2007

Deception in Cyber-Attacks

Rowe, Neil C.; Custy, E. John

Cyber War and Cyber Terrorism, ed. A. Colarik and L. Janczewski, Hershey, PA: The Idea Group, 2007.
https://hdl.handle.net/10945/36422

Deception in Cyber-Attacks

Neil C. Rowe and E. John Custy
U.S. Naval Postgraduate School

Abstract

Cyberspace, computers and networks, is 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.

This is a chapter in *Cyber War and Cyber Terrorism*, ed. A. Colarik and L. Janczewski, Hershey, PA: The Idea Group, 2007.

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 email 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 attacks 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 development of fixes). Since these things are difficult, deception is often used to improve the chances of success of an 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 email messages, which permits "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 email addresses can appear and disappear quite fast, making it difficult to assign responsibility in cyberspace, unlike with real-world businesses which 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 which actually harbors and delivers malicious code.

(Rowe, 2006) and (Rowe & 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 their major categories in the following sections.

Identity deception

Since impersonation is easy in cyberspace, many attacks exploit it. These are generally deceptions in "object", "whole", "instrument", "supertype", and "agent". Military personnel are tempting targets for "social engineering" attacks involving impersonation of one person by another. Social engineers assume a false identity to manipulate people into providing sensitive information or performing tasks (Mitnik, 2002), often by deceiving as to “purpose” and “beneficiary”. An example is pretending to be a representative of the information-technology staff so as to steal a password from a new employee.

Phishing is a particularly dangerous kind of impersonation for social engineering that has increased in frequency and severity recently (MessageLabs, 2005). A perpetrator sends email to a large group of potential targets, urging them to visit a Web site with a familiar-sounding name to resolve some bogus issue. For example, a bogus email from “PayPal, Inc” may urge that “Security updates require that you re-enter your user name and password." The information provided by the victim is used to commit identity theft or enable espionage. Organizations are increasingly being targeted by “spear phishers” who carefully tailor their attacks to specific victims to obtain specific secrets from them, as a form of espionage.

A more subtle category of identity deception in cyberspace is “privilege escalation” where an attacker gains access to a system through a vulnerable account, and then exploits additional vulnerabilities to parlay their limited privileges up to those of a full system administrator (Erbschloe, 2005). This is analogous to what human spies try to do in improving upon their access abilities. Privilege escalation can be accomplished by certain buffer overflows in software. A buffer overflow occurs when a piece of information provided by a user is larger than the space allocated for it by the program, and under the right circumstances when there is a flaw in the software, this can allow a malicious user to overwrite parts of the operating system and execute arbitrary code at a higher level of privilege. Buffer overflows are common because some popular programming languages like C and C++ and some common software products, do not automatically enforce bounds on data placed in memory. Another technique for escalating privileges is to steal a password table, try passwords systematically until a correct one is found, and then impersonate the owner of the password on the system. Usually passwords are stored in a "hashed" form that cannot be decrypted, but the hashing algorithm is often known and attackers can just try to match the hashes repeatedly on a fast machine of their own.

Knowledgeable attackers who successfully escalate privileges may try to install a “rootkit” to conceal or camouflage their presence and actions from system administrators (Kuhnhauser, 2004). A rootkit is a replacement for critical parts of the operating system of a computer to provide clandestine access and total control of the computer by the attacker. This is analogous to occupying the adversary’s terrain in conventional warfare. Rootkits usually include a specially modified file-listing and process-listing commands that hide the attacker’s files and processes from administrators and other users (Denning 1999). A rootkit can provide a “backdoor” by surreptitiously listening on a port for (possibly encrypted) control commands from an attacker.

Other common identity deception on the Internet involves impersonating computers. This includes "spoofing" of Internet addresses by

faking the header information on Internet packets to make it look like it came from someplace other than where it really came from. Impersonation of computers can also use them as screens to camouflage the origin of an attack. That is, a machine on which an attacker has gained unauthorized access can serve as a launching point for further unauthorized accesses, concealing the attacker's identity because it is difficult to trace a connection backwards through many intermediate machines with most Internet protocols. Intervening computers also may be located in many countries throughout the world, and legal coordination between jurisdictions can be difficult (Stoll, 2000).

Denial-of-service attacks

A denial-of-service attack slows or stops the operation of a cyberspace resource or service by overwhelming it with insincere requests. Denial-of-service attacks are deceptions in "frequency" and "purpose" as per (Rowe and Rothstein, 2004). They can occur if large numbers of coordinated computers try to access the same Web site simultaneously. These attacks are easy to do, and have been used successfully against big companies like Amazon and the U.S. Presidential site. Another example is a "SYN flood attack" against the commonly-used TCP protocol (McClure, Scambray, and Kurtz, 2005) which involves the attacker starting, but not completing, a large number of interactions called "three-way handshakes" with a victim computer. This forces the victim to maintain many half-open connections which prevent valid connections from being established. Denial of service can also be achieved by a "Smurf" attack, which involves flooding a network with many ICMP echo (or "ping") requests to different machines. The requests have their source addresses forged as that of the victim machine, which is flooded with echo responses and overwhelmed.

Denial of service is quite valuable militarily as a way to disable adversary computer systems. Potential targets could include command-and-control networks, file servers holding mission plans, Web servers holding enemy communications intercepts, and Domain Name Service (DNS) sites that serve as the Internet's indexes.

Trojan horses

Attacks can be concealed inside otherwise innocent software. These are called "Trojan horses" (Erbschloe, 2005) and are instances of deception in "accompaniment" and "content". To trick a user into running them, they can be provided for free at Web sites, sent as email attachments with forged addresses, hidden in storage media, or even embedded when the software is manufactured. The "cover" software can be a useful utility, a game, or a "macro" (embedded code) within a document file. Running a piece of software is insufficient to confirm it is malicious since its sabotage or espionage may be subtle, or it may be set to trigger later according to the clock or on instructions from a remote attacker. Sabotage can range from changing numbers in data to causing programs to fail completely. Computer viruses and worms are important forms of Trojan horses, but they are usually too obvious to be effective for military use.

An important category of Trojan horses is spyware, or automated espionage in cyberspace. These programs covertly pass useful information back to an attacker about the activities on a computer, and so are deception in "experiencer". Spyware is currently an epidemic although its incidence is decreasing as antivirus and antispyware software is now looking for it. Commercial spyware usually just reports what Web sites a user visits, but the techniques can be adapted for espionage to record everything a user types on a keyboard, enabling theft of passwords and encryption keys. Spyware uses "covert channels" to communicate back to its controller; these can use encryption (messages transformed into unintelligible codes) (Pfleeger, 1997) or "steganography" (concealed messages in what appears to be innocent messages or data) (Wayner, 2002). For instance, an encryption of the password "foobar" might be "&3Xh0y" whereas the steganographic encoding might be "find our own bag at Rita's", using the first letter of every word. Steganography can also use subtle features like the number of characters per line, the pattern of spaces in a text document, or every 137^{th} letter.

Miscellaneous deceptions

Other deceptions from the taxonomy of (Rowe, 2006) can be used in cyberspace:

- Buffer overflows can be done by sending insincere large inputs to programs.
- To achieve surprise, attacks can involve rarely-used software, ports, or network sites.
- Attacks can have surprising targets such as little-used software features.
- Attacks can occur at surprising times (but everyone knows the Internet is always active).

- Attacks can occur from surprising sites (but everyone knows attacks can come from anywhere).
- To maximize concealment, attacks can be done very slowly, as by sending one command a day to a victim computer.
- Attacks can modify file or audit records in time and details to make attackers appear to have been doing something different at a different time.
- Attackers can claim abilities that they do not possess for purposes of extortion, such as the ability to disable a computer system.

Future trends

As defenses to cyber-attack improve, we can expect amateur cyber-attacks to show more deception, and information-warfare attacks can be expected to show more too. Attacks are increasing in technical sophistication as easier attacks are being blocked or foiled. Deception can be a useful "force multiplier" for mission plans in cyberspace just as in real battlespaces (Dunnigan & Nofi, 2001). But we do not expect many new deceptions since most of the possible ploys have already been explored. And it will become more difficult for deceptions to succeed: Defenses are improving, and defenders are becoming more aware of deceptions being practiced, so that the pool of potential victims for many attacks is decreasing.

The diversity of deceptions should increase in the future as the continued development of automated tools will permit attackers to try many methods at once. But diversity in defenses against deceptions should also increase. Deception will be increasingly common in asymmetric cyberwar, as it is in asymmetric conventional warfare (Bell & Whaley, 1991), for tactics and strategies by the weaker participant.

Conclusions

Deception occurs in all military conflicts, and as more military activity shifts to cyberspace we will see more deception there too. An analysis of how deception is used in attacks can help in understanding them, with the goal of developing effective defenses for future attacks. The deception methods we have described here are not difficult to use. While there have not been confirmed instances of cyberwar using deception, information-warfare specialists are developing cyberweapons using these methods. However, a wide variety of methods can be used to ensure that particular cyber-attack deceptions against a particular target are totally ineffective.

References

Bell, J., & Whaley, B. (1991). *Cheating and deception.* New Brunswick, New Jersey: Transaction Publishers.
Bok, S. (1978). *Lying: moral choice in public and private life*. New York: Pantheon.
CERT/CC (2005). CERT/CC Statistics, 1988-2005 (2005). Retrieved from www.cert.org/stats/cert_stats.html, February 15, 2006.
Denning, D. (1999). *Information warfare and security*. New York: Addison-Wesley.
Dunnigan, J. F., & Nofi, A. A. (2001). *Victory and deceit, 2nd edition: deception and trickery in war.* San Jose, California: Writers Press Books.
Erbschloe, M. (2005). *Trojans, worms, and spyware: a computer security professional's guide to malicious code.* Amsterdam: Elsevier.
Ford, C. V. (1996). *Lies! Lies!! Lies!!! The psychology of deceit*. Washington, DC: American Psychiatric Press.
Hutchinson, W., & Warren, M. (2001). *Information warfare: corporate attack and defense in a digital world*. London, UK, Butterworth-Heinemann.
Kuhnhauser, W. (2004, January). Root kits: an operating systems viewpoint. *ACM SIGOPS Operating Systems Review, 38* (1), 12-23.
McClure, S., Scambray, J., & Kurtz, G. (2005). *Hacking exposed, fifth edition.* New York: McGraw-Hill Osborne.
MessageLabs (2005). Annual Security Report. Retrieved from www.messagelabs.com/publishedcontent/publish/threat_watch_dotcom_en/intelligence_reports/2005_annual_security_report/DA_123230.chp.html, February 8, 2006.
Miller, G. R., & Stiff, J. B. (1993) *Deceptive communications.* Newbury Park, UK: Sage Publications.
Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: controlling the human element of security*. Indianapolis, Indiana: Wiley.
Pfleeger, C. P. (1997). *Security in computing, second edition.* Upper Saddle River, New Jersey: Prentice Hall PTR.
Rowe, N., & Rothstein, H. (2004). Two taxonomies of deception for attacks on information systems. *Journal of Information Warfare, 3*(2), 2004, 27-39.
Rowe, N. (2006, March) A taxonomy of deception in cyberspace. *International Conference on Information Warfare and Security*,

Princess Anne, Maryland, USA.
Stoll, C. (2000). *The cuckoo's egg: tracking a spy through the maze of computer espionage.* Pocket Books, New York.
Vrij, A. (2000). *Detecting lies and deceit: the psychology of lying and the implications for professional practice*. Chichester, UK: Wiley.
Wayner, P. (2002). *Disappearing cryptography: information hiding: steganography and watermarking.* San Francisco, California: Morgan Kaufmann.
Yoshihara, T. (2005, December). Chinese information warfare: a phantom menace or emerging threat? Retrieved from www.strategicstudiesinstitute.army.mil/pubs/display.cfm?PubID=62, December 2005.

Terms

Buffer overflow: Techniques by which large inputs are given to software to induce it to do things it normally does not.
Covert channel: A concealed communications channel.
Denial of service: An attack that overwhelms a cyberspace resource with requests so as to prevent authorized persons from using the resource.
Encryption : A systematic and reversible way of making a message unintelligible, using secret keys..
Escalation of privileges: Exploiting security weaknesses to increase one's abilities on a computer system.
Hacker: An amateur attacker of computers or sites on the Internet.
Phishing: Email that tries to steal secrets by directing users to a counterfeit Web site.
Rootkit: Replacement code for the operating system of a computer, placed on a compromised system by an attacker to ensure that their malicious activities will be hidden and to simplify future access to the system by them.
Social engineering: Methods to trick or manipulate people into providing sensitive information or performing a task.
Steganography: Concealed messages within others.