MITRE | The MITRE Center for Technology & National Security

THE CYBERSPACE ADVANTAGE: INVITING THEM IN!

How Cyber Deception Enables Better Resilience

By Deborah L. Schuh

This page intentionally left blank.

The Cyberspace Advantage: Inviting Them In!

How Cyber Deception Enables Better Resilience

Cyber resiliency: "The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources." – National Institute of Standards and Technology (NIST) Special Publication 800-160, Volume 2 (draft)

Building systems that are highly resilient to the cyber threat means employing techniques and technologies that adversaries are unable to anticipate, navigate through, or successfully attack. One option is embedding systems with special-purpose hardware, operating systems, and software, to create a "special sauce" that is unique to that system and not exposed to the adversary. Making systems highly resilient can also mean employing techniques listed in the NIST document, such as non-persistence and diversity. While these mechanisms can limit the adversary's ability to establish a foothold in our most critical assets, there is an often-overlooked approach to cybersecurity that can yield both short- and long-term benefits.

Incorporating deception into cyber defenses can be used to detect malicious actions, manage adversaries once they are inside and collect intelligence about their tactics and techniques. Cyber intelligence derived from deception can better inform defense and resilience.

What Boeing's 787 Code Leak Can Tell Us About Creating Asymmetric Advantage

On July 7, 2019, WIRED reported on the controversy surrounding a cyber researcher's discovery of an unprotected Boeing network server. In September 2018, cybersecurity researcher Ruben Santamarta was poking around the internet for airliner information and happened across Boeing's server, where the software for the 787 Crew Information Service/Maintenance System was hosted. Santamarta then publicly exposed the fact that an unprotected server was accessible to hackers and that the software had serious security flaws.

Most readers of this article might have been concerned with the quality and security of Boeing's 787 airliner and the potential for cyber incidents. But what if the researcher had stumbled across an intentional release of older, now invalid, design information intended for an advanced cyber threat actor to collect – as Boeing watched and surveilled? Even if that isn't the case in this story, it is something to seriously consider as part of an overall cyber strategy.

Many years ago, The MITRE Corporation faced a conundrum when we discovered an advanced cyber threat (also known as an advanced persistent threat or APT) inside our own network. MITRE used that as

an opportunity to learn more about the adversary's methods and tactics. We created an environment where staff watched and collected data on the APT's behavior and techniques as they moved around the environment. As a result, we learned valuable information about the adversary; information we could then share with other organizations for defensive purposes. And we did share, but since there had been no public reporting of a cyber incident or intrusion at The MITRE Corporation, some questioned how MITRE came to learn this information about the adversary's behavior. Thus began our foray into the realm of cyber deception.[1]

What is New About Cyber Deception?

While the basics of cyber deception (i.e., honeypots, honeynets, honeytokens, etc.) have been around for several years, the art of true deception is growing as organizations seek to better understand adversary methods and patterns of behavior. There is an emerging and rapidly growing commercial marketplace providing tools and expertise for deception.

Current technology enables rapid creation of deception environments within existing infrastructure and connected to existing cyber defense mechanisms (i.e., intrusion detection systems). For example, organizations can now create sophisticated deception environments that intentionally lure adversaries in, with fake users and credentials, false or misleading information valuable enough to keep intruders active and engaged, and a network for them to navigate through; all in a controlled environment allowing observation. Cyber deception products and expertise are more available and affordable than ever before.

Basics of Cyber Deception

Honeypots, honeynets, honey tokens, and pocket litter are all terms for computer resources and information assets specifically created to be less secure and attractive to potential cyber attackers. They can be deployed separately or together in what is called a "deception environment." The idea is to create a parallel universe to your internal systems and networks to distract and divert adversaries into a controlled environment where you can contain and observe them.

Honeypots are host computers (a web server, a file server, etc.) configured to entice attackers to navigate the host, steal and exfiltrate data, or further investigate the target network.

Honeynets are networks made up of multiple honeypots. The honeypots and the honeynet are all configured to emulate an actual network such that attackers believe they have successfully infiltrated a real network environment.

Honeytokens are fake data (a document, a URL, etc.) or credentials – not visible to normal users – which, if accessed, are an indication of malicious activity. They are normally used as an alert mechanism.

Pocket litter is information intended to simulate users on the honeynet with associated documents, accounts, web browser history, etc., to instill a sense of reality to the deception environment. The more realistic the pocket litter, the more likely the attacker will believe they are in a real network.

[1] For more information, read Cyber Denial, Deception and Counter Deception: A Framework for Supporting Active Cyber Defense, Kristin E. Heckman et al., Springer International Publishing, 2015.

"All warfare is based on deception.

When able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near."

-Sun Tzu

The Value of Cyber Deception

As the Defense Science Board and Government Accountability Office have made clear in many reports, the Department of Defense (DoD) still struggles with implementing cybersecurity and resilience in weapons and enterprise systems. It is becoming evident that traditional approaches to security are no longer adequate. Deception provides an opportunity to gain important knowledge and advantage on adversaries. The benefits are many

1. Finding and managing adversaries. Current commercial deception tools offer automation that can alert to malicious behavior – with low false-positive returns. The adversary then can be contained or lured toward intentional targets.

2. Learning adversary techniques to better inform defense. Observing and capturing adversary methods and techniques is invaluable for building better cyber defense and resilience. It can also improve deception to the point of sensing the environment in ways that can expose adversary identity.

3. Finding insider threats. Deception techniques used to detect external adversaries also enable detection of internal malicious threats. Deception environments are configured to alert to suspicious behavior in any form, since they are based not on patterns but on presence.

4. Better incident response. Alerts and observations are combined to create a clearer view and understanding of what is happening in the environment. This enables a more efficient and effective response.

5. Deceiving the adversary. Judicious use of networks, pocket litter, and honeytokens can waste the adversary's time and resources, expose their pedigree, and create false knowledge on their part. Deception can also add randomness and unpredictability to an architecture, network traffic, service, or mission activity, making an adversary's understanding of the environment more challenging and at best inaccurate.

In the military domain, sophisticated deception environments can be used in very deliberate ways to achieve higher level military objectives.

Increasing Return on Investment by Sharing Knowledge

Knowledge gained through deception and observation should be shared rapidly among similar classes of systems across the DoD. Following the path of anti-tamper,[2] where everything is intentionally classified and not shared, is not useful or prudent when it comes to dealing with cyber threats, as cyber threats manifest themselves differently. They are instantaneous, morphing, malicious, and pervasive. Holding back valuable intelligence about the adversary's tactics, techniques, and procedures (TTPs) puts the DoD at a disadvantage. The cyber landscape is changing so frequently, and the threat is so pervasive, that timely sharing of adversary operations is the only way to stay abreast of threats and enable better defense across the enterprise.

[2] Anti-tamper technology applies mechanisms that prevent or slow unauthorized reverse engineering of sensitive electronic equipment, computers, software, and other technologies critical to creating U.S. military advantage.

Standards and frameworks exist to enable cyber threat information characterization and sharing (CAPEC™,[3] STIX™,[4] TAXII™,[5] ATT&CK™,[6] and NTCTF[7]). Built mostly to handle information technology-based cyber attacks, these standards are being extended to accommodate the characterization of adversary TTPs within weapons and embedded systems (also referred to as cyber-physical systems). These extensions enable better threat understanding, information sharing, and defense of those unique types of assets.

Better Defense of Our Most Critical Assets

The DoD should combine threat information derived from cyber deception with other cyber intelligence to inform better defense of critical assets.

As a minimum, deception should be deployed strategically across the DoD enterprise, particularly in systems of known adversary interest or intent. The full capabilities of deception should be employed, and the DoD should use the knowledge obtained to continually improve defense and the deception itself.

In parallel, the DoD needs to harden the assets that are most critical to multiple missions and to the enterprise. These are the assets providing common components and capabilities underlying many operational systems and missions. Components like those providing positioning, navigation, and timing; communications; internal busses; radios; programmable logic controllers; engines; and other critical functions would all benefit from hardening.

While hardening every major weapon system is not cost-effective, hardening shared critical components is.

Hardening components requires investment to develop highly resilient technologies embedded in these devices, working directly with the vendors. It also means uniquely developing special-purpose hardware and software that will not be accessible to the adversary. This investment cannot be tied to existing programs of record, but must be managed and funded at an enterprise level to be effective and efficient.

The DoD should question the heavy reliance on commercial off-the-shelf (COTS) components, which are also accessible to adversaries. National defense cybersecurity mission importance must be part of the equation when evaluating COTS solutions. COTS components are more appropriate for common infrastructure, business systems, “and general computing (along with associated cybersecurity and deception products) than for weapon systems.

The commercial marketplace is not as strongly driven by an ongoing sophisticated cyber “war” as the DoD should be. It is not a visible conflict to the public as World War II was. The conflict is visible, however, to the defense industrial base (DIB), which must be an effective partner in developing hardened and resilient components. The DIB has also faced years of persistent exfiltration of intellectual property and military data by the APT and can be an effective partner in deploying deception.

[3] Common Attack Pattern Enumeration and Classification (CAPEC™) provides a comprehensive dictionary of known patterns of attack employed by adversaries to exploit known weaknesses in cyber-enabled capabilities.
[4] Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence. STIX enables organizations to share threat information with one another in a consistent and machine-readable manner.
[5] Trusted Automated Exchange of Intelligence Information (TAXII™) is an application-layer protocol for communicating cyber threat information as represented in STIX. Visit https://oasis-open.github.io/cti-documentation/ for more on STIX and TAXII.
[6] MITRE ATT&CK™ is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. https://attack.mitre.org/
[7] NSA/CSS Technical Cyber Threat Framework (NTCTF) is a National Security Agency standard for characterizing adversary activity with a common technical lexicon closely aligned with industry definitions. This common technical cyber lexicon supports sharing, product development, operational planning, and knowledge-driven operations across the Intelligence Community.

What Does Success Look Like?

The DoD and DIB need to continually improve defenses and become more cyber resilient. This will take new ideas, new strategies, and new ways of partnering to succeed.

1. The DoD should strategically deploy deception across DoD systems and the DIB. By doing this well, they will gather valuable knowledge about the adversary and allow for better defense through adversary containment and management.

2. Sharing the intelligence gained from the various deception environments with communities of like systems will improve the collective understanding of both adversary techniques and effective defensive measures.

3. The degree to which systems employ COTS should be re-evaluated and adjusted. Part of the equation should be a look at the amount of data that has already been exfiltrated and other information available to an APT. This will help determine the protections needed for cybersecurity and resilience.

4. Hardening critical common components across the DoD enterprise will raise the bar for many systems and must be done by working directly with component vendors.

Changing the balance of power in cyber defense is hard. Acquiring more knowledge about the adversary, effective sharing of cyber threat intelligence, and better protection and resilience for the assets most critical to national security will all contribute to success.

About the Author

Deborah Schuh is a Director of Cyber Integration within the Cyber Strategy and Chief Security Office of The MITRE Corporation. She applies cyber, systems engineering and operational expertise to some of the defense department's hardest challenges in cyber.

About the Center for Technology & National Security

MITRE launched the Center for Technology and National Security (CTNS) to provide national security leaders with the data-driven analysis and technologically informed insights needed to succeed in today's hyper-competitive strategic environment. The Center aims to help policymakers better navigate a dynamic, rapidly evolving technology landscape in order to advance U.S. interests and strengthen national security. As a part of the not-for-profit, non-partisan MITRE Corporation, CTNS is built on the experience and expertise of thousands of our nation's most respected scientific and engineering minds. The Center brings together experts and leading authorities from government, academia, industry, media, and policy institutes to drive informed discussion in this era of unprecedented technological change.

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

MITRE Center for Technology and National Security