L'autore ix

Ringraziamenti xi

Prefazione xv

Introduzione xix
A chi è rivolto questo libro xix
Che cosa troverete in questo libro xx
Poche parole per chi ingegnere non è xxi
Terminologia relativa alla sicurezza xxii
Aforismi xxiv
Come è organizzato questo libro xxv
Stili e convenzioni xxvi
Poche parole da un maestro Jedi xxvi

Capitolo 1 – Falsificazione e autenticità 1
Identificatori e autenticazione 2
Identificatori tecnici 3
Identificatori umani 4
Autenticazione fra persone 5
Autenticazione delle persone sui computer 6
Autenticazione dei computer per le persone 8
Autenticazione di computer su computer 9
Attacchi di falsificazione 11
Falsificazione di file 11
Falsificazione di processi 14
Falsificazione di macchine 14
Falsificazione in scenari specifici 18
Internet of Things 18
Telefoni cellulari 20
Cloud 21
Considerazioni sull'autenticazione per le organizzazioni 21
Meccanismi per gli attacchi di falsificazione 22
False dichiarazioni 23

Attacchi ai meccanismi di autenticazione 25
Minacce contro i tipi di autenticazione 27
Difese 33
Autenticare le persone 33
Autenticazione dei computer 34
Conclusioni 34

Capitolo 2 – Manomissione e integrità 37
Introduzione 37
Obiettivi della manomissione 38
Manomissione dell'archiviazione 38
Manomissione delle comunicazioni 39
Manomissione del tempo 42
Manomissione dei processi 43
Manomissione di specifiche tecnologie 46
Meccanismi di manomissione 48
Posizione dell'attività di manomissione 49
Strumenti per le attività di manomissione 50
Difese 52
Crittografia 52
Il kernel 52
Rilevamento 54
Conclusioni 54

Capitolo 3 – Ripudiabilità e dimostrabilità 55
Introduzione 55
La minaccia: la ripudiabilità 57
Ripudio dei messaggi 58
Frodi 59
Furto di identità 63
Registrazione delle minacce 66
La ripudiabilità nelle specifiche tecnologie 69
Internet of Things (e smartphone) 70
Cloud 70
Intelligenza artificiale/machine learning 71
Criptovalute e blockchain 71
Meccanismi di ripudio 72
Difese 74
Crittografia 74
Conservazione dei file log 75
Utilizzo dei file log 79
Strumenti antifrode 82
Conclusioni 82

Capitolo 4 – Divulgazione delle informazioni e riservatezza 85
Minacce alla riservatezza 86
Divulgazione di informazioni, a riposo 86
Divulgazione di informazioni, in movimento 90
Divulgazione di informazioni da un processo 93

Connessioni umane 95
Effetti collaterali e canali nascosti 95
Meccanismi di divulgazione delle informazioni 98
Divulgazione di informazioni in scenari specifici 99
Internet of Things 100
Smartphone 101
Cloud 101
Intelligenza artificiale/machine learning 103
Blockchain 104
Privacy 104
Difese 104
Difese del sistema operativo 105
Difese dei processi 108
Crittografia 110
Conclusioni 114

Capitolo 5 – Denial-of-Service e disponibilità 117
Risorse consumate dagli attacchi Denial-of-Service 118
Calcolo 118
Spazio di memorizzazione 120
Reti 121
Energia elettrica 122
Denaro 123
Altre risorse 124
Caratteristiche di un attacco Denial-of-Service 125
Su misura o generalizzato 125
Amplificazione 126
Autenticazione 127
Effimero o persistente 127
Diretto o progressivo 128
Denial-of-Service contro specifiche tecnologie 128
Servizi di autenticazione 129
Cloud 129
Protocolli 129
IoT e dispositivi mobili 130
Difese 131
Abbondanza e quote 131
Degrado controllato 132
Test di resilienza 133
Conclusioni 134

Capitolo 6 – Espansione dell'autorità e isolamento 135
Meccanismi di espansione e loro effetti 139
Manipolazione del livello di autorità in scenari specifici 142
Deputati confusi 143
Internet of Things 145
Dispositivi mobili 146
Cloud 146

Difese 148
Minimo privilegio e separazione dei privilegi 149
Barriere "architettoniche" 151
Barriere nel codice 154
Autorità e privilegi 157
Controllo degli accessi (la storia) 157
Nuovi approcci ai criteri 162
Conclusioni 165

Capitolo 7 – Prevedibilità e casualità 167
Minacce basate sulla prevedibilità 168
Indovinare e verificare 168
Minacce crittografiche 173
Minacce basate sul tempo 173
Rapporto fra divulgazione delle informazioni e il tempo 173
Manomissione del tempo 174
Prevedibilità in scenari specifici 174
Traffico di rete 174
Minacce al sistema locale 175
Processi aziendali 177
Difese 177
Prevenire le race condition 177
Difese contro le ipotesi e la ricerca 178
Usabilità 182
Adottate trasparenza 183
Conclusioni 186

Capitolo 8 – Parsing e corruzione 187
Che cos'è il parsing? 188
Come funzionano i parser 188
Un po' di contesto 189
Tutti i dati sono contaminati 191
Minacce ai parser 192
Esempio di SQL Injection 193
Un output sorprendente 194
Input eccessivamente potente 199
Minacce Denial-of-Service ai parser 200
Cattivi consigli 200
Parser incatenati 201
Minacce specifiche dello scenario di parsing 202
Protocolli di parsing e formati di documenti 202
Codice C e sicurezza della memoria 203
Difese 206
Il Principio di robustezza 207
Convalida dell'input 208
Sicurezza della memoria 212
LangSec 215
Conclusioni 218

Capitolo 9 – Kill Chain 219
Minacce: Kill Chain 220
Kill chain per server 222
Kill Chain per desktop 224
Acquisire o utilizzare le credenziali 233
Kill Chain per scenari specifici 240
Cloud 241
IoT 242
Dispositivi mobili (IOS, Android) 242
Armamento come sotto-catena 242
"Nessuno lo farebbe mai" 244
Ransomware 244
Kill chain di rete 244
Elementi storici 246
Storia delle kill chain 246
Difese 251
Tipi di difese 252
Scenari di difesa 253
Conclusioni 255

Epilogo 257

Glossario 261

Bibliografia 269

Un indice delle storie 283
Episodio I – La minaccia fantasma 283
Episodio III – La vendetta dei Sith 283
Obi-Wan (serie tv) 284
Rogue One 284
Una nuova speranza 284
L'impero colpisce ancora 285
Il ritorno dello Jedi 285

Indice analitico 287