Cyber Deception

Neil C. Rowe[1*]
[1] U.S. Naval Postgraduate School
ncrowe@nps.edu

Synonyms

Deceptive software and networks

Definition

Deception is the process of deliberately making someone or something have a false belief. Examples in cyberspace are fake sites, fake files, insincere requests, false error messages, and deliberately uncooperative interactions.

Background

Deception is easier in the cyber world because many clues that reveal deception in the real world are missing in cyberspace (Rowe and Rrushi 2016). It is difficult to confirm the persons or organizations with which one is interacting in cyberspace; data recorded can easily be changed without a trace; and data appears uniform and does not provide clues to its origin.

Deception is a normal part of non-cyber social interactions and is an essential part of human nature despite the pronouncements of philosophy and religions (Smith 2004). Deception has a long history in warfare, and is a key issue in law, business, psychology, and entertainment.

Theory and Applications

Offensive deception

Nearly all malicious cyber activity requires some deception. Computers and devices are carefully designed to be predictable and execute only authorized code. The most effective way that malicious activity can circumvent this is by deception. Some example "offensive deceptions" are:

- Masquerade as someone or something different from one's real identity ("spoof" them), as with phishing and identity theft.
- Lie to manipulate someone into doing something you want, as with phishing and social engineering.
- Accompany legitimate activity with something illegitimate, as with concealed Trojan horses in software.
- Overwhelm a target with abnormal amounts of data or requests, as with denial-of-service methods.
- Use surprising tactics against a target, as with some types of social engineering.
- Break suspicious operations into less-suspicious pieces, as with collecting information for espionage.

Because of the limited number of such tactics, security professionals are quite familiar with offensive deception, although recognizing all of it can still be difficult.

Defensive deception

Deception can also be used to defend computer systems and devices automatically, as a third line of defense after authentication and access controls. Defensive deception has been of increasing interest recently since there are more defensive forms than offensive forms. Some example defensive deceptions are:

- Give false but plausible excuses for why a suspicious command cannot be done, as by false error messages claiming that a necessary resource cannot be found.
- Lie about the results of commands, as in falsely claiming download of a suspicious file.
- Masquerade as a different resource than what you are, as with honeypots.
- Provide bait information ("honeytokens"), incorrect information that will cause trouble to a malicious user, such as passwords to honeypots or false bank-card numbers that trigger alarms.
- Delay suspicious users or traffic considerably, since many cyberattacks rely on speed for effectiveness.
- Burden the suspicious user with considerable information to examine, as by having many fake network nodes to impede reconnaissance.
- Deliberately try to confuse a suspicious user, as by providing an interface to an industrial control system where controls work differently from what a cyberattacker expects.
- Camouflage desirable resources like network-topography maps in unexpected ways.
- Send software "beacons" back to a cyberattacker to enable tracing and disabling them.
- Pretend to be a naive victim for social engineering.

Defensive deceptions are usually supported by intrusion-detection systems and other system monitoring for suspicious activity. The higher the probability of malicious behavior, and the higher the benefit of deceiving, the more that deception is warranted. Cost-benefit analysis can quantify these measures.

Deception for encouragement

Deception can be used to encourage cyberattacker interaction with a defender for the purpose of collecting attack data, as with honeypots. Honeypots are decoy computers and devices accessible over a network. They have no assigned functions beyond serving as decoys, so any non-administrative interactions with them must be either scanning or malicious activity.

Honeypots do not require deception, but are more effective if they use deception to conceal that they are honeypots. That is because malicious visitors know that honeypots record interactions, and visitors do not want to reveal their secrets. Furthermore, cyberattackers know that honeypots are designed to be difficult to subvert as a base for malicious activity such as spamming or botnets, so they are unlikely to achieve their goals by attacking a honeypot. To be more appealing, honeypots should also offer a friendly interface to what appears to be an important site with many desirable resources.

Deception by honeypots should hide their logging machinery by using encryption and less-obvious network connections like a second network-interface card. It can also mean placing data on the honeypot copied from real systems, so it looks like a busy system in case a visitor tries to inspect it. Honeypot deception can also include placing especially appealing bait for visitors to find and switching automatically between real and simulated systems.

Deception for discouragement

Deception can also be used to defend normal systems, by neutralizing threats or discouraging them from staying. Deception can try to convince an attacker that the site is not worth attacking because it contains little of value. Or it can try to convince an attacker that the site is too hard to use or too well defended to be exploitable.

The psychology of the attacker matters in deception for discouragement, and in particular, their handling of adversity. Automated cyberattacks by cybercriminals generally retreat when a site does not conform to expectations since their plans are inflexible and will likely then fail, and there are many easier targets available. More narrowly targeted cyberattacks by spies and saboteurs, however, can be more persistent, and will need additional layers of discouragement before they retreat. Some sophisticated attackers like a challenge, and will respond to discouragement with renewed energy, thinking that their target must be valuable if it is well protected. Such attackers can be overwhelmed with unnecessary information, however.

Deceptions benefit from being layered like other cyber defenses. For instance, when cyberattackers find a real site among many fakes on a network and guess its password, they could find many bait listings of honeypots, and then could experience clandestine downloads of Trojan horses onto their machines from those sites. That is three layers.

The costs of deception

Deception often relies on human psychology to succeed, whether in direct interactions with people or indirect interactions through their software. Thus it may fail to achieve its goals if victims recognize it and feel betrayed, and recognized deceptions may even induce anger and retaliation that may cause even worse problems for the deceiver. Detection of deception is more likely when deceptions involve unusual or repeated behavior, so such activity should be avoided by the deceiver. This principle is important with military non-cyber deception, but is contrary to usual software practice and expensive to implement.

Deception also has the odd characteristic that once it is detected by the victim, it is harder to deceive the victim again, even in new ways. This means that effective deceptions must be challenging to detect and can require considerable development time.

Deception can also accidentally harm innocent bystanders, as when a deception for discouragement triggers on mistaken clues and impedes a legitimate user on a system. One must estimate the rarity of this and its cost in advance, and decide if the harm is sufficient to require countermeasures.

Since deception can be used by both sides in cyberspace, it is often useful to model its use as a game, with specific costs and probabilities of events (Kamhoua et al 2021). The game can be simulated and run many times to evaluate the average effects of deceptive tactics and strategies combined with other cybersecurity measures. This can show when tactics such as too-elaborate deceptions are not cost-effective. However, most real cyberattacks fail to notice details of complex deception plans, so game analysis is only occasionally useful.

The ethics of deception

Deception has been roundly decried for centuries despite being ubiquitous. However, most ethical theories support use of deception to prevent a greater harm (Bok 1999) such as destruction of a computer system. Other ethical theories identify actions violating norms of society as “evil” and justifying deceptive countermeasures, and cyberattacks could be considered as evil. Furthermore, some deception is necessary to analyze malicious activity for defensive purposes since attackers will not freely give you their secrets.

Open problems and future directions

Not much innovation is occurring with offensive deception methods since many vulnerable targets do not require sophisticated deceptions to fool. New targets are appearing, but most deception goals are unchanged. However, current work is exploring a wide range of defensive deception methods, many using decoys and honeypots. Over 20 commercial products designed primarily for defensive deception are currently available.

Cross-references

Honeypots, decoys, cyberattacks, spoofing, phishing, Trojan horses, denial of service, identity theft, social engineering, intrusion detection, layered defenses

References

Bok S (1999) Lying: Moral choice in public and private life. Vintage Books, New York.

Kamhoua C, Keikintveldt C, Fang F, Zhu Q, eds. (2021) Game theory and machine learning for cybersecurity. Wiley, Hoboken, US.

Rowe N, Rrushi J (2016) Introduction to cyberdeception. Springer, Switzerland.

Smith D (2004) Why we lie : The evolutionary roots of deception and the unconscious mind. St. Martin's Press, New York.

This article is a chapter in the Encyclopedia of Cryptography, Security, and Privacy, 3rd edition, ed. S. Jagodia, P. Samarati, and M. Young, Springer Berlin, Heidelberg, 2025, pp. 491-494. doi.org/10.1007/978-3-642-27739-9_1766-1