I miei allievi mi insegnano tanto. Mentre ascolto le domande che mi pongono e leggo i compiti che mi consegnano, scopro dove devono rivolgere la loro attenzione per proteggere i loro sistemi. Ho imparato a trovare le minacce nel corso di una lunga carriera, grazie a pochi e saggi insegnanti e dopo molti errori. Come ho in parte detto nei ringraziamenti, questo libro è sorto da una semplice domanda: "Dove devo rivolgermi per conoscere di più queste minacce?".

È un po' come "C'è del buono in lui, l'ho percepito": ho sentito questa domanda in così tante conversazioni. La parola *sicurezza* racchiude una grande complessità e molte sfumature. Stavo per dire che tendiamo a conoscere le minacce per osmosi, ma non è esattamente così. Tendiamo a conoscere le minacce quando scoppia qualcosa. Anche quando quel qualcosa è molto più piccolo di una Morte Nera, spesso le lezioni sono traumatiche, a volte cambiano la carriera. La tragedia è una cattiva maestra.

Se vogliamo essere sistematici nella nostra ricerca delle minacce nei confronti dei nostri prodotti, dobbiamo strutturare bene il modo in cui apprendiamo e insegniamo tali minacce.

A chi è rivolto questo libro

Questo libro è rivolto a ogni ingegnere.

Sarà molto utile a coloro che costruiscono o gestiscono sistemi complessi, ricchi di software. L'ingegneria spinge a difficili compromessi, resi ancor più difficili quando gli obiettivi della sicurezza sono oscuri o vaghi. Il libro è incentrato sui sistemi che comprendono del codice, ma di questi tempi tutti i sistemi contengono codice! Coloro che lavorano nei campi più tradizionali (aerospaziale, chimico, civile, meccanico) scoprono che quei sistemi così eleganti dell'era della mec-

canica vengono sempre più soppiantati. Ora i sistemi devono sempre più spesso interfacciarsi con del codice, e ciò costringe ad affrontare nuove problematiche di sicurezza.

Negli ultimi decenni, lo sviluppo di software e il funzionamento dei sistemi è molto cambiato. Abbiamo imparato che la nostra speranza di adattare a posteriori le proprietà di accessibilità, affidabilità e usabilità ci è costata cara, e che dobbiamo incorporare tutti questi fattori fin dall'inizio. Stiamo imparando che la sicurezza funziona più o meno allo stesso modo. Le scelte fatte in fase di sviluppo di un sistema hanno conseguenze. Ora sappiamo di dover affrontare il fattore sicurezza prima e in modo più olistico.

Questo libro è anche rivolto ai professionisti e agli appassionati della sicurezza. Ci sono molti percorsi, in molti campi, incentrati sulla sicurezza e sull'hacking. Ma pochi di essi contribuiscono a definire una struttura comprensiva, che serva a organizzare il flusso di informazioni relative a minacce, vulnerabilità ed exploit che affronterete. La mia speranza è che questo libro serva anche a tutti loro.

Questo libro è rivolto a ogni ingegnere, anche se non è un fan appassionato di fantascienza; e se invece lo siete, qualunque sia il mondo che preferite. Mentre parlavo di questo libro, i fan di Star Trek sono usciti dalle nebulose per chiedermi: "Perché?". E io adoro Star Trek. Adoro la sua visione ottimistica del futuro, il modo in cui la serie rispetta la competenza e la scienza, la scrittura e lo sviluppo dei personaggi. Ho consegnato il manoscritto con la dedica: "per rendere coraggiosamente sicuro ciò che nessuno ha mai reso sicuro prima!", come una sorta di omaggio affettuoso. Ma nel mio team mi hanno detto che strideva troppo, in apertura, e avevano ragione.

Che cosa troverete in questo libro

Sicurezza.

Per la precisione, acquisirete una consapevolezza della sicurezza in modi che vi consentiranno di creare e gestire sistemi che funzionano nonostante i tentativi di attacco. Proprio come la comprensione della forza (intesa come accelerazione per massa) ci consente di pensare a tanti aspetti del mondo e di applicarli ai nostri progetti, questo libro vi fornisce una struttura duratura per anticipare le minacce.

È tradizione includere in questa sezione una raffica di falle della sicurezza, con lo scopo di motivare i lettori. Ma non mi sembra che funzioni, quindi lo eviterò. Nel 2023, il problema della sicurezza non sta più nel "perché", ma nel "cosa" e nel "come".

Poche parole per chi ingegnere non è

Ho scritto questo libro per gli ingegneri: persone che costruiscono o gestiscono sistemi tecnologici complessi, in particolare gli algoritmi, i chip, i sensori e i componenti attuativi di tali sistemi. È scritto per essere il più chiaro possibile, ragionevolmente, ma se non siete esperti di tecnologie e siete in cerca di consigli, voglio suggerirvi tre cose che dovreste fare.

Innanzitutto, attivate l'aggiornamento automatico di tutto, in particolare di dispositivi, sistemi operativi e browser web. Gli aggiornamenti forniti spesso risolvono gravi problemi di sicurezza che possono essere sfruttati in modo del tutto automatico dagli hacker. Se il vostro fornitore unisce insieme cambiamenti di funzionalità e correzioni della sicurezza, lamentatevene a gran voce. In ogni caso, questo suggerimento è una difesa cruciale contro i difetti sensibili a un exploit.

In secondo luogo, usate un gestore di password e fategli creare password lunghe e casuali. Spesso la sicurezza è pregiudicata dal fatto che i siti web rivelano il vostro indirizzo e-mail e la vostra password. Gli hacker raccolgono e scambiano tali elenchi e sottopongono a test le combinazioni raccolte su ogni sito web possibile, comprese tutte le varianti concepibili. Immaginano che la mia password per Amazon potrebbe essere "adamamazon" o "amazonas1?" e i computer sono molto efficaci nel comporre questo tipo di combinazioni, insieme ad "amazon-feb" e a ogni altra password cui potete aver pensato. Utilizzate una password lunga e casuale. Se vi aspettate di doverla digitare spesso, usate la funzione che impiega come password tre o quattro parole casuali. A proposito, io utilizzo il gestore di password 1Password di Agilebits e ve lo consiglio. E… no, non ho un interesse commerciale in ciò.

Terzo, usate il buon senso. Se ritenete che un sito web non sia sicuro, non apritelo. Trovate l'azienda cercandola o seguendo un segnalibro. Se ritenete che un'e-mail sia sospetta, chiamate la persona o l'entità che afferma di averla inviata. Se necessario, utilizzate il numero posto sul retro della vostra carta per chiamare la vostra banca. In ciascuno di questi casi, state assumendo il controllo e state utilizzando risorse che un hacker non può influenzare.

Un hacker potrebbe clonare la carta che avete nel portafoglio; se avete problemi del genere, cercate un aiuto professionale. Non lo dico con sarcasmo. Se avete contro di voi un ente di spionaggio che dedicherà tempo ed energie per creare una carta e metterla nel vostro portafoglio, questo consiglio non vi salverà.

Altri due passi facoltativi se desiderate maggiore sicurezza. Innanzitutto, create indirizzi e-mail speciali per le vostre relazioni speciali.

Create qualcosa come hiufdsuapre8wafdsjkf@gmail.com e usatelo per la banca o le transazioni. Questo vi proteggerà se un hacker riuscisse a impossessarsi del vostro account principale e vi aiuterà a ridurre le e-mail di phishing. Se lo usate solo per la vostra banca, qualsiasi messaggio che sostiene di provenire dalla "vostra banca" sarà automaticamente sospetta. E poi, l'ho già detto, applicate il buon senso.

Infine, per l'online banking utilizzo un apposito browser e un profilo specifico. Il software dei browser è piuttosto solido di questi tempi, ma con tutti gli attacchi che si sentono, mi sento più a mio agio dedicandogli un browser apposito. Al momento, uso Firefox e Chrome. A volte ho usato due diversi profili di Firefox, con due temi visuali radicalmente differenti.

Questo è tutto. Questi sono i miei consigli. Vi ringrazio per aver acquistato questo libro. Potete leggerlo o regalarlo a un ingegnere o a un appassionato. A ogni modo, presumerò che il lettore sia un tecnico, quindi inizierò fin da subito a parlare di linguaggi binari, che sono alla base sia di "una galassia molto, molto lontana", sia del nostro mondo.

Consentitemi di puntualizzare un principio di base: l'isolamento. Un gestore di password isola i siti l'uno dall'altro, così come l'utilizzo di due account di posta elettronica o di due browser. Uscire da un sito o chiamare la vostra banca vi permette di uscire dal luogo in cui si sta svolgendo un attacco. Questo isolamento, che separa le parti di un sistema l'una dall'altra, è anche il motivo per cui utilizziamo account differenti, firewall e una miriade di altre tecniche di difesa.

Naturalmente, ogni livello di isolamento ha un costo in termini di comodità. Non permettere ai software di lavorare insieme, senza soluzione di continuità, significa che dovete fare voi le cose che li farebbero funzionare insieme, perché in questo modo l'hacker sarà costretto a indurvi a fare le operazioni che gli occorrono.

Questo, purtroppo, non è un consiglio che ascolterete spesso. Ci mancano informazioni sulle cause profonde e sulla storia degli attacchi, che ci aiuterebbero a stabilire le priorità. È un problema di cui scrivo spesso e su cui non mi soffermo più di tanto in questo libro.[1]

Terminologia relativa alla sicurezza

Questo libro parla di *minacce*. Riconosciamo tutti una minaccia quando ne sentiamo una: "O la borsa, o la vita!", "Ho cambiato il nostro

1 Potete trovare ulteriori informazioni su questo argomento su shostack.org/resources/lessons.

accordo. Prega che non lo cambi ancora". Uso il termine minaccia per indicare un problema futuro e che spesso può essere evitato, intraprendendo azioni preventive.

I responsabili della sicurezza usano la parola *minaccia* in vari modi. Chiamiamo minaccia un hacker. Chi si occupa di anti-malware definisce minaccia ogni virus o frammento del malware.

Mettere in atto una minaccia è un attacco. Ogni minaccia, la sua manifestazione e il suo impatto possono essere motivo di preoccupazione. La legge considera una minaccia come un'aggressione, in quanto può provocare lesioni. Nel campo della sicurezza informatica, spesso ci preoccupiamo sia della minaccia sia del suo risultato. Se qualcuno viola un sistema impersonando un utente legittimo, può rapidamente mettere in atto a catena altre minacce, come la manomissione o la divulgazione di informazioni. Soprattutto mentre state imparando, è bene essere specifici sulla relazione tra meccanismo e impatto. Un *rischio* è la quantificazione di una minaccia e tali quantificazioni spesso implicano la probabilità di successo e l'entità dell'impatto in termini economici o di vite umane.

Un hacker utilizza un *exploit* per sfruttare una vulnerabilità. Un exploit è un software che consente all'hacker di fare qualcosa che il proprietario del sistema vorrebbe impedire. Sfruttare un exploit significa usare quel software contro un obiettivo. Una *vulnerabilità* è un problema specifico del codice (un bug), un difetto in cui determinati requisiti di progettazione sono stati trascurati o il risultato di un compromesso scelto dai progettisti o dagli operatori. A volte essere specifici aiuta anche a essere più chiari; altre volte la cosa trascende nella pedanteria.

La parola *fiducia* è usata molto nel campo della sicurezza informatica e può essere sfruttata per far inciampare gli incauti. In generale, fiducia significa "una ferma convinzione nell'affidabilità, nell'onestà o nelle capacità di qualcuno". *Affidabile* è qualcuno o qualcosa che merita quella fiducia. Nel campo della sicurezza informatica, *affidabile* è qualcosa che ha la capacità di infrangere la sicurezza. Ross Anderson, professore dell'Università di Cambridge fornisce un esempio: "La spia sorpresa a vendere segreti era affidabile, ma non degna di fiducia". Altri hanno sottolineato che la parola viene spesso usata in una forma passiva o orwelliana. Un "sistema affidabile" non riesce a specificare chi si fida di lui. L'Impero Galattico spesso etichettava i sistemi come "affidabili" per aggirare qualsiasi discussione sul loro impatto sulle cose.

Aforismi

Ci sono alcune perle di saggezza che vorrei condividere con voi perché possono informare positivamente il vostro lavoro in quanto riguardano la sicurezza.

"Gli attacchi migliorano sempre; non peggiorano mai." Bruce Schneier lo fa risalire alla NSA (*National Security Agency*) americana. Mentre si approntano le difese, la lezione di un attacco non deve mai andare perduta. Gli strumenti sviluppati per condurlo non scompaiono. Vengono solo affinati e migliorati.

"Le teorie della sicurezza derivano dalle teorie dell'insicurezza." Lo ha affermato Rick Proto della NSA. Gli attacchi migliorano sempre, e la successione di attacchi informa meglio ciò che consideriamo essere la sicurezza.

"Tutti i modelli sono sbagliati; alcuni modelli sono utili." Lo ha detto lo statistico britannico George Box.

"La sicurezza informatica è perversa. Quando volete che qualcosa sia difficile, è facile, e quando volete che sia facile, è difficile. Considerate la cancellazione dei file. Far sparire davvero un file è difficile, e recuperarlo, è sorprendentemente difficile. È difficile far scomparire davvero un file, perché l'eliminazione di solito rimuove solo i puntatori nel file system. Se provate a sovrascrivere i suoi bit sul supporto disco magnetico, accade che le registrazioni fisiche sul disco siano differenti per dimensioni, e quindi i dati possono ancora essere letti dopo essere stati sovrascritti. E le unità flash non aiutano a riscrivere nelle stesse posizioni. Allo stesso modo, è facile trovare casualità quando si cerca la prevedibilità. I computer sembrano imprevedibili e i bug sono cosa comune, ma provate a scrivere un generatore di numeri davvero casuali.

"Gli hacker spenderanno il loro budget come vogliono, non come sperate voi." Potete anche sperare che gli hacker si comportino come pensate voi, ma allora non sarebbero hacker.

"La sicurezza è una proprietà dei sistemi." Non è chiaro chi l'abbia detto per primo. Questa è un'affermazione vera, e significa che spesso la sicurezza dei sistemi è determinata dagli "anelli deboli". Questo libro vi aiuterà a rimuovere tali anelli deboli.

"L'invio è una funzionalità." Questo è un detto comune in Microsoft. Tutte le nuove funzionalità che sono state create non servono a nulla fino a quando non vengono utilizzate dai clienti, quindi ritardarle è poco saggio. Allo stesso modo, ritardare un invio nella speranza di perfezionare la sicurezza significa che nessuno, nel frattempo, potrà utilizzare le nuove funzionalità. La stessa cosa vale per questo libro, ora: spero che i suoi pregi superino i suoi difetti.

"Il diavolo si nasconde nei dettagli." Chiunque l'abbia detto non pensava alla sicurezza, ma l'affermazione si presta benissimo. Molte cose si rivelano meno sicure a mano a mano che vengono studiate, e gli esperti della sicurezza hanno un grande rispetto per coloro che eseguono attività di reverse engineering e che studiano i sistemi per comprenderne il funzionamento interno, e così facendo scoprono proprietà inaspettate dei sistemi.

Come è organizzato questo libro

Questo libro inizia con STRIDE, un modo classico di considerare minacce. STRIDE è l'acronimo di *Spoofing, Tampering, Repudiation, Information disclosure, Denial-of-Service, Expansion of authority*. La sigla ci aiuta a ricordare i sei grandi gruppi di minacce, argomento dei primi sei capitoli, seguiti poi da capitoli su prevedibilità, parsing e kill chain.

La maggior parte dei capitoli di questo libro segue un determinato piano generale: inizia con una descrizione della minaccia, quindi spiega come si manifesta in determinate tecnologie, i meccanismi utilizzati dagli hacker e infine presenta una breve sezione sulle difese.

Occorre operare molte scelte nella scrittura di un libro come questo. Mi sono confrontato con i diversi modi in cui l'informatica viene impiegata e sui diversi modi in cui operano le varie minacce: Internet of Things, dispositivi mobili, cloud e intelligenza artificiale/machine learning. Gli aspetti specifici di queste parti si aggiungono ai temi più ampi trattati nel capitolo, non li sostituiscono: il fatto che un computer abbia la forma di un orsacchiotto IoT non significa che il resto del capitolo vada tralasciato. In altri capitoli troverete ulteriori parti, perché la natura della minaccia ha proprietà interessanti in uno scenario specifico che vale la pena di trattare.

L'unica tecnologia emergente non trattata in questo modo è l'informatica quantistica. La maggior parte delle minacce STRIDE riguarderà i sistemi che circondano un computer quantistico e probabilmente funzionerà anche su quel sistema. Per esempio, l'assorbimento di energia degli specchi nella crittografia quantistica determina importanti attacchi di divulgazione delle informazioni. La crittografia quantistica utilizza le informazioni sulla rotazione per distribuire le informazioni sulla chiave crittografica in modi che sono difficili da intercettare, spesso facendo affidamento sulle connessioni in fibra. È una cosa molto diversa dall'uso della meccanica quantistica per l'informatica. L'impatto iniziale dell'informatica quantistica sembra infrangere la crittografia asimmetrica classica violando le chiavi, una minaccia che

provoca la divulgazione delle informazioni. Se siete desiderosi di saperne di più, *Law and Policy for the Quantum Age* (Hoofnagle e Garfinkel, 2021) è un'eccellente introduzione.

Un'altra scelta organizzativa cruciale è quella di parlare più volte delle minacce. Ho imparato dall'insegnamento che la prima volta che viene esposta un'informazione, questa potrebbe non essere assorbita appieno. Tornare su di essa da una diversa angolazione spesso può essere più utile di quanto si possa pensare.

Stili e convenzioni

Troverete nominati molti prodotti e produttori. I nomi dei prodotti vengono utilizzati per rendere concreti gli esempi. La convenzione di includere un "per esempio" per ciascuno di essi fa solo perdere il tempo.

Poche parole da un maestro Jedi

Yoda: […] Il vigore di un Jedi scaturisce dalla Forza. Ma attento al lato oscuro. Rabbia, paura, violenza: sono loro il lato oscuro. Veloci ti raggiungono quando combatti. Se anche una sola volta la strada buia tu prendi, per sempre dominerà essa il tuo destino. Consumerà te, come consumò l'apprendista di Obi-Wan.

Luke Skywalker: Vader… Il lato oscuro è più forte?

Yoda: No, no, no. Più rapido, più facile, più seducente.

Luke Skywalker: Ma come distinguo quello cattivo dal buono?

Yoda: Lo imparerai. Quando sei calmo, in pace, passivo. Un Jedi usa la Forza per saggezza e difesa, *mai* per attaccare.

Il sentiero oscuro è quello che ignora la sicurezza. Il codice gira, ciò basta. Ma una volta che intraprendete quel sentiero, dominerà per sempre il vostro destino. La scelta facile è ignorare la sicurezza e concentrarsi solo sulle funzionalità, che sono più visibili ai clienti. I linguaggi più moderni rendono possibile l'esecuzione di un'analisi statica completa limitando parte del potere seducente dei puntatori. Ma c'è un costo: il lato oscuro del C è avere codice più veloce, ma ciò dominerà per sempre i vostri allarmi di sicurezza. E 20 anni fa, quando la sicurezza era meno importante, questa è stata la scelta di molte aziende, spesso in modo sconsiderato. È stata la scelta fatta da Microsoft nel suo periodo di massimo splendore.

Ma Yoda aveva ragione: "Consumerà te". Ho lavorato in Microsoft per la maggior parte di un decennio e ho un enorme rispetto per i

miei colleghi che hanno migliorato la sicurezza di Office e Windows e ne hanno sostituito le "viscere". Hanno ottenuto molto più di quanto avrei mai creduto possibile. Ma le viscere molto differenti di IoS e ChromeOS consentono a questi concorrenti di muoversi molto più velocemente, oggi.

Infine, davanti a voi c'è un intero percorso di carriera nel campo della sicurezza, un percorso fatto di attacchi. È brillante. È potente: "Lasciate che vi mostri come posso attaccare con pwn il vostro sistema". E se volete seguire quel percorso, la mia unica richiesta è che lo facciate in modo etico, usando le vostre capacità e conoscenze per condurre attacchi autorizzati, con lo scopo di edificare difese sempre più solide. Il mio percorso è iniziato con la scoperta delle vulnerabilità, ma ultimamente si è concentrato sul rafforzamento dei sistemi. È un percorso più difficile, ma l'impatto a lungo termine può essere molto superiore.