



Cybersecurity for Space

Protecting the Final Frontier

—
Jacob G. Oakley

Apress®

Cybersecurity for Space

Protecting the Final Frontier

Jacob G. Oakley

Apress®

Cybersecurity for Space: Protecting the Final Frontier

Jacob G. Oakley
Owens Cross Roads, AL, USA

ISBN-13 (pbk): 978-1-4842-5731-9
<https://doi.org/10.1007/978-1-4842-5732-6>

ISBN-13 (electronic): 978-1-4842-5732-6

Copyright © 2020 by Jacob G. Oakley

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Coordinating Editor: Rita Fernando

Cover designed by eStudioCalamar

Cover image designed by Freepik (www.freepik.com)

Distributed to the book trade worldwide by Springer Science+Business Media New York, 1 New York Plaza, New York, NY 10004. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit <http://www.apress.com/rights-permissions>.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at <http://www.apress.com/bulk-sales>.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/9781484257319. For more detailed information, please visit <http://www.apress.com/source-code>.

Printed on acid-free paper

To my children,

*If a crayon-eating Marine can get published writing a book about
hacking computers in outer space, you can accomplish anything.*

Table of Contents

About the Author xiii

About the Technical Reviewerxv

Acknowledgmentsxvii

Introductionxix

Chapter 1: Space Systems 1

 Tipping Point 1

 An Introduction to Space Systems 2

 The Ground Station Design..... 4

 SV Design 6

 Ground Station Functionality 7

 SV Functionality..... 8

 Space System Architectures 12

 Conclusion..... 17

Chapter 2: Space Challenges 19

 Environmental Challenges..... 20

 Radiation 20

 Temperature 21

 Space Objects and Collisions 22

 Gravity 23

 Operational Challenges 24

 Testing..... 24

 Launch..... 25

 Deployment 26

TABLE OF CONTENTS

Detumble	26
Power	27
Emanations	28
Frequency.....	28
De-orbit	29
Conclusion.....	30
Chapter 3: Low Earth Orbit	31
LEO, Smallsats, and the General Challenges of Space	32
Environmental Challenges.....	32
Operational Challenges	34
Unique Aspects of LEO and Smallsats.....	36
Communications	36
Ground Footprint	38
Persistence.....	39
LEO Mesh Space Systems.....	40
The Challenge of the Mesh.....	40
The Anomaly.....	41
Conclusion.....	42
Chapter 4: Other Space Vehicles	43
Medium Earth Orbit	43
Geostationary Orbit	45
Multi-orbit Constellations.....	46
Special Systems.....	49
Weapons.....	49
Human Aboard.....	50
Extraterrestrial	51
Deep Space	52
Conclusion.....	53

Chapter 5: Threats to the Vehicle	55
Electrical Power System (EPS)	56
Non-cyber Threat to EPS 1	56
Non-cyber Threat to EPS 2	56
Cyber Threat to EPS 1.....	57
Cyber Threat to EPS 2.....	57
Communication	58
Non-cyber Threat to Communication 1	58
Non-cyber Threat to Communication 2	58
Cyber Threat to Communication 1	59
Cyber Threat to Communication 2.....	60
Guidance, Navigation, and Control (GN&C)	60
Non-cyber Threat to GN&C 1	60
Non-cyber Threat to GN&C 2	61
Cyber Threat to GN&C 1	61
Cyber Threat to GN&C 2.....	62
De-orbit	62
Non-cyber Threat to De-orbit	62
Cyber Threat to De-orbit 1	62
Cyber Threat to De-orbit 2.....	63
Non-LEO Space Systems.....	63
Weapons.....	63
Crewed	64
Extraterrestrial	65
Deep Space	66
Conclusion.....	67
Chapter 6: Threats to the Mission	69
Cyber and Safeguards.....	69
Watchdogs.....	70
Gold Copies	70

TABLE OF CONTENTS

Fallback Encryption 71

Resource Limits..... 72

Sensing Missions 72

 Radio Signal 72

 Terrestrial Photo-Imagery 73

 Terrestrial Thermal Imagery 74

 Terrestrial Monitoring..... 75

 Space Monitoring 76

 Space Imaging 77

Emitting Missions 78

 Positioning..... 78

 Jamming 79

Communication Missions 80

 Broadcast..... 80

 Pipe 81

Weapon Missions 82

 Non-cyber Threat to Mission 82

 Cyber Threat to Mission..... 83

Life Support..... 83

 Non-cyber Threat to Mission 83

 Cyber Threat to Mission..... 84

Other Mission Threats 84

 Watchdog Abuse..... 84

 Bus/Payload Communications..... 84

Conclusion..... 85

Chapter 7: Pre-operational Vectors 87

 Design 87

 Confidentiality 88

 Integrity 89

Availability	89
Development	91
Confidentiality Threat to Confidentiality	91
Integrity	92
Availability	93
Supply Chain Interdiction	94
Confidentiality	95
Integrity	96
Availability	97
Testing and Validation	98
Confidentiality	98
Integrity	99
Availability	100
General Interdiction	102
Conclusion	102
Chapter 8: Communication Vectors	103
Between Ground and Space	103
Confidentiality	103
Integrity	105
Availability	105
Between Space and Space	107
Confidentiality	107
Integrity	108
Availability	109
Between Bus and Payload	111
Confidentiality	111
Integrity	112
Availability	113
Conclusion	114

TABLE OF CONTENTS

Chapter 9: Operational Vectors..... 115

Flight and Operation 115

 Confidentiality 116

 Integrity 117

 Availability 118

Analysis and Dissemination 119

 Confidentiality 120

 Integrity 121

 Availability 122

Consumers 123

 Confidentiality 123

 Integrity 124

 Availability 125

Conclusion..... 126

Chapter 10: Compromise Microanalysis..... 127

A Series of Unfortunate Events 128

 The Plan 128

 Targeting 128

 Personal Computer..... 129

 Phone 130

 Lab Computer 132

 Ground Station Computer 133

 Payload Computer 135

 Data Handler 137

 SDR 138

Conclusion..... 140

Chapter 11: Compromise Macroanalysis..... 141

Initial Ground Station..... 141

 How 142

 Why 143

Payload 1 Computer	143
How	143
Why	144
Payload Ground Network.....	144
How	145
Why	145
Flight Computer.....	146
How	146
Why	147
Flight Ground Network	147
How	147
Why	148
Payload 2 Computer	148
How	149
Why	149
Mesh.....	150
How	150
Why	151
Conclusion.....	152
Chapter 12: Summary.....	153
The Cost Problem	153
The Cyber Warfare Problem.....	155
The Test Problem	156
The Adaptation Problem	156
The Defense in Depth Problem.....	157
The Modernization Problem	157
The Failure Analysis Problem	158
Conclusion.....	159
Index.....	161

About the Author



Dr. Jacob G. Oakley spent over seven years in the US Marines originally involved in satellite communications and later was one of the founding members in the operational arm of the Marine Corps Forces Cyberspace Command. After his enlistment, he wrote and taught an advanced computer operations course, eventually returning back to mission support. He left government contracting to do threat emulation and red teaming at a private company for commercial clients, serving as the principal penetration tester and director of penetration testing and cyber operations. He is currently working as a cybersecurity subject matter expert for a government customer, advising on cybersecurity integration and strategy. He completed his doctorate in IT at Towson University, researching and developing offensive cybersecurity methods, and is the author of *Professional Red Teaming: Conducting Successful Cybersecurity Engagements* (Apress, 2019) as well as *Waging Cyber War: Technical Challenges and Operational Constraints* (Apress, 2019).

About the Technical Reviewer

Dr. Albert B. Bosse is a practicing spacecraft engineer, currently serving as chief engineer for electro-optical and infrared space vehicles for a government customer. He has over 28 years of experience applying his expertise in aerospace vehicle structures, structural dynamics, guidance, navigation and control, and systems engineering for the advancement of tactical intelligence, surveillance, and reconnaissance capabilities within the U.S. Department of Defense. His notable past positions include Spacecraft Control Systems Branch Head at the Naval Research Laboratory (2001–2005), Associate Professor of Aerospace Engineering at the University of Cincinnati (2005–2008), Technical Director of the Missile Defense Agency Interceptor Knowledge Center (2009–2017), and Chief Scientist of the Missile Defense Agency Ground-Based Midcourse Defense Program (2019). The organizations he previously served include the Naval Research Laboratory, Swales Aerospace, Draper Laboratory, and the Johns Hopkins University Applied Physics Lab.

Dr. Bosse earned M.S. and Ph.D. in aerospace engineering from the University of Cincinnati in 1991 and 1993, respectively, as well as a B.S. in physics from Thomas More University in 1987.

Acknowledgments

I would like to thank my beautiful wife and family for putting up with this and other nerdy endeavors.

To Dr. Al Bosse who performed the technical review for this book and has been a font of knowledge about space and space vehicle operations, this book would not be possible without you.

To all you keyboard-wielding cyber warriors out there protecting freedom, I salute you.

Introduction

As a cybersecurity professional, the more I learn about space systems, the more I realize how underprepared the space industry is against cybersecurity threats and how unaware the cybersecurity industry is of the space domain in general. I wrote this book to provide a primer on space systems and the concepts of space vehicle operations to cybersecurity practitioners. The environmental and operational challenges and constraints faced by space systems are considerable. The threats and vectors by which those threats will affect space systems are imposed or created by these challenges and constraints. After reading this book, cybersecurity professionals will have the building blocks of knowledge necessary to develop and implement solutions to space system issues which not only improve the resiliency and security of those systems but allow them or enable them to conduct their mission. I also provide macro- and microanalysis of compromise scenarios involving space systems to drive home the very real and present risk to such systems via the cyber domain. Though written from the perspective of and for the primary audience of the cybersecurity industry, space domain operators, designers, and developers can surely benefit from understanding the threats, vectors, and issues that cyber brings with it. This is especially relevant given the interconnectivity and continued digitization and software definition of space system components.

CHAPTER 1

Space Systems

Before I get into the specifics of space systems, I just want to make clear that this book is written with cybersecurity professionals in mind and by a cybersecurity professional. That is not to say that those who design and operate space vehicles (SVs) or the generally curious have nothing to gain from reading it. Quite the opposite in fact. This book is written with the intent of priming the cybersecurity community on the intricacies of space systems, their high difficulty and risk during operation, as well as the distinct challenges of security in outer space.

As such, there will be descriptions, illustrations, and scenarios involving space systems and their operation that will be at times simplified and potentially unrealistic. I am trying to educate the security perspective on the difficult task ahead regarding creating and implementing solutions to protect systems in space. Any space topics are covered only to the extent necessary to aid in that understanding. There is plenty of literature regarding designing and operating systems to fly in outer space, and if that topic interests you, as it does openly or secretly all nerds, I encourage you to read up on the fascinating subject. This book is my attempt to address what I feel is a gap in the cybersecurity community's awareness for the growing presence of computers in outer space and a lack of comprehension for the implications of space operations on cybersecurity.

Tipping Point

We are currently at a precarious position in the evolution and accessibility of space operations to academic, commercial, and government entities. More and more computing platforms are being launched into orbit and beyond. Unfortunately, these systems, as a necessity, have a heavy focus on functionality, and any regard to cybersecurity is oftentimes a byproduct of attempts at safeguarding the space system from failure and not any malicious intent. This means that we are revisiting an era in computing where the operators and any operation passed to the device are trusted; after

all, why would I do anything to damage my multimillion-dollar satellite program? Why would someone do that?

The problem is that plenty of people would do that, from hacktivists, cybercriminals, and nation state actors to commercial competitors engaging in industrial espionage. Exacerbating this potential nasty situation is the fact that everything is becoming increasingly connected; after all, why wouldn't you want to check the status of your SV with a smart phone application? How else are you going to show off your space program to fellow academics or sell the accessibility of your space system to potential customers in the commercial world?

It is not hard to imagine that a large percentage of space operations moving forward will be inherently accessible for one reason or another to some system or systems on the Internet. Even if not, recent history is littered with examples of malicious code that has allowed the spread and infection of cyber attack effects across devices connected not to the Internet or even any other network at all.

Worst of all, the computational resources available to any would-be attacker are immense when compared to the available resources on a space system that could be dedicated in some way to cybersecurity. As we will cover more in depth later, once a malicious actor gains access to the computer on the ground that communicates with a space system, there is almost implicit trust and no further defense in depth for the space system or systems that communicate with that terrestrial computer.

An Introduction to Space Systems

The most basic example of a space system is where there is a device on the ground transmitting to and/or receiving from a device in space that is transmitting and/or receiving. For the purpose of this book, we will refer to the device on the ground that transmits and/or receives as the “ground station” and will refer to the device in space that transmits or receives as the “SV.” Often nowadays, the ground station is where the SV is flown from—although it has not always been the case and will not always be the case that the SV is flown. For instance, if we go back to one of the most famous space systems, the Sputnik 1 satellite, it had no way of flying at all. It was shot into orbit and flew around the Earth with no ability for steering. In fact, it did not receive any instructions from a ground station at all, it just broadcast a radio wave signal that could be heard by anyone on Earth with a radio antenna tuned to the correct frequency.

This is a far cry from some of the extremely complex systems of today. Consider the International Space Station (ISS). It regularly makes maneuvers using onboard propulsion to move out of the way of space debris that is on a collision path with it. In the case of the ISS, it can be flown from on board the station itself as well as by individuals at a ground station on Earth. The orbital planes of the Earth are inhabited by SVs spanning the full spectrum of sophistication from derelict or antiquated satellites to complex constellations of multifunctional SVs. The simple example of one SV and one ground station is shown in Figure 1-1.

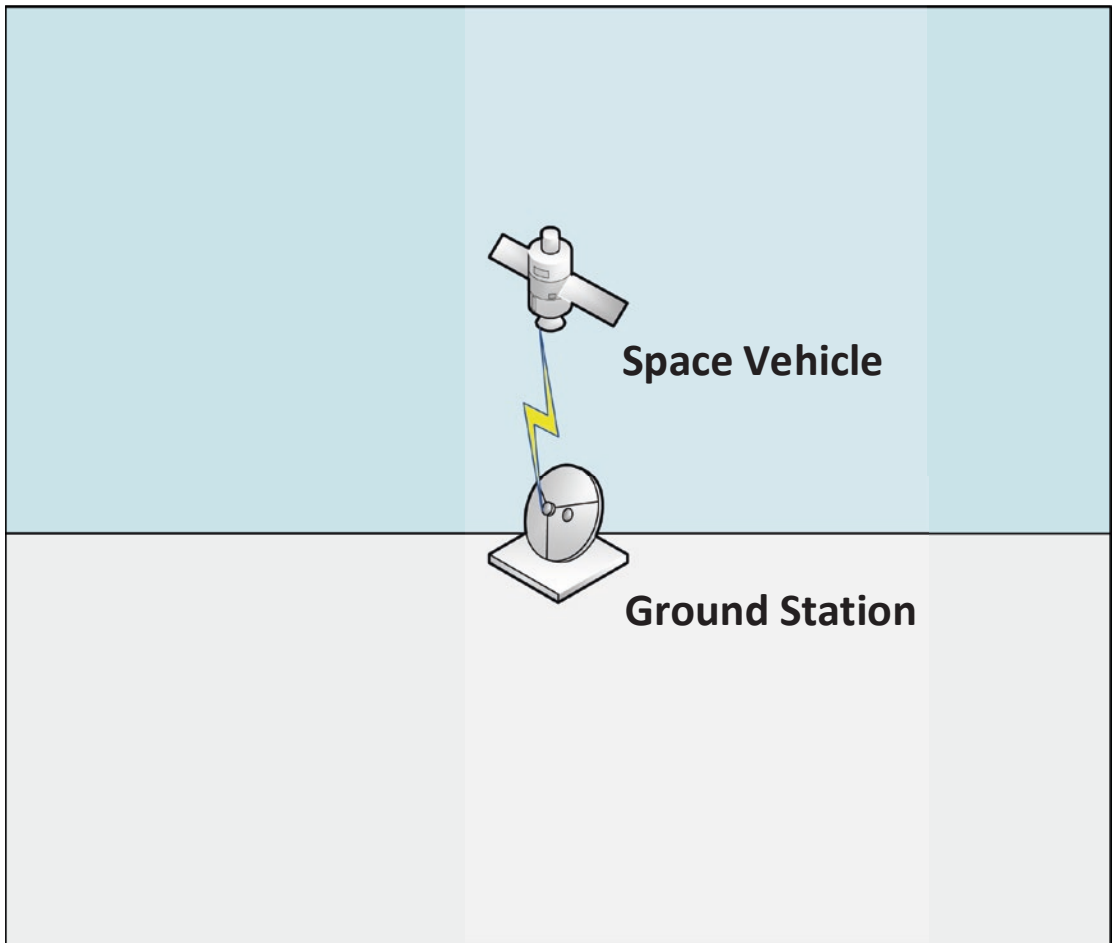


Figure 1-1. *Basic Space System*