Come fa R2-D2 a sapere chi è Ben Kenobi? Come decide di riprodurre la registrazione della principessa Leia per Ben, ma non per Luke? In che modo la principessa Leia comunica a R2 le sue intenzioni? Queste tre domande toccano aspetti fondamentali della sicurezza: autenticazione, autorizzazione e usabilità (i fan di Star Wars hanno una risposta alla prima domanda, grazie ai prequel, ma Leia non conosce tale risposta). Inoltre, il modo in cui il mondo di Star Wars interagisce con la tecnologia e i computer ci offre una base per scoprire come la tecnologia funziona nel nostro mondo.

Ero un fan di Star Wars prima ancora di scrivere una riga di codice e molto prima di violare il mio primo sistema. Quando sono diventato un esperto di sicurezza informatica, mi è diventato chiaro che sul campo siamo molto più bravi a lavorare con il codice che con le storie, e sebbene sia allettante dire "Ecco perché fallisci", raccontare storie migliori non è la nostra unica speranza. Quando riflettevo su Guerre stellari, mi sono reso conto che, mentre svaniscono i testi, la telecamera scende sulla nave della principessa Leia inseguita per… un nastro di dati rubato! Ho capito che Star Wars non è solo la storia del viaggio di Luke Skywalker verso l'età adulta, ma è anche una storia sulla divulgazione di informazioni e sulle relative conseguenze. Nell'ultimo decennio, ho usato Star Wars per raccontare l'evoluzione della sicurezza informatica perché la sua epica ci fornisce punti di riferimento e immagini utili per affrontare questioni importanti e complesse.

In questo libro, quasi ogni riferimento è alla trilogia originale. C'è materiale che potrei aver tratto da *Rogue One*, dai prequel e sequel, da spettacoli televisivi, da libri e altro ancora. Ma presumo che la maggior parte dei lettori abbia visto e abbia bene in mente solo i tre principali: *Guerre stellari*, *L'Impero colpisce ancora* e *Il ritorno dello Jedi*.

Così come la Forza è una proprietà di tutti gli esseri viventi, la sicurezza è una proprietà di tutti i sistemi tecnologici. E come la Forza

ha un lato chiaro e un lato oscuro, la sicurezza ha difese e attacchi. Questo libro si concentra principalmente sugli attacchi, le minacce, i problemi. È necessario comprendere le minacce per approntare le difese appropriate. È drammatico vedere l'Imperatore scatenare fulmini viola di Forza su Luke Skywalker, ma un migliore addestramento avrebbe potuto preparare Luke alla minaccia e insegnargli a difendersene. Né un firewall né una lista di controllo bloccheranno mai i fulmini della Forza.

Se volete rendere sicura una casa, dovete pensare a tutte le cose che potrebbero andare storte. Ci sono gli eventi naturali (inondazioni), eventi naturali o artificiali (incendi) ed eventi attuati da esseri intelligenti (furti).

Abbiamo dei modelli impliciti di cosa sia una casa, dei tipi di case e dei tipi comuni di minacce. Questi problemi variano in qualche modo: certe zone hanno i tornado, certe altre hanno i monsoni e altre ancora hanno le tempeste di sabbia. Ma il vostro assicuratore saprà offrirvene un elenco (suddiviso fra "coperture opzionali" ed "esclusioni").

I nostri modelli impliciti di come sono impostati i sistemi tecnologici sono più deboli. La tecnologia offre una maggiore varietà e presenta cambiamenti più rapidi rispetto alle nostre case o ai nostri uffici. Le architetture a tre livelli sono differenti dai microservizi. Le implementazioni cloud dei microservizi differiscono dalle macchine virtuali implementate anche solo dieci anni fa.

I costruttori e gli utilizzatori di sistemi di difesa hanno uno svantaggio: è difficile evitare di pensare a come rendere funzionale un sistema. Sappiamo tutti che è difficile far funzionare un sistema. Che tutto è frutto di compromessi per far funzionare il codice, per renderlo fruibile e perfino per distribuirlo.

La risposta tradizionale della sicurezza a questa situazione è stata un'esortazione a "pensare come un hacker". Ma è difficile. Piuttosto, io incoraggio le persone con cui parlo a pensare come uno chef professionista, immaginando che centinaia di commensali si siedano stasera alla nostra tavola. La maggior parte di noi non saprebbe da dove cominciare. Ma l'idea è che non siamo costretti a "pensare come hacker" per cogliere prospettive differenti dei sistemi su cui stiamo lavorando.

La sicurezza differisce da tanti altri potenziali problemi perché abbiamo a che fare con aggressori intelligenti che imparano a adattarsi. Se qualcuno vuole rubare il vostro stereo di casa, può entrare dalla porta principale in molti modi: può aprirla a calci, rompere o forzare la serratura o rubare una chiave. Alcuni attacchi sfruttano vulnerabilità: la serratura può avere una piastra frontale debole, che può essere perforata facilmente a causa di un difetto costruttivo. Alcuni sfruttano i difetti di progettazione: la serratura impiega solo pochi perni, cosa

che la rende facile da forzare. Possono aggirare del tutto la porta, entrando da una finestra. Nei sistemi tecnologici, la gamma di attacchi sembra infinita e forse inconoscibile: un problema che questo libro intende risolvere.

Uno dei motivi per cui non riusciamo a rendere sicuri i sistemi è che gli hacker hanno molti vantaggi. Possono studiare il loro obiettivo, pianificare i loro attacchi e lanciarli solo quando si sentono sicuri. Possono operare in modo da prendere il controllo di un sistema, possono sfruttare un difetto progettuale o possono puntare su chi ha creato il sistema stesso. Parte di ciò che fanno gli hacker è davvero molto intelligente e tutto è inaspettato. Questo è estremamente importante. In un piccolo video fantastico *The Death Star Architect Speaks Out*, l'architetto dice: "L'attacco è stato possibile solo grazie a poteri magici. Se qualcuno mi avesse detto di tenere conto dei maghi spaziali nella progettazione delle aperture di scarico, avremmo comunque una Morte Nera!".

Ed è così. Troppo spesso, i responsabili della sicurezza ricevono pubblicità per aver preso un sistema e individuato i suoi difetti… come ingegneri che non sanno che un siluro potrebbe percorrere chilometri di tubazioni senza che una turbolenza lo devii. Sembra quasi che gli esperti della sicurezza vi giudichino e rispondano a ogni vostra domanda alzando gli occhi al cielo e dicendo: "Cerca nel tuo cuore". Questo libro si concentra sulle minacce più importanti.

L'esperto della sicurezza e autore Bruce Schneier una volta ha scritto: "Quando ho visitato la National Security Agency, ho chiesto di vedere il 'grande libro degli attacchi'. Mi hanno detto che tale cosa non esiste: non c'è un posto dove si trova tutto scritto". Questo libro ha lo scopo di risolvere proprio questa situazione. Ed è importante, perché comprendere "gli attacchi" è più facile se esiste un insieme definito di "attacchi". Questo non vuole essere un tentativo di classificare ogni attacco o di essere esaustivi. Tale arroganza sarebbe probabilmente sorprendente e potrebbe perfino preoccuparvi. Ma la realtà è che i problemi di sicurezza sono violazioni dei requisiti di sicurezza. I requisiti di sistemi differenti sono differenti. Devo includere le violazioni dei requisiti per gli arsenali nucleari o la stampa di valuta? "Solo meno di due persone possono attivare il sistema" o "Quale altro cliente può ottenere la stessa scorta di carta"? Tale pretesa di completezza oscurerebbe gli attacchi più comuni e impedirebbe di fare riferimento alle minacce che potrebbero ispirarvi e consentirvi di ragionare per analogia nello scoprire gli attacchi ai vostri sistemi. Il punto cruciale è comprendere le minacce, e finora è stato proprio questa la difficoltà.

Qualcun altro ha scritto: "Tutti i sistemi complessi sorprendono il loro creatore". Questa è la proprietà che li porta a essere da utili a

interessanti. E i problemi di sicurezza spesso sono vere e proprie sorprese. Si basano non solo sugli errori in ciò che c'è, ma sull'incapacità degli architetti di sviluppare difese appropriate.

L'attenzione umana è un severo maestro. È difficile percepire quello che manca. Il mio intento nel catalogare i problemi comuni consiste nel dire: questi sono importanti. Questi devono essere considerati e, raccogliendoli, organizzandoli e presentandoli, intendo fornirvi una certa chiarezza su ciò che rientra nell'insieme delle cose che "dovete considerare". Se ignorerete ciò che presento in questo libro, è ragionevole affermare che si tratta di un fallimento di ingegnerizzazione. Questo non vuole affatto dire che "Potete ignorare ogni altra cosa". Proprio come un pilota deve saper far atterrare l'aereo oltre a spuntare una lista di controlli o un chirurgo deve curare il paziente, ciò che deve essere affrontato non si limita a ciò che troverete nelle pagine di questo libro.

L'attenzione umana è davvero un severo maestro. Daniel Kahneman è fondatore dell'economia comportamentale e vincitore del Premio Nobel. Nel suo libro, *Thinking Fast and Slow*, usa un solo acronimo: *WYSIATI*, *What You See Is All There Is* ovvero "quello che vedete è tutto quello che c'è". L'importanza di ciò che è di fronte a voi è così esteso che spiazza tutti i nostri sforzi di "rimanere consapevoli" e di "tenere in considerazione". Tuttavia, come ingegneri, dovete fare esattamente questo: tenere in considerazione l'affidabilità, le prestazioni, l'usabilità, la manutenibilità e molte altre proprietà. Abbiamo molti strumenti per gestire queste cose, tra cui l'automazione, le liste di controllo e il giudizio di vari team.

Per questo libro, adotto un compromesso progettuale e presumo che i sistemi di difesa siano noti e compresi, o almeno compresi tenendo conto delle minacce. Quindi mi concentro sulle minacce e accenno solo brevemente alle difese. Questo è un compromesso consapevole, che ha lo scopo di rendere il libro più breve e fruibile.