1.

Record Nr.	UNINA9910677231703321
Autore	Grimes Roger A.
Titolo	Hacking multifactor authentication / / Roger A. Grimes
Pubbl/distr/stampa	Indianapolis, Indiana : , : Wiley, , [2021] ©2021
ISBN	1-119-65080-1 1-119-67235-X 1-119-67234-1
Descrizione fisica	1 online resource
Disciplina	005.8
Soggetti	Hacking Hackers Cryptography Computers - Access control - Testing Computer networks - Security measures Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Introduction -- Who This Book Is For -- What Is Covered in This Book? -- MFA Is Good -- How to Contact Wiley or the Author -- Part I Introduction -- Chapter 1 Logon Problems -- It's Bad Out There -- The Problem with Passwords -- Password Basics -- Identity -- The Password -- Password Registration -- Password Complexity -- Password Storage -- Password Authentication -- Password Policies -- Passwords Will Be with Us for a While -- Password Problems and Attacks -- Password Guessing Password Hash Cracking -- Password Stealing -- Passwords in Plain View -- Just Ask for It -- Password Hacking Defenses -- MFA Riding to the Rescue? -- Summary -- Chapter 2 Authentication Basics -- Authentication Life Cycle -- Identity -- Authentication -- Authorization -- Accounting/Auditing -- Standards -- Laws of Identity -- Authentication Problems in the Real World -- Summary -- Chapter 3 Types of Authentication -- Personal Recognition -- Knowledge-Based

Authentication -- Passwords -- PINS -- Solving Puzzles -- Password Managers -- Single Sign-Ons and Proxies -- Cryptography -- Encryption

Public Key Infrastructure -- Hashing -- Hardware Tokens -- One-Time Password Devices -- Physical Connection Devices -- Wireless -- Phone-Based -- Voice Authentication -- Phone Apps -- SMS -- Biometrics -- FIDO -- Federated Identities and APIs -- OAuth -- APIs -- Contextual/Adaptive -- Less Popular Methods -- Voiceover Radio -- Paper-Based -- Summary -- Chapter 4 Usability vs. Security -- What Does Usability Mean? -- We Don't Really Want the Best Security -- Security Isn't Usually Binary -- Too Secure -- Seven-Factor MFA -- Moving ATM Keypad Numbers -- Not as Worried as You Think About Hacking

Unhackable Fallacy -- Unbreakable Oracle -- DJB -- Unhackable Quantum Cryptography -- We Are Reactive Sheep -- Security Theater -- Security by Obscurity -- MFA Will Cause Slowdowns -- MFA Will Cause Downtime -- No MFA Solution Works Everywhere -- Summary -- Part II Hacking MFA -- Chapter 5 Hacking MFA in General -- MFA Dependency Components -- Enrollment -- User -- Devices/Hardware -- Software -- API -- Authentication Factors -- Authentication Secrets Store -- Cryptography -- Technology -- Transmission/Network Channel -- Namespace -- Supporting Infrastructure -- Relying Party Federation/Proxies -- Alternate Authentication Methods/Recovery -- Migrations -- Deprovision -- MFA Component Conclusion -- Main Hacking Methods -- Technical Attacks -- Human Element -- Physical -- Two or More Hacking Methods Used -- "You Didn't Hack the MFA!" -- How MFA Vulnerabilities Are Found -- Threat Modeling -- Code Review -- Fuzz Testing -- Penetration Testing -- Vulnerability Scanning -- Human Testing -- Accidents -- Summary -- Chapter 6 Access Control Token Tricks -- Access Token Basics -- Access Control Token General Hacks -- Token Reproduction/Guessing -- Token Theft

Sommario/riassunto

"Multi-Factor Authentication (MFA) is spreading like wildfire across digital environments. However, hundreds of millions of dollars have been stolen from MFA-protected online accounts. How? Most people who use multifactor authentication (MFA) have been told that it is far less hackable than other types of authentication, or even that it is unhackable. You might be shocked to learn that all MFA solutions are actually easy to hack. That's right: there is no perfectly safe MFA solution. In fact, most can be hacked at least five different ways. Hacking Multifactor Authentication will show you how MFA works behind the scenes and how poorly linked multi-step authentication steps allows MFA to be hacked and compromised. This book covers over two dozen ways that various MFA solutions can be hacked, including the methods (and defenses) common to all MFA solutions. You'll learn about the various types of MFA solutions, their strengthens and weaknesses, and how to pick the best, most defensible MFA solution for your (or your customers') needs. Finally, this book reveals a simple method for quickly evaluating your existing MFA solutions. If using or developing a secure MFA solution is important to you, you need this book."