Brought to you by

ACALVIO

Deception 2.0

for dummies®
A Wiley Brand

Acalvio Special Edition



Blend Deception and data science

Deceptions across public and private clouds

Deceptions in IT, ICS/SCADA, and IoT

Team Acalvio

About Acalvio

Acalvio is a leading provider of deception-based Advanced Threat Defense (ATD) solutions to detect, engage and respond to malicious activity within enterprises. ShadowPlex™, Acalvio's next-generation distributed deception solution, provides completely automated, pervasive deception on an enterprise scale. ShadowPlex is anchored on Deception 2.0 technologies — patented innovations in Deception and its interplay with artificial intelligence (AI). Acalvio complements its threat analytics with data from customer and partner ecosystems, enabling customers to benefit from defense in depth, reduce false positives, and derive actionable intelligence for remediation.

Acalvio's solutions are architected for application in Enterprise IT, ICS/SCADA, and IoT environments.

ShadowPlex addresses the Threat Defense Life Cycle: Detect → Engage → Respond in a comprehensive manner. ShadowPlex *detects* advanced, multistage attackers with precision and speed and *engages* with adversaries in a Shadow Network to understand tools, techniques, and procedures (TTPs) to delay impact to assets and take corrective actions. Finally, ShadowPlex *responds* by identifying attacker trajectory, understanding latent vulnerabilities in the network and generating indicators of compromise (IOCs) to trigger remedial and preventive actions. Acalvio's solution employs a very rich and expansive palette of deception artifacts — decoys, lures, and breadcrumbs. Acalvio's AI engine recommends the deployment and makeup of decoys. In addition, it includes smart blending of data and credential breadcrumbs across enterprise servers and endpoints. These breadcrumbs both detect data theft and redirect attacks to Fluid Deception™ for engagement, thereby providing more actionable security intelligence to enterprises.

ShadowPlex is built for enterprise and IoT scale. Deception 2.0 enables a Devops approach to Deception, which allows for high efficacy at any scale and maintains ease of deployment and management. Deception 2.0 affords flexible deployment options — on-premises, Private Cloud and Public Cloud (AWS, Azure, and GCP).

Acalvio, based in the Silicon Valley, is led by an experienced team with a track record of innovation and market leadership and backed by marquee investors. For more information, please visit **www.acalvio.com**.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.



Deception 2.0

Acalvio Special Edition

by Team Acalvio

for dummies®
A Wiley Brand

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Deception 2.0 For Dummies®, Acalvio Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

Copyright © 2017 by John Wiley & Sons, Inc., Hoboken, New Jersey

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

Trademarks: Wiley, For Dummies, the Dummies Man logo, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

ISBN 978-1-119-36652-2 (pbk); ISBN 978-1-119-36646-1 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Development Editor: Elizabeth Kuball

Copy Editor: Elizabeth Kuball

Acquisitions Editor: Amy Fandrei

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Production Editor: Magesh Elangovan

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Introduction

Since the beginning of time, deception has been used in nature and warfare as a powerful defense mechanism. Deception is a very useful and effective tactic to detect and evade threats in many situations. The modern cybersecurity situation is one such example.

Cybersecurity breaches are active on enterprise networks for an average of 200 days before they're discovered. Once inside your network, attackers pivot to other systems and networks, stealing valuable and sensitive data with impunity.

Unfortunately, traditional network and endpoint prevention technologies are too little, too late. The rapid rise of cloud computing, the proliferation of mobile technology, and the spread of Internet-facing applications have all scorched the notion of firewalls providing security at the network perimeter.

Cyber warfare today requires an effective solution to detect, engage, and respond to malicious activity on enterprise networks using many of the same principles of warfare espoused by Sun Tzu in *The Art of War*, including the use of deception to learn the tactics of your adversaries and crush them!

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

About This Book

This book explains cybersecurity deception concepts and technologies in six short chapters covering

- How the modern cyber threat has evolved and how deception can break the cyberattack life cycle (Chapter 1)
- Why prevention technologies alone aren't enough to protect enterprise networks and how honeypots can help (Chapter 2)
- Which innovations define advanced second-generation deception technologies (Chapter 3)
- How to create an enterprise deception strategy (Chapter 4)
- Where and how to deploy a deception architecture (Chapter 5)
- What to look for in an effective deception solution (Chapter 6)

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but we assume a few things nonetheless.

First, we assume you're a politician.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Just kidding! We assume you're an IT executive, manager, or professional, and you're responsible for securing your enterprise network. As such, we assume that you're a somewhat technical reader with at least a basic knowledge of networking and security concepts and technologies. But if you're a nontechnical reader, fear not. We spell out any technical acronyms used in the book and promise not to get too technical.

If any of these assumptions describes you, then this book is for you! If none of these assumptions describes you, keep reading anyway. The title will intrigue others that see you reading it, and you'll learn a lot about deception — for cybersecurity.

Icons Used in This Book

Throughout this book, we occasionally use icons to call out important information. Here's what to expect:


REMEMBER

This icon points out information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays!


TECHNICAL STUFF

You won't find a map of the human genome or the secret to cold fusion here, but if you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.



TIP

Tips are always appreciated, never expected — and we sure hope you'll appreciate these tips! This icon points out helpful suggestions and useful nuggets of information.



WARNING

This icon points out the stuff your mother warned you about (well, probably not). But these helpful alerts do offer practical advice to help you avoid potentially costly and frustrating mistakes.

Beyond the Book

There's only so much we can cover in 64 short pages, so if you find yourself at the end of this book thinking, "Gosh, this is an amazing book. Where can I learn more?," just go to `www.acalvio.com`.

Where to Go from Here

With apologies to Lewis Carroll, Alice, and the Cheshire cat:

"Would you tell me, please, which way I ought to go from here?"

"That depends a good deal on where you want to get to," said the Cat — er, the Dummies Man.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

"I don't much care where . . . ," said Alice.

"Then it doesn't matter which way you go!"

That's certainly true of *Deception 2.0 For Dummies,* which, like *Alice in Wonderland,* is also destined to become a timeless classic!

If you don't know where you're going, any chapter will get you there — but Chapter 1 might be a good place to start! However, if you see a topic that piques your interest, feel free to jump ahead to that chapter. Each chapter is written to stand on its own, so start reading anywhere. We promise you won't get lost falling down the rabbit hole!

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Surveying the cyber threat landscape
- Breaking the attack life cycle
- Looking at deception in nature, war, and security

Chapter 1

The Truth about Deception in Cyber Security

The Internet is the new battlefield of the 21st century with information warfare becoming as prevalent, devastating, and potentially lethal, as more traditional forms of warfare. In this chapter, we explain the role of deception in modern information warfare.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Recognizing the Modern Cyber Threat

Despite a generally greater awareness of cyber threats and a renewed focus on IT security, the number and scale of successful cyber attacks continues to grow at an alarming rate. The Identity Theft Resource Center and CyberScout recently reported a record 1,093 data breaches in the United States in 2016 — a 40 percent increase over the near-record high reported in 2015. The Ponemon Institute's 2016 *Cost of Data Breach Study: Global Analysis* estimated that the average total cost of a data breach in 2016 was $4 million and Juniper Research predicts that cybercrime will cost $2.1 trillion globally by 2019, averaging $150 million per breach by 2020.

Hardly a month goes by without some news story about a massive data breach affecting millions of victims, and many enterprises have already been compromised — they just don't know it yet. The 2016 *Verizon Data Breach Investigations Report* found that nearly 70 percent of threat actors go undetected in victim enterprise networks — stealthily exfiltrating valuable information assets (such as sensitive customer information, credit card data, and intellectual property) — for days, weeks, or months.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Understanding the Kill-Chain Model

The Law Enforcement Cyber Center uses the following "kill-chain" model (see Figure 1-1) to define the cyber attack life cycle, as follows:

1. **Perform initial reconnaissance (recon).**

   The attacker identifies systems and determines operating systems, security, applications, protocols, addresses, and other runtime characteristics.

2. **Make initial compromise.**

   The attacker uses an exploit or attack to probe and break through the system's defenses. This compromise could be achieved through social engineering, phishing, or other means.

3. **Establish a foothold.**

   The attacker establishes or creates persistence on a system, perhaps by installing a backdoor or installing utilities or malware to maintain access.

4. **Escalate privileges.**

   The attacker gains greater access to systems and data by obtaining credentials, leveraging privileges belonging to an application or service, or exploiting vulnerable software.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

5. **Perform internal recon.**

   The attacker explores other systems and networks to map the entire environment, identify the roles and responsibilities of key staff, and locate interesting or valuable data.

6. **Move laterally.**

   The attacker jumps from system to system on the network, using network shares, scheduled tasks, and remote access tools or clients.

7. **Maintain a presence.**

   The attacker maintains ongoing access and activity on the systems and networks. This may involve using backdoors or remote access tools.

8. **Complete the mission.**

   The attacker achieves his attack objectives, such as stealing intellectual property (IP), classified information, financial data, or personally identifiable information (PII).


TIP

There are numerous variations of this model, such as the Lockheed Martin Cyber Kill Chain and others, that roughly approximate the different attack stages described here.

For a cyber attack to be successful, the attacker must successfully execute all eight stages of the cyber attack life cycle. Thus, the key to preventing a successful cyber

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

attack is to thwart the attack at any phase, or break the chain, in the life cycle — hence, a "kill-chain" model.

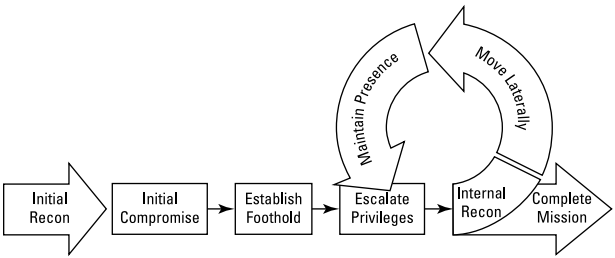


FIGURE 1-1: The cyber attack life cycle.

Discovering the Science and Art of Deception

Evolution has often relied on deception as a survival technique. For creatures with higher cognitive abilities, the capability to deceive is linked to creativity. (Try explaining that to your significant other!) The same cognitive skills that enable imagination are used to tell a successful lie. The inventiveness of mankind has further improved upon nature's design and made deception an art. To quote the Roman philosopher Cicero, "Art is born of the observation and investigation of nature."

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Deception in nature

In nature, every organism is driven to survive and propagate. Deception has been employed in various forms as a successful strategy and has played an important role in the physical and behavioral adaptations of all organisms. As psychologist Harriet Lerner observed, "Deception and 'con games' are a way of life in all species and throughout nature. Organisms that do not improve their ability to deceive — and to detect deception — are less apt to survive."

The following few examples illustrate a variety of deceptions in nature:

- **Western skunk cabbage** emits a scent like that of skunk spray to draw in its pollinators — scavenging flies and beetles.
- **Rye** used to be a weed in wheat fields, until it began mimicking the qualities of wheat, and even surpassing it in some areas, through a phenomenon called Vavilovian mimicry.
- **Lamium albium,** known as "dead nettle," evolved to look just like stinging nettle. It doesn't have the same painful sting, but it gets the same benefits by association and often grows near its doppelganger.
- **Angler fish** have a long filament on top of their head that they can wiggle to resemble a prey animal so they can lure other predators close.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Mimic octopi** can mimic up to 15 species of local marine organisms as a primary defense mechanism.



REMEMBER

So, what can we learn about deception from nature? Well, deceptions in nature are

- **Varied:** There are literally thousands of examples of deception.
- **Specialized:** Each type of deception works only for a specific species, in a specific environment, for a specific threat or opportunity.
- **Dynamic:** The arms race between predator and prey keeps throwing up newer deceptions as opponents evolve to circumvent previous deceptions.

Deception in warfare

Deception has always been a strategic component of warfare. In Sun Tzu's *The Art of War*, deception is a key principle of warfare. Throughout history, different ploys have been used to draw an adversary into a weak position, or to defeat or completely rout an enemy.

Various types of deceptive tactics have been employed throughout the history of warfare, such as the following:

- **Feigned retreat:** Leading the enemy, through a false sense of security, into a prepositioned ambush.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

In ancient times, Hannibal used this tactic to make it appear that the center of his lines was withdrawing, and then folded his flanks onto the Roman army as it advanced toward the deceptively weak center.

- **Fictional units:** Creating entirely fictitious forces or exaggerating the size of an army. In the Battle of Megiddo during World War I, allied forces used 15,000 dummy horses (or horses for dummies?) to deceive the Ottomans and prevent them from withdrawing to the coast.
- **Smoke screen:** Using smoke, fog, or other obscurations to hide battlefield movements. Smoke screens have been used throughout history in land and naval warfare.
- **Strategic envelopment:** Deploying a small force to distract the enemy while a much larger force moves to attack from the rear. This was a favored tactic of Napoleon Bonaparte.
- **Trojan horse:** Gaining admittance to a fortified area under false pretenses to later admit a larger attacking force. The most famous example is the ploy used by the Greeks to enter Troy.



REMEMBER

As in nature, there are several important lessons about deception that we can learn from warfare. A successful deception in warfare is always the result of an extremely well-orchestrated and well-executed plan, and depends on the following:

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Secrecy:** The deception must blend into the environment. When dummy horses were used at the Battle of Megiddo, real horses were walked to the nearest water source multiple times a day to complete the illusion.
- **Originality:** The same deception can't be used multiple times nor is it appropriate in all circumstances.

Deception in cyber security

As the modern battlefield has been extended to cyberspace, so, too, have warfare tactics — including deception. Deception was employed in one of the earliest known and most notorious cases of phone hacking, or "phreaking." In 1971, John Draper (now known as "Captain Crunch") used a toy whistle from a box of Cap'n Crunch cereal to emulate the 2,600 hertz (Hz) tone of AT&T long lines that indicated when a trunk line was ready and available to route a new call. This deception enabled hackers to make free long-distance calls.

Table 1-1 summarizes key events in the history of deception and honeypots (discussed later in this chapter) in cyber security, as summarized in Lance Spitzner's 2002 book, *Honeypots: Tracking Hackers.*

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

TABLE 1-1 **Deception in Cyber Security**

Year	Event
1990–1991	Cliff Stoll's *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage* (see the sidebar, "*The Cuckoo's Egg:* An 'over easy' synopsis") and Bill Cheswick's *An Evening with Berferd* are published.
1997	Version 0.1 of Fred Cohen's Deception Toolkit (DTK) is released.
1998	Development begins on CyberCop Sting, a pioneering honeypot product that uses multiple virtual systems tied to a single honeypot.
1998	BackOfficer Friendly, a free Windows-based honeypot, is released,
2000–2001	Honeypots are used to capture and study Internet worm activity.
2002	Honeypots are used to detect attacks in the wild, such as Solaris *dtspcd.*

THE CUCKOO'S EGG: AN "OVER EASY" SYNOPSIS

In his 1989 nonfiction bestseller, *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage,* author Cliff Stoll recounts his year-long cat-and-mouse pursuit of a German hacker.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

On his second day as a systems manager at Lawrence Berkeley Lab (LBL), Stoll began investigating a seemingly trivial 75-cent accounting error in a Unix-based billing system. His investigation led to the discovery of a "dormant" account that was being used by a hacker.

To track the hacker's activity without being detected, Stoll physically wired four dozen teletypes and portable terminals to each of the system's modem lines to record every keystroke sent across the network. At this point, you may be thinking, "That's an awful lot of work to track down a two-bit [it was actually 75 cents, so more like 6 bits] thief," but the accounting error was merely a clue. The hacker was using LBL's powerful computers to breach military and defense contractor systems and steal valuable classified information.

Stoll worked with German authorities to set a sophisticated trap for the hacker. He created a trove of fake documents with official-sounding terms like *nuclear* and *SDI* to entice the hacker. At this point, the hacker, of course, had no chance. SDI referred to U.S. President Ronald Reagan's Strategic Defense Initiative, popularly known as "Star Wars." So, whether the hacker

(continued)

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

(continued)

thought he was stealing plans for a space-based missile defense system or the dark truth about Luke Skywalker's daddy issues, he was hooked (and just in case the hacker was more of a *Weird Science* fan, Stoll also created a fake secretary)!

The hacker fell for the trap and downloaded the files over his blazing 1,200-baud connection, which took a couple of hours — enough time for the German Bundespost to trace the hacker and arrest him. (Just to be certain, Stoll jingled his keychain across the modem lines to cause noise-generated errors and slow down the transmission.)

Stoll's story is one of the first documented cases of a sophisticated computer attack (though the hacker's methods themselves weren't that sophisticated) and illustrates many important uses of deception in detecting, understanding, and responding to such attacks.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Following the cyber doctor's orders (not exactly)
- Attracting (and distracting) flies with honeypots
- Recognizing the limitations of honeypots

Chapter 2

Deception 1.0: The Inception of Deception

In this chapter, we look at how honeypots can supplement traditional perimeter defenses, explain the pros and cons of low- and high-interaction honeypots, and explore some enterprise challenges inherent in first-generation deceptions.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

An Ounce of Prevention Isn't Enough

The proverbial "ounce of prevention" no longer suffices to keep the bad guys safely at bay. Prevention technologies — such as access controls, email gateways, intrusion detection/prevention systems (IDS/IPS), network firewalls, proxy servers, and web application firewalls (WAFs) — are important foundations of cyber security, but they aren't enough.

The traditional network perimeter — where many of these prevention technologies are typically deployed — has become porous and is routinely being breached. Proliferation of cloud computing, mobility and bring your own device (BYOD), and Internet-facing applications has rendered these perimeter defenses largely ineffective.

Threats inside the Network

Solutions to detect threats inside the network are either anomaly based or deception based.

Anomaly-based detection

Anomaly-based detection creates a behavior baseline of various network components — hosts, data access,

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

network traffic, user behavior, and so on. Any activity that is inconsistent with the baseline is flagged as an alert.

Anomaly-based solutions have two significant drawbacks:

- Capturing, storing, and distilling the data lake is complex, expensive, and time consuming.
- False positives occur at a high rate, adding a significant burden to overloaded security teams.

Deception-based detection

Deception-based detection provides an effective alternative to anomaly-based detection. Any component in an enterprise network — a computer system, a service, a credential, a data item, and so on — can be used for deception-based detection. The deceptions are not part of the normal operations of the business or network and are revealed only by an attack. When an intruder expends the time and effort to locate and access a deception that is set up specifically to invite attack, it is a positive affirmation of a compromise. In other words, in a deception-based solution, a highly positive anomaly announces itself.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Heffalumps and Honeypots

In case you didn't have the privilege of enjoying A.A. Milne's *Winnie the Pooh* while growing up — or you've repressed those memories — a *Heffalump* is an imaginary, primitive creature that tries to steal Pooh's honey.

Honeypots are the mainstay of the first iteration of deception-based detection. A *honeypot* is a computer system that is not part of the normal enterprise network or systems. Theoretically, no one in the organization should be interacting with a honeypot. Honeypots come in two varieties — low interaction and high interaction — depending on how an adversary is engaged.

Low-interaction honeypots

Low-interaction honeypots are based on emulations of pieces of the operating system, or the network stack, and any needed services. These honeypots are relatively easy to set up, and the emulations are not resource intensive. The main advantages of low-interaction honeypots are

- A single computer can effectively emulate many honeypots.
- The emulations do not allow an adversary to gain access to the system, thereby avoiding any risk of the honeypots themselves being compromised.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

However, low-interaction honeypots are limited to capturing known activity using a relatively limited set of emulations. An enterprise network usually has many complex systems offering a variety of services. Even a basic service, such as File Transfer Protocol (FTP), usually has many versions and the same version may be implemented a little differently (such as customized greeting banners) on various systems. Low-interaction honeypots offer only a standard set of network services and the simplicity of the emulations (for example, canned responses, incomplete emulations, and so on) makes it easy for adversaries to fingerprint and bypass them.

High-interaction honeypots

High-interaction honeypots are actual systems, rather than emulations. They're identical to normal enterprise systems, running actual operating systems, offering real services — and potentially allowing login access to attackers. However, any data in a high-interaction honeypot is fake, and the operating system and services are instrumented to capture a detailed account of the attacker's actions on the system. The honeypot is also usually wired to capture all network traffic, thus providing detailed attack data that can help understand an attacker's intentions, what systems are compromised, which exploits are used, and how command-and-control (C2) infrastructure is setup.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

The disadvantages of high-interaction honeypots are that they're costly (because they're real systems) and hard to configure, deploy, and maintain. Significant effort is required to change the nature of a high-interaction honeypot, for example, to provide an upgraded operating system, modify the services, or create fake data. Because the attacker is allowed access to the honeypot, there is also a risk that the honeypot may be compromised and used to launch attacks against other systems or networks. However, for an enterprise that needs to understand targeted attacks and mount a proper defense, there is no better alternative to high-interaction honeypots.

Limitations and Exclusions Apply

The first generation of deception technologies — honeypots — were successful in demonstrating the effectiveness of deception as part of a layered security strategy. Open-source projects, especially *Honeyd* and *Honeynet,* allowed organizations to experiment with honeypots. However, the need for enterprise-grade deception solutions brought up several challenges with this first iteration, including the following:

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Low interaction *or* high interaction:** Enterprise deception solutions need both scale and the ability to provide a detailed understanding of attacks.
- **Emulation-based low interaction:** The simplicity of emulations makes them easy to fingerprint. In addition, developing and customizing emulations to match the breadth and characteristics of the services in every organization is a huge task.
- **Static honeypots:** First-generation honeypots exhibit distinct characteristics that never change and many open-source solutions have well-publicized fingerprints. This enables attackers to easily fingerprint and identify these honeypots.
- **Ease of use:** Honeypots were not designed for large enterprises, making administration at scale impractical. Even if setting up a honeypot took only a minute, setting up a thousand honeypots would take more than 16 hours! Maintaining honeypots was nearly impossible, and attackers could easily identify them because they were static.
- **Honeypots are the only deception type:** Effective deception should be in every part of the enterprise network and must extend to files, emails, cached credentials, network shares, databases, routers, printers, and so on.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Stand-alone product:** Honeypots are mostly stand-alone products and do not interact with the security ecosystem typically present in any enterprise network.
- **Threat analysis:** High-interaction honeypots are used primarily to capture malware payloads, though there have been some advances to study attack patterns and identify C2 infrastructure.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Mitigating advanced threats with deception
- Building a tackle box of deception tools
- Using Fluid Deception for depth and scale
- Getting agile with DevOps for deception

Chapter 3

Deception 2.0: The Next Generation of Deception

In this chapter, you learn about the next generation of deception technologies: Deception 2.0.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Detecting, Engaging, and Responding to Advanced Threats

Effective mitigation of advanced threats requires a detailed understanding of the tactics, techniques, and procedures (TTPs) of the threats. Deception solutions must interact with threats at three levels to provide effective detection and mitigation:

- **Detect:** Any access to a deception reveals a threat with a high degree of confidence. The deception could be a fake privilege inserted in an endpoint, a fake network share, a honeypot server, or any mimicked resource.
- **Engage:** When a threat is detected, deception enters the engage phase and starts interacting with the threat to gather information. The engage phase collects detailed threat TTPs, specifically the payload, lateral movement exploits, command-and-control (C2) centers, accounts compromised, and the attack objectives.
- **Respond:** Understanding the attacker's techniques and objectives helps to both impede the attack progress and close all exploits. This requires

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

automated intelligence to correlate the threat TTPs collected in the engage phase and devise an appropriate response strategy. For example, shutting down access to the external exfiltration sites can be a typical response.



WARNING

An emulation-based low-interaction honeypot can only do detection. It cannot identify all the TTPs used. Engagement is necessary to completely eliminate a threat.

A *detection system* focuses on finding intruders or malware that have circumvented traditional perimeter defenses. Detection does not replace perimeter defenses, but rather provides an additional layer of protection.

Think of this concept like your home. You no doubt have locks on the exterior doors, but you might also use motion sensors to detect unwanted intruders inside your home. Like motion sensors, detection solutions provide visibility to unauthorized and dangerous activity inside your network.



TECHNICAL STUFF

Deploying a detection system *inside* your network represents a paradigm shift from traditional "full trust" enterprise network models, in which organizations have limited visibility of unusual or unauthorized activity once users gain access. Even "zero trust" network models that enforce access controls

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

between different network segments (or zones) typically provide limited visibility within the individual network segments.

Using Pervasive Deception

Deception takes many forms to detect and engage threats at every step of the kill chain (discussed in Chapter 1). Deceptions can be broadly divided into four types:

- **Decoys:** A decoy is a fabricated system or a software service that presents an attractive target to an attacker. A honeypot is a type of decoy. Other types of decoys include routers, printers, database services, and more. A decoy is usually more tempting to an attacker than production network neighbors, because it is seeded with interesting (but fake) data and known vulnerabilities are left open.
- **Breadcrumbs:** Breadcrumbs are used to lead an attacker to a decoy. They're important because the initial compromise is usually an enterprise endpoint. When an attacker does reconnaissance, breadcrumbs on the endpoints and in the network point to decoys as interesting targets.
- **Baits:** Baits are honey tokens — for example, counterfeit data or fake credentials to a service — which the attacker finds valuable. Baits are carefully

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

laid so that ordinary IT procedures or normal user behavior does not touch them. An attack can be detected by monitoring the access or usage of the bait.

- **Lures:** A lure makes a decoy, a breadcrumb, or a bait more attractive than the actual enterprise network assets. For example, to make a software service decoy attractive, it can be set with factory default credentials. A file used as bait may contain fabricated financial data.

Pervasive deception is required to disrupt each of the kill-chain stages after an initial foothold is established during an attack. Here are a few examples of deceptions that can disrupt the kill chain:

- **Escalate privileges:** Counterfeit user credentials in operating system caches (bait)
- **Internal reconnaissance:** File Transfer Protocol (FTP), Remote Desktop Protocol (RDP), Secure Shell (SSH) links, and credentials that direct attackers to honeypots (breadcrumb)
- **Move laterally:** Fake network shares and honeypots (decoy)
- **Complete mission (data exfiltration):** Fake data files in honeypots (bait)

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Creating a "Lie-on-the-Fly" with Fluid Deception

The industrialization of deception technology requires deploying deception across enterprise networks with potentially thousands of machines. In Deception 1.0, low-interaction honeypots were the only viable solution to cost-effectively achieve this level of scale. However, to effectively mitigate advanced threats, high-interaction honeypots are required to identify and neutralize the TTPs of an attack.

Fluid Deception is an Acalvio-patented solution that combines scale and depth, by dynamically escalating the interactivity of a decoy as needed. The interactivity of the decoy services is now not just binary — low or high — but is progressively varied, based on the attack activity.

Fluid deception projects a large number of decoys in the enterprise and uses a few high-interaction systems to back them up. The decoys leverage the actual services in the high-interaction systems to provide bespoke deceptive services. The continuum of interactivity, enabled by using actual services instead of emulations, helps engage the attack and capture TTPs with minimal resource usage.

If an attacker needs to be provided shell access, the decoy is dynamically replaced by a high-interaction system, while preserving the characteristics of the original decoy,

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

including hostname, IP address, open ports, and services.

As you learn in Chapter 2, building and customizing emulations in low-interaction decoys to match all the services in a given enterprise is a huge task. By avoiding emulations and leveraging actual services, decoys can now provide realistic services virtually identical to the customized services in the enterprise network.

Fluid Deception is a powerful technology that can be applied to all types of decoys. For example, a database may have a fabricated table with no data, but with fake statistics showing that the table has millions of rows. On access, real rows of fake data can be returned on the fly, and all TTPs of the attack are recorded.

Enabling Dynamic Deception with DevOps

As defined by Jez Humble, author of *Continuous Delivery*, DevOps (Development and Operations) is "building, managing, and operating rapidly changing resilient systems at scale." Enterprise-scale deception requires a DevOps approach to configuring, deploying, and managing deceptions.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

In a continually evolving enterprise network, threat scenarios also continually evolve. Deception 2.0 analyzes the changing ecosystem and dynamically adapts deceptions to continue blending into the target IT environment. For example, endpoint devices on a network connect and disconnect frequently throughout the day. Staleness is the enemy of deception in such environments. In order to be effective, deceptions must follow the same patterns as the real information assets they're trying to protect.

Deception 2.0 also understands the context in which it runs, for example, the differences between healthcare and financial systems, as well as the differences between a Windows 7 system and a Windows 10 system. The deceptions conform to, and change with, the nature of the network resources in the environment.

Threat intelligence provides another sophisticated input to Deception 2.0. As attackers' methods and exploits change, the deployed deceptions must change as well. If the latest malware targets a specific service or exploits a particular vulnerability, more deceptions need to provide that service or display that vulnerability. All these considerations form the basis of DevOps for deception.

DevOps is enabled by combining machine intelligence with domain expertise. In the next chapter, you learn how data science enables DevOps for deception.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Leveraging data science
- Building a layered defense
- Extracting threat intelligence
- Revisiting deception challenges

Chapter 4
Creating a Deception Strategy

In this chapter, you learn how to develop an effective deception strategy for your enterprise network and how data science can help automate the process. You also learn about implementing security best practices with a layered defense ecosystem and leveraging advanced threat analysis for threat intelligence.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Blinding the Enemy with (Data) Science

Enterprise-scale deception requires automated intelligence to configure, deploy, and manage thousands of deceptions. The deception should change as the enterprise environment changes and as the threat landscape evolves. Effective deception needs to be customized to blend into the enterprise IT environment and lure attackers. Data science provides the intelligence to automate the deception deployment in an enterprise, such that it blends in seamlessly with the enterprise IT infrastructure. Data science leverages the security ecosystem — security information and event management (SIEM), endpoint detection and response (EDR), privileged identity management (PIM), and so on — and external data feeds, such as information sharing and analysis centers (ISACs).

Using these inputs, data science builds a deception recommendation model that can be used to determine the number, position, and configuration of deceptions to deploy. The recommendation model may be revised periodically, based on new or modified inputs, and the effectiveness of the previous deployment strategies. For example:

» If the network has a mix of services and operating systems installed, the decoys will show the same mix.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

» If threat intelligence warns of new attacks against SQL Server databases, more fabricated SQL Server database services are deployed.

Data science is also used by Fluid Deception to decide when to escalate the interactivity of a decoy and how far. Escalation triggers may depend on the service accessed and existing threat intelligence (among others), and they may keep changing with the environment. By building intelligence into deception escalation, data science helps to minimize the overhead of high-interaction decoys.



Deception-triggered data science is significantly different from conventional security data science. Conventional security data science primarily leverages anomaly detection techniques to identify anomalous behavior in network traffic and user, host, or network element behavior. In contrast, deception-triggered data science starts with a real attack (for example, an anomaly announced by a deception event), so it doesn't require anomaly detection algorithms.

Data science correlates other security event data with high-fidelity deception alerts to generate insights about adversary behavior. This approach is used to collect and describe the context around a deception alert, instead of looking for an anomaly like a needle in a haystack. Instead, data science focuses on capturing everything about how an attack begins and proceeds.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.



REMEMBER

Deception-triggered data science significantly reduces false positive alerts, thereby reducing the overall infrastructure and maintenance cost associated with security-related tasks.

Analysis of attacker behavior also enables security data science recommendations on the types of deceptions to present to attackers, and can use statistical analysis to help determine the number of deceptions to include in an enterprise environment. Moreover, based on the deception triggered, the response can be dynamically modified to either confuse an attacker or divert him away from the production environment.

In a deception-based environment, analysis starts after deceptions get triggered. Deception-triggered alerts correlate with alerts from other security data sources, such as NetFlow or user authentication and asset data from SIEM database. Such deception context data provides insights into adversary behavior, movements, and tactics.

Deception-triggered security science enables numerous use cases, including the following:

- **Adversary profiling:** Provides details about intruders based on deception-context data, along with hosts visited, vulnerabilities exploited, and tools or malware used. Based on this information, analysts can weigh different response scenarios.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Adversary tracking:** Correlates deception event data with other data (for example, SIEM, EDR, PIM, and so on) to construct the probable path that led the intruder to a deception sensor. Armed with this knowledge, analysts can trace the attack path and gain insights about vulnerable access points and paths that may otherwise go undetected.
- **Similarity analytics:** Permits hosts that are like compromised hosts to be identified and remediated. Analysts can see the similarities in various dimensions, enabling them to get a snapshot of possible compromised machines.
- **Threat hunting:** By correlating deception alerts with IDS alerts, firewall alerts, and vulnerabilities, InfoSec playbooks can be built to assist security analysts hunting for threats in the enterprise environment.



REMEMBER

Data science creates opportunities to seek out patterns in deception events, and to anticipate future adversaries or patterns and indicators of compromise (IOCs). Moreover, data science enables seamless deployment of deceptions and operational efficiency in the enterprise network.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Weaving a Tangled (Enterprise-Wide) Web: Layered Defense

A layered defense strategy combines multiple mitigating security controls to protect computing and network resources, and data. A combination of security systems, each using different techniques, is required to effectively counter modern cyber threats. Layering security systems ensures that different systems compensate for vulnerabilities or weaknesses in other systems.

Deception 2.0 (discussed in Chapter 3) uses innovative new techniques to provide layered defense for enterprise networks. Internal and external threat intelligence from other security systems provides input to the DevOps for the deception model. A threat may, for example, be an anomaly detected by an intrusion detection system (IDS) or an alert triggered on a firewall due to failed connection attempts.

Leveraging a DevOps approach, Deception 2.0 can quickly deploy relevant additional deceptions around an alert to intelligently lure the attacker away from production assets. When an attacker is engaged, analysis can be shared with other systems on the network. For example, an indicator of compromise (IOC) can be generated for an attacker's command-and-control (C2) infrastructure

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

and shared with the perimeter firewall to automatically stop data exfiltration attempts.

Leveraging Advanced Threat Analysis

Threat analysis extracts intelligence from attack artifacts collected during threat engagement (discussed in Chapter 3) and provides the input to generate an appropriate response to the attack. Advanced threat analysis requires a high-interaction honeypot. To perform effective threat engagement, a high-interaction honeypot must satisfy the following conditions:

- Multiple decoys, breadcrumbs, and baits should be installed to determine the exploits and lateral paths used.
- The collection mechanism must be invisible to the attacker.
- Network traffic must be collected and correlated to the attacker's actions. This helps determine C2 infrastructure, exfiltration activity, and more.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- All attacker actions must be recorded, for example, through instrumented binaries, screen captures, keyboard loggers, and so on.
- Memory dumps must be performed to determine any files not saved to disk.
- Downloaded or dropped files must be identified.

Threat analysis is done in real-time as the threat artifacts are collected. Analysis determines the malicious actions being carried out by the attacker and the objectives of the attack (for example, exfiltrating data, encrypting data, building a botnet, and so on). Once the attack is analyzed, data science (discussed in Chapter 3) determines the appropriate response.



A high-interaction decoy is different from a sandbox, both in its requirements and functionality. A decoy is an interactive system, designed for studying both malware and threat actors, while a sandbox is primarily designed for malware detonation. Both decoys and sandboxes collect detailed attack information. However, a decoy is part of a networked environment and is uniquely positioned to study how the attack plays out beyond the system — for example, how it interacts with domain name system (DNS) servers, dynamic host configuration protocol (DHCP) server, or Active Directory (AD) servers.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Limitations and Exclusions Need Not Apply

Recalling the challenges of Deception 1.0 (discussed in Chapter 2), let's look at how Deception 2.0 addresses these same challenges:

- Fluid Deception provides both scale/density and depth/quality of deception.
- Customized low-interaction services avoid emulations to provide complete coverage and resist fingerprinting.
- DevOps for Deception enables deceptions to be dynamic, which avoids staleness and counters fingerprinting.
- DevOps for Deception automatically deploys and maintains deceptions.
- Deceptions now mimic all enterprise resources.
- Deception 2.0 actively gets input from, and provides intelligence to, the security ecosystem.
- Threat engagement and analysis is an integral part of Deception 2.0.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Harvesting attack information
- Taking deception to the cloud
- Flushing out attackers
- Getting smart about smart home security

Chapter 5

Deploying a Deception Architecture

In this chapter, you learn about different deployment scenarios and use cases for deception technologies.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Keeping the Fox Out of the Henhouse with a Deception Farm

A high-interaction decoy is used to engage and study an attacker by allowing unrestricted access to the decoy. The decoy may be easier to exploit than neighboring production assets, and may be set up with known vulnerabilities, or factory default settings to attract the attacker.

However, when the attacker takes control of a decoy, the decoy may be used to launch attacks against real production assets. To avoid this risk, decoys must be separated from the production network. However, decoys must also need to be intertwined with and part of the production network to successfully blend. *Deception farms* satisfy both contradictory requirements.

A deception farm provides the ability to consolidate all decoys to a single location. A projection point, deployed in an on-premises enterprise network, builds a software tunnel to the central deception farm and provides logical Data Link layer (Open Systems Interconnection, or OSI, model layer 2) adjacency to the enterprise network for decoys in the central deception farm (see Figure 5-1).

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

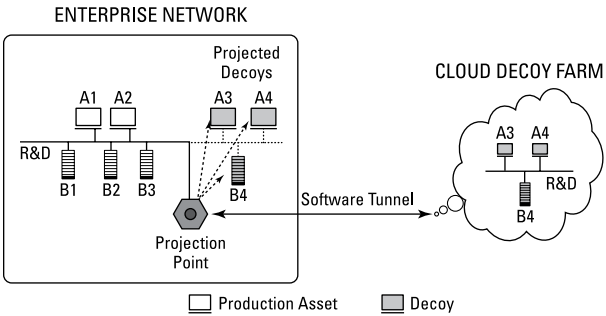


FIGURE 5-1: A cloud-based deception farm.

All the decoys are deployed in the deception farm, but they appear to be adjacent to the resources in multiple subnets in the enterprise network through the projection points. An attacker cannot distinguish whether a neighbor is physically or logically adjacent and an attack on any projected decoy is moved through the tunnel to the deception farm in the cloud. The tunnel is "invisible" to the attacker and is used to monitor traffic generated by the attack. Network traffic through the tunnel is controlled to ensure that any attack or malware is allowed only one way from the enterprise network to the deception farm, but blocked if it tries to move in the other direction. This ensures that any compromise stays in the deception farm and is disposed of by recycling the decoy.

A cloud-based, centralized deception farm is ideal because it further reduces the risk of compromise. Vulnerable decoys are separated from the on-premises

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

enterprise network, and any compromise can be isolated in the cloud. Cloud-based decoys are also not physically accessible in the enterprise, providing an additional level of security.

Cloud-based deception farms have other significant advantages compared to on-premises deception farms, including the following:

- **They're more scalable.** The cloud is elastic, so the deception farm can expand if the need arises and contract when the need no longer exists.
- **They're less expensive.** Fluid deception (discussed in Chapter 3) uses resource-intensive, high-interaction decoys only when needed. But the cost for an on-premises deception farm is fixed, because it must be deployed in an appliance. In a cloud-based deception farm, costs are variable and are incurred only when the high-interaction decoys are deployed.

Obscuring Your Network from Threats in the Cloud

Public clouds are an increasingly popular destination for enterprise computing resources, given the scalability, cost effectiveness, and reliability benefits, among others, of cloud computing. CloudEndure's 2016 *Cloud Migration*

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Survey Report found that more than half of large enterprises plan to migrate to public clouds within the next two years, while the share of on-premises virtual machines and physical servers is set to decrease. Still more enterprises leverage a hybrid cloud infrastructure, with parts of their networked computing resources located on-premises and other parts in the cloud.

In addition to the inherent vulnerabilities in an on-premises environment, public and hybrid cloud computing environments have their own peculiarities that can be exploited. For example:

- **Connectivity between on-premises and cloud networks:** Volume 21 of the *Microsoft Security Intelligence Report* details multiple attack methods that are unique to public clouds. The pervasive deception strategy (discussed in Chapter 4) of Deception 2.0 includes deception to detect and engage these new vectors of compromise.
- **Secret access keys to the cloud:** Source code repositories or emails may contain secret keys that are used to access a cloud environment. Deception can help detect these attacks by strategically placing fabricated secret access keys in places likely to be targeted by the attackers.
- **Persistent brute force attacks on public-facing endpoints in the cloud:** Pivot-back attacks start with compromised servers in the public cloud and laterally

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

move into the on-premises network. For cloud networks with public-facing endpoints, decoys that are also public facing can generate threat intelligence for a specific cloud environment. By engaging the attacks before they manage to breach the cloud environment, these decoys can collect information on the tactics, techniques, and procedures of the attacks and avoid breaches.

- **Lateral movement — at your service:** In an on-premises network, lateral movement occurs from machine to machine — an attacker compromises a machine, escalates privileges, performs recon, and moves to the next target machine (see Chapter 1). In the cloud, lateral movement also occurs from service to service. The attacker compromises a service, does recon for credentials to other services, and uses them to move laterally to the next service. A Deception 2.0 solution, with decoy services and breadcrumbs, can detect lateral movement in these situations.


TIP

Learn about Deception 2.0 in Chapter 3.

An enterprise-scale deception solution deployed on-premises and in the cloud, should

- Provide a consistent interface for both environments

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- Make deception easy to install and manage in both environments
- Scale equally well across both environments

Deception farms and projection points (introduced in the previous section) enable an enterprise-scale deception solution. Projection points can be installed in both on-premises and public cloud networks. The centralized deception farm, which may be located on-premises or in the cloud, projects customized deceptions through the projection points based on network segments.

Cloud computing is continually evolving and undergoing significant improvements and changes. The Deception 2.0 approach — using fluid deception, deception farms with projection points, and data science — helps enterprises address future advances in cloud computing. For example, a current emerging trend is the use of software containers in cloud deployments. Major public cloud providers including Amazon, Microsoft, and Google already provide software container services. A centralized deception farm enables enterprises to easily add deception containers to the deception farm, and automatically have them projected across any network segment.



REMEMBER

The architectural and deployment flexibility of Deception 2.0 solutions makes it possible — and plausible — to extend deception to public and hybrid cloud environments.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Keeping Adversaries in the Dark about Critical Infrastructure

Industrial control systems (ICS), such as supervisory control and data acquisition (SCADA) systems, are used to monitor and control critical infrastructure components in industrial processes and environments, such as chemical factories, power grids, oil and gas pipelines, and sewage management, among others. There are two essential components in an ICS:

- **Remote terminal unit (RTU):** An RTU is usually a programmable logic controller (PLC) with sensors and actuators. An RTU has communication ports to allow it to send and receive signals (data and commands).
- **Human-machine interface (HMI):** An RTU is connected to operator workstations, called HMIs, which provide continuous, real-time information about the process state. HMIs are used by the operators to both monitor and control RTUs.

ICS components used to be air-gapped (not physically connected) to the enterprise network. ICS components were designed for reliability and safety, but not for security. ICS components are increasingly connected to the Internet to enable integrating ICS data with other

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

functionality in the enterprise network (for example, production data can automatically update inventories).

By standardizing on the Internet Protocol (IP), the networking of ICS components has been greatly simplified. But this also means that ICS components are also vulnerable to the same threats as other IP-based systems. ICS components also have some unique challenges not associated with traditional enterprise networks:

- RTUs run on small processors with limited computing power, which precludes running antivirus software.
- A significant percentage of RTUs are old and are rarely patched for vulnerabilities. Also, patches may not be available or may make the system unstable.
- False positives, or even delays in transmission, associated with inline network security systems may result in loss of view or control, which may cause harm to life or the environment in critical infrastructure services.
- Many ICS protocols are not designed for security. For example, Modbus is a communications protocol used in most ICS components. First designed in 1979, this protocol has no security features. An attacker that can reach a device with the Modbus protocol can read and write anything on that device.

These challenges limit the security systems that can be deployed in an ICS environment, but deception technology is one of the few exceptions. Deception solutions are

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

not deployed inline and do not affect regular control system processes. Deception technology also generates few false positives.

Early honeypot experiments, such as Gaspot and Conpot, focused exclusively on ICS environments. Conpot simulated a basic Siemens PLC used in many critical infrastructure ICS components to support Modbus and the simple network management protocol (SNMP). Gaspot emulated ICS and SCADA systems that monitor gasoline in storage tanks. These first-generation deception solutions demonstrated the interest of the hacker community in breaching ICS environments, as well as the effectiveness of deception in these environments, even at a very basic level.

Deception 2.0 solutions, deployed in an ICS environment, consider multiple attack entry points and automatically deploy deceptions throughout the network. Figure 5-2 shows a few possible attack vectors in a two-firewall control system architecture. As an example, the infamous Stuxnet worm used malware-infected USB drives as the entry point to attack an air-gapped Iranian nuclear facility.

A deception architecture in an ICS environment can be deployed as follows:

- **Enterprise network:** Deception in the enterprise network shows the existence of multiple counterfeit control system firewalls using well-placed breadcrumbs in the servers in the network. Any access to a counterfeit firewall detects an attack.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

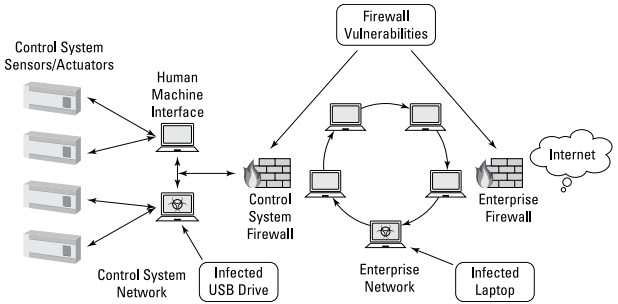


FIGURE 5-2: Potential ICS attack vectors in a two-firewall control system architecture.

- **HMIs:** Fabricated HMIs with fake traffic blend in with real HMIs. The fabricated HMIs connect to realistic PLC emulators and display continuous process state.
- **PLC controls:** The real control system network is also populated by many PLC decoys. Fluid deception (discussed in Chapter 3) is used to engage any access to PLC decoys. Pervasive deception (discussed in Chapter 4) enables attacks to be detected at each of the entry points.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Recognizing That the Internet of Things Is Not Always What It Seems

The Internet of Things (IoT) is a network of smart, connected devices, such as sensors and actuators (like those in ICS components) that are embedded in physical objects — from appliances and equipment in "smart" homes and offices, to devices implanted in humans. These "things" intelligently communicate with other devices and networks, and are driving a huge market for new products and services. Conservative estimates predict a $4 trillion market opportunity with more than 25 billion IoT devices by 2020.

Here are some unique security challenges in IoT:

- **IoT devices contain increasingly complex and powerful technology.** As processors and storage get faster and cheaper, smart objects become more powerful with every iteration.
- **Smart devices are installed everywhere — homes, offices, cars, roads, human bodies, and more.** Many of these devices are accessible via an IP address, without any firewall protection.
- **The market opportunity for IoT is huge and expanding, which encourages more companies**

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

to participate. For many of these device manufacturers, security is an afterthought.

- **IoT systems are often managed by people who have little background or understanding of cyber security.**

Figure 5-3 illustrates the use of deception technologies in a smart home:

- **Deception farms and projection points:** A single projection point can project multiple deceptions of smart objects and appliances in the home. The deceptions themselves exist in the deception farm deployed in the cloud, and only appear to be in the network neighborhood.
- **DevOps for deception:** DevOps helps to dynamically create and manage deceptions based on the devices in the smart home and developing threat profiles. For example, if an exploit is known to compromise cameras with factory default settings, DevOps projects similar cameras in the smart home to detect if malware has entered the home network.
- **Fluid deception:** Any observed attacks on projections can be escalated to high-interaction decoys located in the deception farm. For example, a projected camera can be dynamically replaced by a real camera to engage a suspected attack, capture the payload, and understand the variations of the exploit. Fluid

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

deception becomes very cost-effective to implement in the context of deception farms, since thousands of projected low-interaction decoys across thousands of residences can be successfully backed by only a few high-interaction decoys.

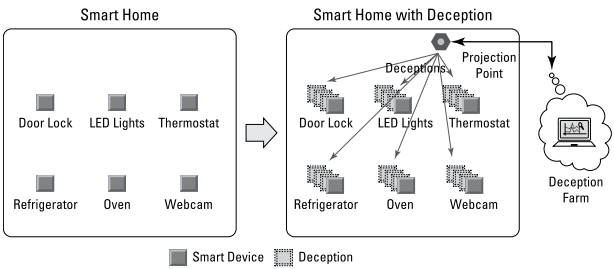


FIGURE 5-3: Deception in the smart home.



WARNING

IoT — "the next big thing" — has already arrived. Powerful computing and storage resources are being interwoven into everyday life. For example, with the advent of nano-technologies, the near future will see smart devices being used inside the human body. Thus, the ability of perimeter defenses to secure the IoT is rapidly being diminished. Deception 2.0 provides one of the few viable and effective cyber security solutions for IoT.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Maintaining effectiveness at scale
- Adapting, persisting, and automating deception
- Mitigating risk and leveraging data
- Learning your enemy's tactics
- Building a layered defense

Chapter 6

Ten Keys to Effective Deception for Cyber Protection

Here are ten essential requirements for a potent cyber deception solution:

- **Deception must provide both scale and depth.** Enterprise deception solutions should scale up cost-effectively to deploy thousands of decoys,

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

while also providing the ability to engage and respond to attacks. Solutions that provide only one of these options or the other are based on first-generation deception technologies.

- **Deception must be dynamic.** Staleness is the enemy of deception. As network and threat environments evolve, deceptions must adapt. Solutions with static deceptions are easy to fingerprint and are of little value to the enterprise.
- **Deception must be pervasive.** Effective deception requires various decoys, baits, and breadcrumbs. One-dimensional honeypot- or breadcrumb-only solutions are incomplete.
- **Deception must be automatic.** An enterprise-scale deception solution needs to lay out a multitude of deceptions and manage them dynamically. Automation at every step is a requirement for practical and effective deception at scale. Solutions that require manually deploying or managing deceptions do not scale.
- **Deception must blend into the enterprise.** A deception should not look any different from the network neighborhood. This requirement applies to all decoys, baits, and breadcrumbs, and means dynamic deception must keep up with changes in the network. Solutions that need manual setup for blending do not scale.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Deception must not introduce new risk.** Deception technologies, by design, introduce vulnerable systems in the enterprise network to lure and engage attacks. With any vulnerable system, there is the potential risk of an attack compromising the system and using the system to launch attacks against other servers. A good deception solution must mitigate the risk of compromise. Solutions that physically deploy high-interaction decoys in the enterprise network (connected directly to an access port or a trunk port) run the risk of a compromise pivoting to the enterprise servers.
- **Deception must be intelligent.** Data science is an integral part of an effective deception solution. Machine intelligence is imperative for automation. Beware of solutions without machine intelligence as every other feature of a deception solution is dependent on this capability.
- **Deception must be data driven.** A deception solution must be driven by the vulnerabilities in the network and the current threat landscape. Integration with security information and event management (SIEM) tools and cyber threat feeds is essential for effective deception. Solutions that do not integrate with SIEM cannot be dynamic.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Deception must provide attack details.** Threat engagement and analysis is an intrinsic part of a complete deception solution. A thorough understanding of the attack helps security teams identify and fix vulnerabilities targeted by the attack and close backdoors to completely neutralize the attack. Solutions that do not provide attack tactics, techniques, and procedures (TTPs) are equivalent to low-interaction solutions.
- **Deception must be part of a layered defense.** A deception solution can't function effectively in isolation. It needs to integrate with the security ecosystem to provide effective deception and quick response. Solutions that do not interact with the security ecosystem cannot respond effectively to attacks.

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

DECEPTION 2.0

DETECT MALICIOUS ACTIVITY
RESPOND TO ADVANCED THREATS

Using Automated, Dynamic Distributed Deception Technology

ShadowPlex™



ACALVIO

www.acalvio.com

These materials are © 2017 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Use deception to thwart advanced cyberattacks

This book explains the basics of the next generation of deception technology — how to dangle lures to draw hackers away from production networks and data with attractive and engaging "fake" assets. While attackers search for treasure, deception technologies monitor them and learn their ways. Best of all, while attackers are distracted by deceptions, they aren't exploiting your production networks, systems, and data.

Inside…

- Learn Deception techniques for Advanced Threat Defense
- Recognize the limits of Deception 1.0 solutions
- Discover the key tenets of Deception 2.0 technologies



Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!



ISBN: 978-1-119-36652-2
Not for resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.