context has been extensively defined and commented in recent research. However, there is not yet a commonly accepted definition of context (Bazire & Brézillon, 2005). Nevertheless, a consensus begins to appear around "*Context is what constrains a problem solving without intervening in it explicitly*" (Brézillon & Pomerol, 1999). This definition suggests that the context is always let implicit and tacit, and is rarely mentioned explicitly.

Then, the authors consider it by extension as the focus of an actor. Several elements justify this definition, the three main elements being that:

1. Context is relative to the focus,
2. As the focus evolves, its context evolves too, and
3. Context is highly domain-dependent. As a consequence, one cannot speak of context in an abstract way.