Chapter XII
Deception in Cyber Attacks

Neil C. Rowe
U.S. Naval Postgraduate School, USA

E. John Custy
U.S. Naval Postgraduate School, USA

ABSTRACT

Cyberspace, computers, and networks are now potential terrain of warfare. We describe some effective forms of deception in cyberspace and discuss how these deceptions are used in attacks. After a general assessment of deception opportunities in cyberspace, we consider various forms of identity deceptions, denial-of-service attacks, Trojan horses, and several other forms of deception. We then speculate on the directions in which cyber attacks may evolve in the future.

INTRODUCTION

Any communications channel can convey false information and, thus, be used for deception (Miller & Stiff, 1993). The communications resources of cyberspace have several characteristics that make them attractive for deception. Identity is hard to establish in cyberspace. So mimicry is easy and often effective, as with the false e-mail addresses used in spam, the fake Web sites used for identity theft, and software "Trojan horses" that conceal malicious functions within. The software-dependent nature of cyberspace also encourages automated deceptions. So the infrastructure of cyberspace itself can fall victim to denial-of-service attacks that overwhelm sites with massive numbers of insincere requests for services.

Amateur attackers (hackers) are attacking sites on the Internet all the time. These attacks can range from vandalism and sabotage to theft and extortion. The rate of attack incidents reported to the Computer Emergency Response Team (CERT) at Carnegie Mellon University continues to grow due to the increased use of automated attack tools (CERT/CC, 2005). Most attack techniques involve deception in some form, since there are many possible countermeasures against attacks in general. Hacker attack techniques can be adopted by information-warfare specialists as tools of warfare (Hutchinson & Warren, 2001; Yoshihara,

2005). Attacks generally exploit flaws in software; and once flaws are found, they get fixed, and the corresponding attacks no longer work. Web sites, such as www.cert.org, serve as up-to-date clearinghouses for reports of security vulnerabilities used by attackers and how to fix them. So information-warfare attacks either need to find software that is not current with vulnerability fixes (something rare for important infrastructure sites) or else develop new techniques that no one knows about (for which the results are only useful for a limited time given the pace of the development of fixes). Since these things are difficult, deception is often used to improve the chances of a successful attack.

DECEPTION IN CYBERSPACE

Deception can be defined as an interaction between two parties, a deceiver and a target, in which the deceiver successfully causes the target to accept as true a specific incorrect version of reality, with the intent of causing the target to act in a way that benefits the deceiver. Because conflicts of interest are almost inevitable whenever humans interact, many deceptions are commonly encountered in everyday life. Though familiarly associated with income taxes, politics, and the sale of used cars, deception can occur in any financial or economic interaction, as well as in advertising, in sports, and other forms of entertainment, in law, in diplomacy, and in military conflicts (Ford, 1996). Deception carries a stigma because it violates the (usually unspoken) agreement of cooperation between the two parties of an information exchange, and thus represents a misuse of and threat to the normal communication process. However, the moral status of deception can sometimes be unclear, as it has been justified in crisis situations, to avoid a greater evil, against enemies, for the public good, or to protect people like children from harmful truths (Bok, 1978).

Cyberspace differs in many ways from our natural environment, and two differences hold special relevance for deception in cyber attacks. First, cyberspace communications channels carry less information than channels of normal "face-to-face" interactions (Vrij, 2000). Cues that we normally use to orient ourselves during a face-to-face interaction may not be available or may be easily forged in cyberspace. For instance, body language, voice inflections, and many other cues are lost in e-mail messages, which permit "spoofing," where a message appears to come from someone other than the author. Second, information in cyberspace can quickly and easily be created or changed so there is little permanence. For instance, Web sites and e-mail addresses can appear and disappear quite fast, making it difficult to assign responsibility in cyberspace, unlike with real-world businesses that have buildings and physical infrastructure. The link between labels on software objects and their human representatives can be tenuous, and malicious users can exploit this. Also, it is difficult to judge the quality of a product in cyberspace, since it cannot be held in the hand and examined, which permits a wide range of fraudulent activities. An example is an antivirus product made available for a free trial that actually harbors and delivers malicious code.

Rowe (2006) and Rowe and Rothstein (2004) identify 23 categories of possible deceptions in attacks in cyberspace, based on case grammar in linguistics. Arranged in decreasing order of their estimate of suitability and effectiveness in cyberspace, these categories are deception in agent (deceiving the target about who performs an action), accompaniment (what the action is accompanied by), frequency (of the action), object (of the action), supertype (category of the action), experiencer (who observes the action), instrument (used to accomplish the action), whole (to which the action belongs), content, external precondition (environmental effects on the action), measure, location-from, purpose, beneficiary, time-at, value (of data transmitted by the action), location-to, location-through, time-through, internal precondition (self-integrity of the action), direction, effect, and cause. We elaborate on these major categories in the following sections.