To appear in *Proc. IFIP Eighteenth Int. Inf. Security Conf.*, Kluwer Acad. Publishers (Athens, Greece, May 2003).

Lawful Cyber Decoy Policy

James Bret Michael and Thomas C. Wingfield
Naval Postgraduate School, Department of Computer Science, Monterey, California USA
ManTech Aegis Research Corporation, Falls Church, Virginia USA

Abstract: Cyber decoys provide a means for automating, to a degree, counterintelligence activities and responses to cyber attacks. Like other security mechanisms for protecting information systems, it is likely that cyber decoys will in some instances be misused. In the United States, criminal law provides us with analogies for preventing or punishing improper state use of deception, and criminal and civil law give us a range of tools to use against private actors. However, in addition to states, nongovernmental entities and individuals can employ cyber decoys. In this paper we present a principled analysis of the use of cyber decoys. We explore the absolute minima in terms of customary principles for what might be considered to be acceptable use of deception.

Key words: Deception, Law, Computer security

1. DECEPTION IN CYBERSPACE

In [1], Michael *et al*. propose to use software-based deception as a means for hardening operational systems against attack. Critical units of software are wrapped with "decoying" rules, which are the cyber embodiment of both the policy (including doctrine) of an organization or individual for conducting counterintelligence and applying countermeasures against attackers. The wrappers are placed around critical units of software (*e.g.*, a component or method) to be protected. By critical, we mean units of software that are integral to the continued survivability of an information system and the correct enforcement of the policy embedded in the system.

When a wrapper detects a suspicious pattern of system calls by one or more computer processes, it begins to conduct counterintelligence tasks and initiates countermeasures; pattern recognition is performed at runtime. The

wrappers, referred to as "decoys," conduct counterintelligence by allowing the interaction with suspicious processes to continue, collecting information about the nature of the processes' behavior. The wrappers respond to requests for service from the processes by applying countermeasures, with coordination of their responses provided by "decoy supervisors." The countermeasures include actions taken to shield the wrapped software from any ill effects of the interaction, and the responses to the processes that are needed to deceive the attacker into concluding that his or her computer processes are successfully carrying out their mission. As new patterns of suspicious behavior are discovered, the database of rules for counterintelligence and countermeasure actions is updated.

1.1 A potential "homeland security" application

Homeland security within the United States encompasses, among other things, the protection of public and private cybernetic property against espionage and sabotage, especially if such a compromise would have a significant adverse effect on the national security of the United States.[1]

Let's make the discussion of software decoys more concrete by considering how they can be used to protect a particular type of cybernetic property—a public-switched telephone network (PSTN). Within a PSTN, software units that authenticate subscribers to the network are necessary for enforcing policy against unauthorized eavesdropping on conversations. In addition, the survivability of a PSTN is contingent on the continued correct functioning of the software that implements the Signaling System 7 (SS7) protocol. Thus, by our definition, these software units are system-critical.

Software decoys can be created for both the subscriber-authentication and SS7 software units. For instance, these software units can be wrapped so that they discover patterns of system-level events that are indicative of attempts to cause exceptions to be raised in normally infrequently-called methods of these software units—such invocations of methods constitute a form of suspicious behavior. On detecting a sequence of invocations, such as one that would cause a buffer overflow, the decoys would begin gathering information about the nature of the calling processes' behavior. If a process continues to try to raise exceptions, the decoys could, for instance, fake error-handling messages with the aim of making it appear to the process that the exception was raised and not handled. The goal of the decoy at this point is to maintain interaction with the process, providing the decoy with the opportunity to gather more information about the nature of the interaction. If analysis of the interaction is indicative of an attack, the decoy may be able to discern the sources and methods of the attack, using this information to make decisions about whether to applying passive (*i.e.*, strictly defensive on the

attacked system) or active (*i.e.*, counterattack) countermeasures. Likewise, the decoys may discover the interaction is non-malicious in nature, notifying the owner of the process of his or her egregious use of the software units; this addresses, to some extent, the need to correctly handle false positives.

1.2 Potential for misuse of decoys

The users of software decoys need to employ counterintelligence and countermeasures in a judicious manner, so as to prevent their misuse. For instance, software decoys, like any other software, can behave in unanticipated ways due to the presence of unknown software defects; defects can cause side effects that result in the generation of inappropriate responses. Similarly, the decoys may be poorly designed in terms of the breadth of responses, or in terms of the fidelity with which they implement the owning organization's policy. Alternatively, the decoys may not have built-in controls to prevent users or their decoys from inadvertently contravening an organization's policy on the use of countermeasures and counterintelligence; the foregoing examples exemplify the *technical misuse* of decoys.

Suppose that a public telephone company instructs the decoys used in conjunction with its SS7 software to provide deceptive responses, such as exaggerated delays, to the communication devices used by customers of competing telephone service providers, with the aim of providing those users with a degraded level of service. In the United States, injecting such delays is legal as there is no general duty on the part of nongovernmental entities to tell the truth: suboptimal performance is rarely, if ever, unlawful *per se*. In the eyes of some, the exaggerated delays represent a misuse of the technology in that the company might gain an unfair competitive advantage. We call this *intentional lawful misuse* of decoys.

Further, suppose the federal agencies within the United States employ software decoys. If the National Security Agency were to use the decoys to collect information about attackers who turn out to be U.S. citizens, this would be a violation of federal law. We refer to this as an example of *unintentional unlawful* use of decoys. One means proposed in [2] for countering this and the other types of misuse is to make the decoy supervisors responsible for checking whether the rules for conducting counterintelligence and applying countermeasures in a particular context do not contravene policy.

2. LAWFUL CYBER DECOY POLICY

Policy can be used to provide guidance within an organization on how to properly use software-based deception mechanisms. For instance, the tele-

phone company in the preceding example could have a policy that all of its networks must require knowing intelligent waiver by the user of certain privacy rights after reasonable notice has been given to both legitimate users and intruders that software deception is in use would protect the company, absent any other egregious behavior on its part, from being held legally responsible for damage incurred by the user due to the user's interaction with the software decoys.

Criminal law already goes a long way toward giving us analogies for preventing or punishing improper state use, and criminal and civil law give us a range of tools to use against private actors. However, there are gaps in the law. For example, what if corporations start using software decoys within acceptable limits and contract out those aspects of deception that would cross the line (*i.e.*, be unlawful) while maintaining plausible deniability? (*N.B.*: Nations often contract out covert operations to civilians.)

2.1 The view of deception in society

Deception or "ruses of war" is permissible in military campaigns, and only runs afoul of the law when it rises to the level of "perfidy," the treacherous misleading of an enemy about his—or your—status under the law. However, there is a cultural bias in the United States against the use of deception by any level of government, as evidenced by the recent reluctance to institutionalize deception by quashing the effort to create the U.S. Office of Strategic Influence, whose charter was to conduct perception management across agencies, including disseminating misinformation to foreign journalists in support of the war on terrorism [3]; there is also a strong legal and cultural predisposition against using domestic U.S. journalists for active deception (vice selectively withholding information, which can be enormously effective in crafting the desired conclusion), including formal guidance within the intelligence community against using them in covert operations. It is possible that proposals by the Department of Homeland Security and other government agencies, to defend against terrorist attacks on cyber property, may also fall victim to negative public sentiment: there are enough mainstream concerns about civil liberties to render a potentially intrusive program politically unpalatable. Thus, we propose that individuals and organizations apply principled analysis in assessing the legality of using software-based deception.

2.2 Principled analysis of decoy usage

Principled analysis of the use of deception involves taking into account the value of the target, the nature and immediacy of the threat, the identity of

the actors, the degree to which any state is supporting them, etc. For instance, consider the principle of proportionality, as it pertains to the *jus in bello*, or the law which operates between belligerents in time of war: "[t]he principle of proportionality requires the military commander to balance the collateral damage (against civilians and their property) of a planned attack against the concrete and direct military advantage expected to be gained" [4]. In other words, while civilians and their property may never be targeted as such, the amount of permissible collateral damage varies with the immediate importance of the military target. This applies to digital in cyberspace as certainly as it does to kinetic warfare in realspace. Beyond proportionality, there are three additional customary principles of the law of armed (and information) conflict: chivalry, which embodies the distinction between lawful ruses of war and unlawful perfidy, as mentioned above; discrimination, which allows military objectives, such as combatants and their equipment and facilities, to be targeted, but prohibits the intentional targeting of civilians or their property; and necessity, which has two components. Its quantitative component allows the use of all the force necessary to accomplish a lawful military mission, but no more; its qualitative component permits all means for accomplishing such a mission, with the exception of a small number of uncivilized weapons and techniques deemed too inhumane to be used to *any* degree. Such outlawed means include chemical weapons, biological weapons, x-ray transparent bullets, and blinding lasers. These four customary rules, described as they pertain to military use of software decoys to protect semantic webs, may be found in [2].

Let's proceed to the example of software decoys generating unwanted side effects due to the presence of software defects in the decoys. The principle of proportionality applies here: if the government fails to allocate adequate resources to test and validate its decoys, it would be difficult to conduct a proper proportionality analysis in the heat of information operations in a time of war. Numerous other legal problems, particularly under the principle of necessity, also arise, potentially generating legal liability up to and including the status of "war criminal" for information operators, mission planners, military commanders, and civilian approval authorities. With appropriate advance work, these potential consequences—certainly those due to advance negligence or recklessness—may be virtually eliminated.

3. CONCLUDING REMARKS

It is possible that software decoys can be used as an airlock between the technology and the law in that the decoys can be programmed with a wide spectrum of options for taking action. Software decoys provide for antici-

patory exception handling. In other words, the decoy anticipates the types of inappropriate interaction between the calling process and the wrapped unit of software, providing in advance rules for learning about and evaluating the nature of the interaction, in addition to rules for response. One could envision developing policy that places boundaries on the extent and type of deception to be employed, but providing some degree of latitude to the user of decoys to inject creativity into deceptions so as to increase the likelihood that the deceptions will be effective. The boundaries could be used to delineate the thresholds that if breached could result in the misuse or unlawful use of decoys. That is, principled analysis can be used to meet all domestic legal criteria, and set absolute minima in terms of the four customary principles of discrimination, necessity, proportionality, and chivalry.

Lastly, the U.S. Department of Homeland Security will be responsible for coordinating the protection of both public and private cybernetic property using cyber weapons. There are gray areas in the law regarding how to coordinate counterintelligence activities and countermeasures that need to take place at the intersection of law enforcement, intelligence collection, and military activity. Principled analysis can help here too, but public policymakers will need technically and legally sophisticated advice to manage the best technological defense available within the framework of the law.

NOTES

1. Conducted under the auspices of the Naval Postgraduate School's Homeland Security Leadership Development Program, this research is supported by the U.S. Department of Justice Office of Justice Programs and Office of Domestic Preparedness. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Government.

REFERENCES

[1] Michael, J. B., Auguston, M., Rowe, N. C., and Riehle, R. D. Software decoys: Intrusion detection and countermeasures. In *Proc. Workshop on Inf. Assurance*, IEEE (West Point, N.Y., June 2002), 130-138.

[2] Michael, J. B. On the response policy of software decoys: Conducting software-based deception in the cyber battlespace. In *Proc. Twenty-sixth Annual Computer Software and Applications Conf.*, IEEE (Oxford, Eng., Aug. 2002), 957-962.

[3] Pentagon closed besieged strategic office, *L.A. Times*, 27 Feb. 2002, A6.

[4] Wingfield, T. C. *The Law of Information Conflict: National Security Law in Cyberspace*. Falls Church, Va.: Aegis Research Corp., 2000.