CERIAS

The Center for Education and Research in Information Assurance and Security

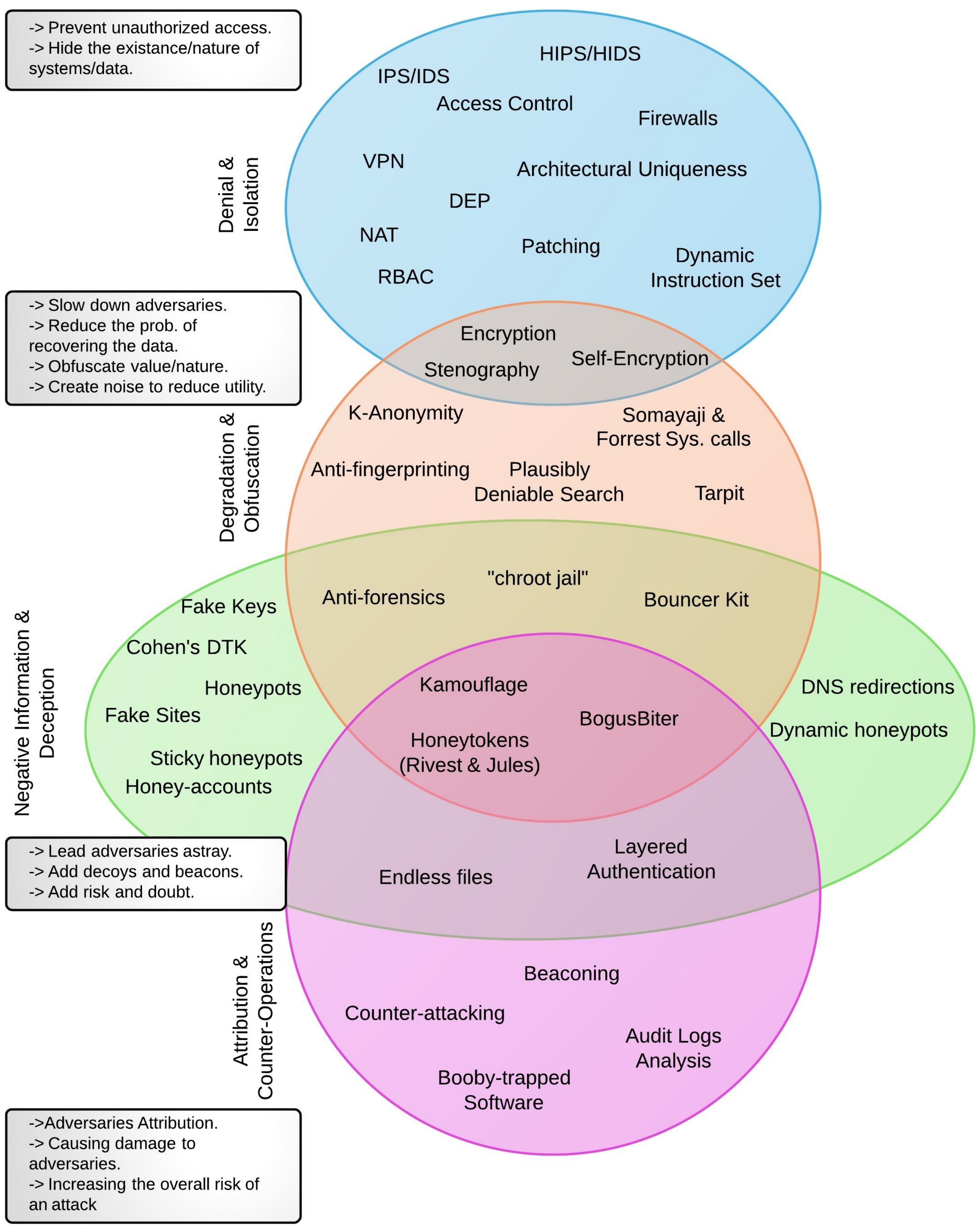
The Case of Using Negative (Deceiving) Information in Data Protection

Mohammed H. Almeshekah and Eugene H. Spafford

Abstract

In this paper we develop a novel taxonomy of methods and techniques that can be used to protect digital information. We explore complex relationships among these protection techniques grouped into four categories. We present analysis of these relationships and discuss how can they be applied at different scales within organizations. We map these protection techniques against the cyber kill-chain model and discuss some findings. Moreover, we identify the use of deceit as a useful protection technique that can significantly enhance the security of computer systems. We posit how the well-known Kerckhoffs's principle has been misinterpreted to drive the security community away from deception-based mechanisms. We examine advantages these techniques can have when protecting our information in addition to traditional methods of denial and hardening. We show that by intelligently introducing deceit in information systems, we not only lead attackers astray, but also give organizations the ability to detect leakage; create doubt and uncertainty in leaked data; add risk at the adversaries' side to using the leaked information; and significantly enhance our abilities to attribute adversaries. We discuss how to overcome some of the challenges that hinder the adoption of deception-based techniques.

How do we Protect Our Information/Systems



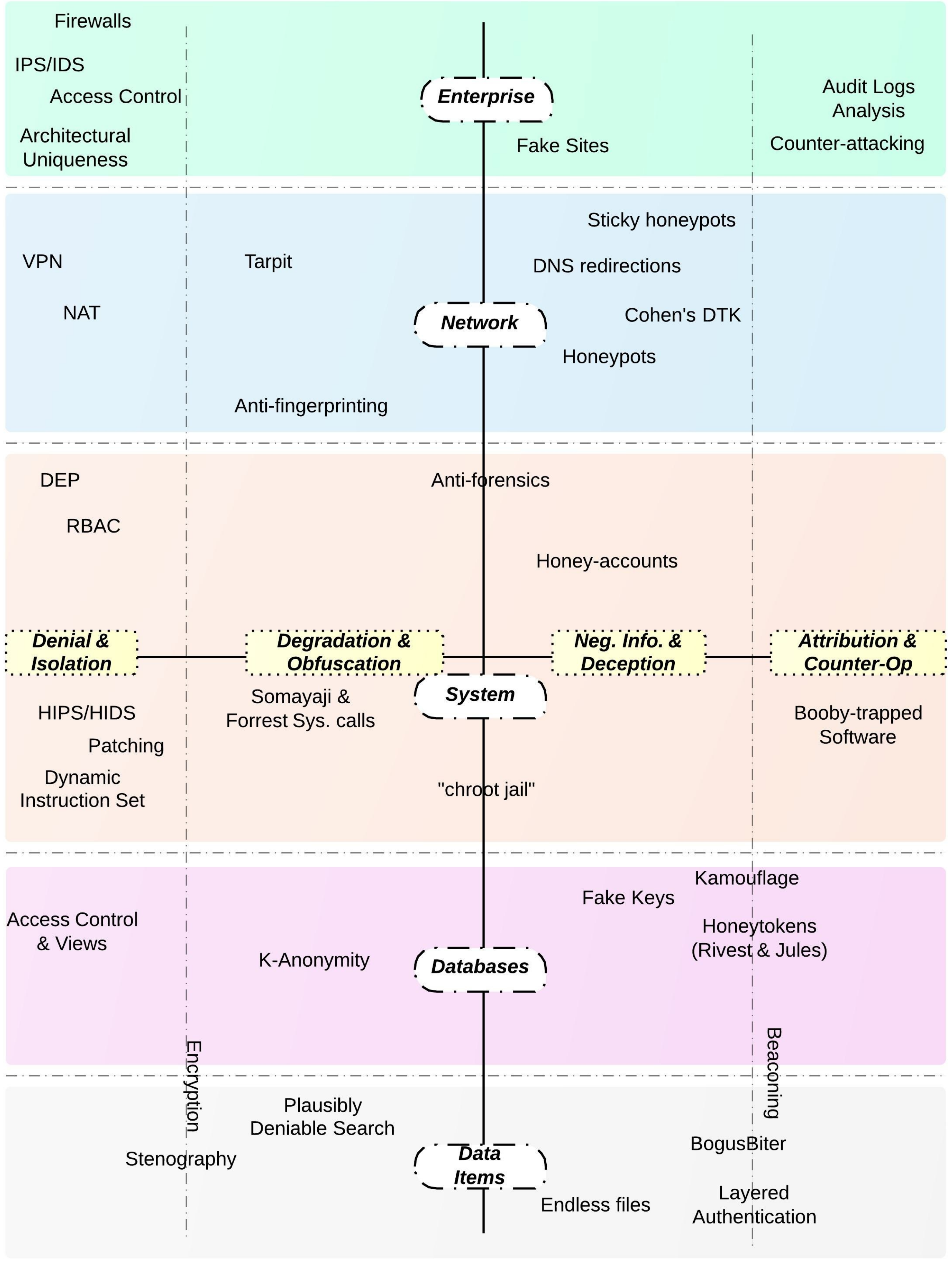
-> Prevent unauthorized access.
-> Hide the existance/nature of systems/data.

-> Slow down adversaries.
-> Reduce the prob. of recovering the data.
-> Obfuscate value/nature.
-> Create noise to reduce utility.

-> Lead adversaries astray.
-> Add decoys and beacons.
-> Add risk and doubt.

->Adversaries Attribution.
-> Causing damage to adversaries.
-> Increasing the overall risk of an attack

Protection Mechanisms Plotted across a Data Scale



Mapping Protection Mechanisms against the Kill-Chain

	Denial & Isolation	***Degradation & Obfuscation***	***Deception & Negative Information***	***Attribution & Counter Operations***
Reconnaissance	Firewalls, Architectural Uniqueness, NAT	Anti-fingerprinting	Artificial ports, Fake Sites	Audit Logs Analysis
Weaponization & Delivery	In-line Filters, IPS, Tarpit, IDS		Create artificial bouncing back, Sticky Honeypots	
Exploitation & Installation	Dynamic Instruction Set, Somayaji & Forrest sys. calls, HIPS, Patching, DEP, "chroot jail", HIDS		Create artificial exploitation response	
Command & Control (operation)			Honeypot	
Lateral Movement & Persistence	VPN, Access Control, RBAC	Encryption, Self-Encryption	HoneyAccounts, HoneyFiles	
Staging & Exfiltration		Stenography	Honeytokens, Endless files, Fake Keys	Beaconing, Counter-Attacking, Booby Trapped Software