NIST Controls: SC – System and Communications Protection

Written By: Altamash Ali

Publication Date: March 12, 2021

Since the dawn of the internet, there has been a war raging between black hats and white hats. The goal of white hats and the organizations they work for has been to minimize their susceptibility to ongoing attacks. NIST, a non-regulatory agency, is trying to establish a set of industry standards which hopes to bind federal agencies to guidelines which will reinforce safe practices. The legal nature of these standards requires one to also consider any potential legal implications these policies may have. The specific NIST family of controls which we will analyze here are called 'SC – System and Communications Protection'. More specifically, we will consider legal issues regarding 'SC – 26: Decoys' and 'SC – 30: Concealment and Misdirection'. Though some of the strategies outlined in SC-26 and SC-30 seem like they would be illegal or unethical if used any other sense, they instead have been made a part of the guidelines under NIST when it comes to protecting oneself or securing one's environment.

Many organizations implement decoys, which are "specifically designed to be the target of malicious attacks" [1]. A popular example of how this is implemented is through the use of honeypots or honeynets. The goal of these decoys is to lure attackers toward a mock asset, on which if harm is done will have no effect on the organization, while simultaneously deflecting them away from more meaningful assets. Honeypots have always been at the center of controversy for various legal and ethical reasons. Many try to point their use by companies as being a form of entrapment, however this simply cannot be the case since it does not involve a government agent trying to induce an individual into committing a crime in hopes of later prosecuting them. Furthermore, many try to delegitimize the use of honeypots by saying they violate privacy laws in the US. Now while it may be illegal to record data on an attacker breaking into your honeypot, there certainly are exceptions to this. For example, if your honeypot is actively being used to protect your environment, it is exempt from privacy restrictions [3]. While the use of honeypots does not seem to step over any legal restrictions set in place, their use has still been considered unethical. The persisting argument has been that "[if] it is both unethical and illegal to lure someone into stealing an object, why is it legal or ethical to lure an individual into committing a computer crime" [2]? Let's further explore this topic now by analyzing SC-30, which is similar to SC-26.

Concealment and misdirection, which is the premise of SC-30, is used to "significantly reduce the targeting capabilities of adversaries to initiate and complete attacks" [1]. The strategies employed here vary from randomness to uncertainty, in hopes of misleading attackers.

The issue with this practice is that it seems to be borderline deception. Deceit is often described as someone or something "which fraudulently makes a misrepresentation of intention…for the purpose of inducing another to act…in reliance upon it," which is what SC-30 encourages organizations to do [4]. However, this seems to apply more properly to cases in which two parties had made a formal agreement and one of them had failed to deliver what was agreed upon. An example of this is in *Salzman v. Maldaver* where the "seller allegedly placed undamaged aluminum plates on the top of bundles to conceal corroded ones beneath" [4]. In the case of an organization deceiving potential attackers, the act of deception is performed under the pretense of self-defense and for the purposes of defending their systems. Furthermore, no formal agreement was made where an organization had promised to let their guard down and give up their systems to an attacker. In other words, the organization does not owe anything to the attacker since it was the attacker who was actually caught trying to break into their unauthorized systems.

With people describing the internet as a digital warzone nowadays, many questions regarding legality and ethicality have come into the picture. Is deception okay if it means protecting yourself or your organization? Do two wrongs make a right? Many even argue against the use of honeypots because, ironically, their existence only serves to make hackers better at their craft. From popular rulings to guidelines established by NIST, it seems that organizations are encouraged to employ tactics such as deception, misdirection, and concealment for the purpose of protecting their environment.

Sources

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[2] https://ethics.csc.ncsu.edu/abuse/hacking/honeypots/study.php

[3] https://www.netsurion.com/articles/are-honeypots-illegal

[4] https://core.ac.uk/download/pdf/70374446.pdf