Chapter IX
Effects of Digital Convergence on Social Engineering Attack Channels

Bogdan Hoanca
University of Alaska Anchorage, USA

Kenrick Mock
University of Alaska Anchorage, USA

ABSTRACT

Social engineering refers to the practice of manipulating people to divulge confidential information that can then be used to compromise an information system. In many cases, people, not technology, form the weakest link in the security of an information system. This chapter discusses the problem of social engineering and then examines new social engineering threats that arise as voice, data, and video networks converge. In particular, converged networks give the social engineer multiple channels of attack to influence a user and compromise a system. On the other hand, these networks also support new tools that can help combat social engineering. However, no tool can substitute for educational efforts that make users aware of the problem of social engineering and policies that must be followed to prevent social engineering from occurring.

INTRODUCTION

Businesses spend billions of dollars annually on expensive technology for information systems security, while overlooking one of the most glaring vulnerabilities—their employees and customers (Orgill, 2004; Schneier, 2000). Advances in technology have led to a proliferation of devices and techniques that allow information filtering and encryption to protect valuable information from attackers. At the same time, the proliferation of information systems usage is extending access to

Copyright © 2009, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

more and more of the employees and customers of every organization. The old techniques of social engineering have evolved to embrace the newest technologies, and are increasingly used against this growing pool of users. Because of the widespread use of information systems by users of all technical levels, it is more difficult to ensure that all users are educated about the dangers of social engineering. Moreover, as digital convergence integrates previously separated communications channels, social engineers are taking advantage of these blended channels to reach new victims in new ways.

Social engineering is a term used to describe attacks on information systems using vulnerabilities that involve people. Information systems include hardware, software, data, policies, and people (Kroenke, 2007). Most information security solutions emphasize technology as the key element, in the hope that technological barriers will be able to override weaknesses in the human element. Instead, in most cases, social engineering attacks succeed despite layers of technological protection around information systems.

As technology has evolved, the channels of social engineering remain relatively unchanged. Attackers continue to strike in person, via postal mail, and via telephone, in addition to attacking via e-mail and online. Even though they arrive over the same attack channels, new threats have emerged from the convergence of voice, data, and video. On one hand, attacks can more easily combine several media in a converged environment, as access to the converged network allows access to all media types. On the other hand, attackers can also convert one information channel into another to make it difficult to locate the source of an attack.

As we review these new threats, we will also describe the latest countermeasures and assess their effectiveness. Convergence of voice, data, and video can also help in combating social engineering attacks. One of the most effective countermeasures to social engineering is the continued education of all information systems users, supplemented by policies that enforce good security practices. Another powerful countermeasure is penetration testing, which can be used to evaluate the organization's readiness, but also to motivate users to guard against social engineering attacks (see for example Argonne, 2006).

Throughout this chapter we will mainly use masculine gender pronouns and references to maleness when referring to attackers, because statistically most social engineering attackers tend to be men. As more women have become proficient and interested in using computers, some of the hackers are now female, but the numbers are still small. Nonetheless, there are some striking implications of gender differences in social engineering attacks, and we discuss those differences as appropriate.

SOCIAL ENGINEERING

Social engineering includes any type of attack that exploits the vulnerabilities of human nature. A recent example is the threat of social engineers taking advantage of doors propped open by smokers, in areas where smoking is banned indoors (Jaques, 2007). Social engineers understand human psychology (sometimes only instinctively) sufficiently well to determine what reactions they need to provoke in a potential victim to elicit the information they need. In a recent survey of black hat hackers (hackers inclined to commit computer crimes), social engineering ranked as the third most widely used technique (Wilson, 2007). The survey results indicate that 63% of hackers use social engineering, while 67% use sniffers, 64% use SQL injection, and 53% use cross site scripting.

Social engineering is used so widely because it works well despite the technological barriers deployed by organizations. Social engineers operate in person, over the phone, online, or through a combination of these channels. A report on the

13 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/effects-digital-convergence-social-engineering/29050

Related Content

The Impact of Privacy Risk Harm (RH) and Risk Likelihood (RL) on IT Acceptance: An Examination of a Student Information System
Joseph A. Cazier, E. Vance Wilsonand B. Dawn Medlin (2009). *Techniques and Applications for Advanced Information Privacy and Security: Emerging Organizational, Ethical, and Human Issues (pp. 211-224).*
www.irma-international.org/chapter/impact-privacy-risk-harm-risk/30107

Safeguarding Australia from Cyber-Terrorism: A SCADA Risk Framework
Christopher Beggsand Matthew Warren (2012). *Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions (pp. 369-384).*
www.irma-international.org/chapter/safeguarding-australia-cyber-terrorism/63100

Secure Anonymous Query-Based Encryption for Data Privacy Preserving in Cloud: Moye()
Martin Konanand Wenyong Wang (2018). *International Journal of Information Security and Privacy (pp. 1-23).*
www.irma-international.org/article/secure-anonymous-query-based-encryption-for-data-privacy-preserving-in-cloud/216846

Identification and Authentication for RFID Systems
Behzad Malek (2013). *Advanced Security and Privacy for RFID Technologies (pp. 101-124).*
www.irma-international.org/chapter/identification-authentication-rfid-systems/75514

PAKE on the Web
Xunhua Wangand Hua Lin (2009). *International Journal of Information Security and Privacy (pp. 29-42).*
www.irma-international.org/article/pake-web/40359