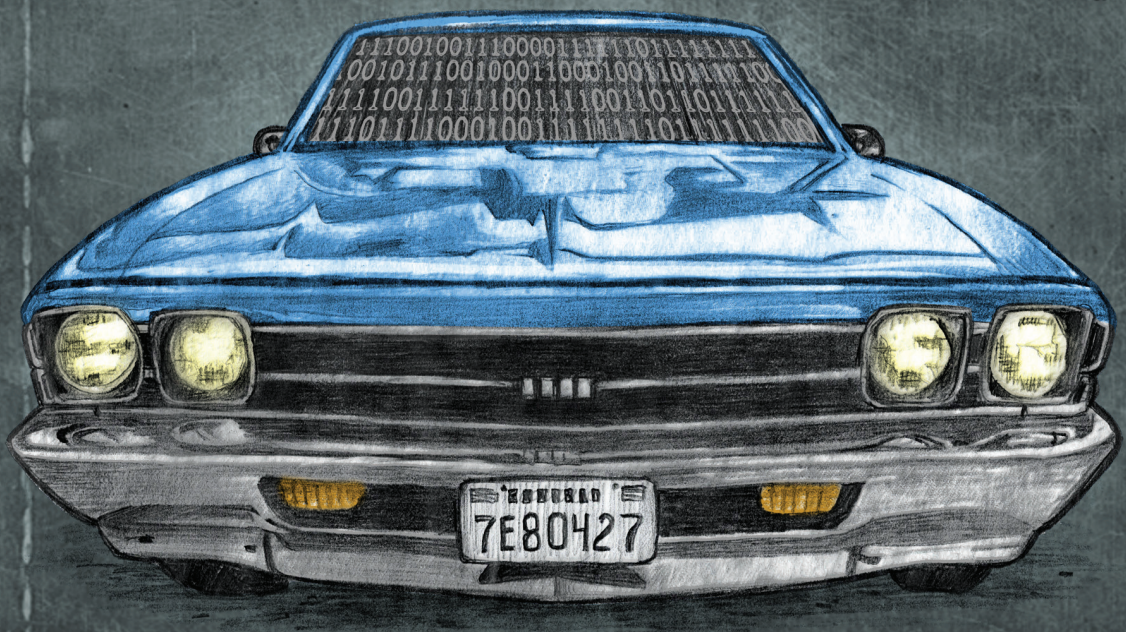
EDIZIONI
LSWR

Il manuale dell'hacker di automobili

Guida per il penetration tester



Craig Smith

Prefazione di Chris Evans

*pro
Digital LifeStyle

Il manuale dell'hacker di automobili

Guida per il penetration tester

Craig Smith

Prefazione di Chris Evans

EDIZIONI LSWR

no starch press

Titolo originale: *The Car Hacker's Handbook | A Guide for the Penetration Tester*
ISBN: 978-1-59327-703-1
Published by No Starch Press, Inc.
245 8th Street, San Francisco, CA 94103
www.nostarch.com
Cover Illustration: Garry Booth
Copyright © 2016 by Craig Smith. All rights reserved.

Autore Craig Smith

Collana: *pro DigitalLifeStyle

Edizione italiana:
Il manuale dell'hacker di automobili | Guida per il penetration tester

Editor in Chief: Marco Aleotti
Progetto grafico: Roberta Venturieri
Traduzione: Virginio B. Sala
Redazione: Stefano Andreini

© 2016 Edizioni Lswr* – Tutti i diritti riservati

ISBN: 978-88-6895-239-6

I diritti di traduzione, di memorizzazione elettronica, di riproduzione e adattamento totale o parziale con qualsiasi mezzo (compresi i microfilm e le copie fotostatiche), sono riservati per tutti i Paesi. Le fotocopie per uso personale del lettore possono essere effettuate nei limiti del 15% di ciascun volume dietro pagamento alla SIAE del compenso previsto dall'art. 68, commi 4 e 5, della legge 22 aprile 1941 n. 633.

Le fotocopie effettuate per finalità di carattere professionale, economico o commerciale o comunque per uso diverso da quello personale possono essere effettuate a seguito di specifica autorizzazione rilasciata da CLEARedi, Centro Licenze e Autorizzazioni per le Riproduzioni Editoriali, Corso di Porta Romana 108, 20122 Milano, e-mail autorizzazioni@clearedi.org e sito web www.clearedi.org.

La presente pubblicazione contiene le opinioni dell'autore e ha lo scopo di fornire informazioni precise e accurate. L'elaborazione dei testi, anche se curata con scrupolosa attenzione, non può comportare specifiche responsabilità in capo all'autore e/o all'editore per eventuali errori o inesattezze.

L'Editore ha compiuto ogni sforzo per ottenere e citare le fonti esatte delle illustrazioni. Qualora in qualche caso non fosse riuscito a reperire gli aventi diritto è a disposizione per rimediare a eventuali involontarie omissioni o errori nei riferimenti citati.

Tutti i marchi registrati citati appartengono ai legittimi proprietari.

EDIZIONI LSWR

Via G. Spadolini, 7
20141 Milano (MI)
Tel. 02 881841
www.edizionilswr.it

Printed in Italy

Finito di stampare nel mese di ottobre 2016 presso "LegoDigit" Srl, Lavis (TN)

(*) Edizioni Lswr è un marchio di La Tribuna Srl. La Tribuna Srl fa parte di LSWR GROUP.

Sommario

Prefazione

Il mondo ha bisogno di più hacker, e ha assolutamente bisogno di più car hacker. La tecnologia degli autoveicoli tende a una maggiore complessità e a una maggiore connettività; combinate, queste tendenze richiederanno una maggiore attenzione alla sicurezza degli autoveicoli e persone di talento che vi si dedichino.

Ma che cos'è un hacker? Il termine è stato largamente corrotto dai media, ma se lo si usa correttamente *hacker* si riferisce a qualcuno che crea, che esplora, che modifica — qualcuno che fa scoperte applicando l'arte della sperimentazione e smontando i sistemi per capire come funzionano. In base alla mia esperienza, i migliori professionisti (e anche dilettanti) della sicurezza sono quelli che per natura nutrono una profonda curiosità per il funzionamento delle cose. Queste persone esplorano, manipolano, sperimentano e smontano, qualche volta anche solo per il piacere della scoperta. Questi sono gli hacker.

Un'automobile può essere un incredibile obiettivo per l'hacking. La maggior parte dei veicoli non si presenta con una tastiera e un invito al login, ma possiede una schiera, con tutta probabilità assai poco nota, di protocolli, CPU, connettori e sistemi operativi. Questo libro smonterà i componenti comuni delle automobili e vi presenterà gli strumenti e le informazioni disponibili per mettervi sulla buona strada. Quando avrete finito di leggerlo, vi sarà chiaro che un'automobile è un insieme di computer collegati tra loro – che casualmente è dotato di quattro ruote. Armati degli opportuni strumenti e delle informazioni adeguate, sarete pronti per i vostri hack.

Questo libro parla molto anche di "apertura": siamo tutti più al sicuro quando i sistemi da cui dipendiamo sono ispezionabili, controllabili e documentati – e questo riguarda *assolutamente* anche le automobili. Perciò vi esorto a utilizzare le conoscenze acquisite con questo libro per ispezionare, controllare e documentare. Non vedo l'ora di leggere delle vostre scoperte!

Chris Evans (@scarybeasts)
Gennaio 2016

1

Introduzione

Nel 2014, Open Garages, un gruppo di persone interessate alla condivisione e alla collaborazione in tema di sicurezza degli autoveicoli, ha pubblicato il primo *Car Hacker's Manual* come materiale per i corsi di car hacking. Il manuale originale era stato progettato in modo che potesse essere infilato nel cassetto portaoggetti di un'auto e che coprisse gli aspetti fondamentali del car hacking per corsi di uno o due giorni sulla sicurezza degli autoveicoli. Non avevamo idea di quanto interesse avrebbe suscitato quel libro: è stato scaricato oltre 300.000 volte nell'arco della prima settimana. In effetti, il successo è stato tale da far cadere per ben due volte il nostro fornitore di servizi Internet, il che non l'ha reso proprio felice. (Va tutto bene, ci hanno perdonato, per fortuna, perché voglio molto bene al mio piccolo ISP. Un saluto a SpeedSpan.net!)
I feedback ricevuti dai lettori sono stati quasi tutti molto positivi; la maggior parte delle critiche erano rivolte al fatto che il manuale fosse troppo breve e non scendesse abbastanza nei particolari.
Questo libro intende rispondere a quelle lamentele, entra molto più in dettaglio nel car hacking e tratta anche alcune cose che non sono direttamente in relazione con la sicurezza, come la messa a punto delle prestazioni e gli strumenti utili per capire e lavorare con i veicoli.

Perché il car hacking è un bene per tutti noi

Se avete in mano questo libro, forse sapete già perché fare del car hacking; per andare sul sicuro, però, ecco un comodo elenco dei benefici di questa attività:

Capire come funziona il vostro veicolo

L'industria dell'auto ha prodotto veicoli stupefacenti, con sistemi elettronici e di calcolo complessi, ma ha fatto circolare poche informazioni su come funzionano questi sistemi. Quando saprete come funziona la rete di un veicolo e come comunica all'in-

terno e all'esterno del proprio sistema, sarete meglio in grado di diagnosticare e risolvere i problemi.

Lavorare sui sistemi elettrici del veicolo

Evolvendo, i veicoli sono diventati sempre meno meccanici e sempre più elettronici. Purtroppo, i sistemi elettronici delle auto normalmente sono chiusi per tutti, tranne i meccanici delle officine specializzate. Anche se questi hanno accesso a più informazioni di quelle che potete normalmente recuperare voi come individui, le stesse case produttrici acquistano parti da fornitori terzi e hanno bisogno di strumenti proprietari per diagnosticare i problemi. Imparando come funziona l'elettronica del vostro veicolo potrete aggirare questa barriera.

Modificare il veicolo

Capire come comunicano i veicoli può portare a modifiche migliorative, per esempio a una riduzione del consumo di carburante e all'uso di ricambi di terze parti. Quando vi sarà chiaro come funziona il sistema di comunicazione, potrete integrare nel vostro sistema altri sistemi, per esempio un display ulteriore per tenere sotto controllo le prestazioni o un componente di terze parti che si integri alla perfezione come quello uscito dalla fabbrica.

Scoprire caratteristiche non documentate

A volte i veicoli sono dotati di caratteristiche che non sono documentate o sono semplicemente disabilitate. Scoprire e utilizzare tali caratteristiche vi permetterà di sfruttare al massimo il potenziale del vostro veicolo. Per esempio, il veicolo può avere una "modalità parcheggiatore", che permette di mettere l'auto in una modalità vincolata, prima di consegnare le chiavi a un parcheggiatore.

Convalidare la sicurezza del veicolo

Al momento in cui scriviamo, le direttive per la sicurezza dei veicoli non tengono conto di minacce elettroniche maligne. I veicoli sono soggetti agli stessi malware del vostro desktop, ma le case produttrici non hanno l'obbligo di audit della sicurezza dell'elettronica di un veicolo. La situazione è semplicemente inaccettabile: in questi veicoli viaggiamo noi, le nostre famiglie e i nostri amici, e tutti abbiamo bisogno di sapere con certezza che i nostri veicoli siano il più sicuri possibile. Se scoprirete come intervenire da hacker sulla vostra automobile, saprete dove si trovano i punti vulnerabili del vostro veicolo, e potrete prendere le vostre precauzioni e sostenere meglio la richiesta di standard di sicurezza più elevati.

Aiutare l'industria dell'auto

Anche l'industria dell'auto può trarre vantaggio dalle conoscenze contenute in questo libro. Queste pagine presentano indicazioni per identificare le minacce e anche tecniche moderne per aggirare le protezioni attuali. Oltre ad aiutarvi a progettare le vostre misure di sicurezza, questo libro offre ai ricercatori una guida su come comunicare le loro scoperte.

I veicoli odierni contengono più elettronica che mai. In un articolo pubblicato sullo *IEEE Spectrum*, intitolato "This Car Runs on Code", Robert N. Charette notava che nel 2009 un veicolo già conteneva oltre 100 microprocessori, 50 unità di controllo elettriche, 7,5 km di cavi e 100 milioni di righe di codice (http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code). I tecnici della Toyota dicono scherzando che l'unica ragione per cui mettono delle ruote ai veicoli è per impedire che i computer si rovinino strisciando sull'asfalto. I sistemi informatici stanno diventando una parte sempre più integrante dei veicoli e perciò le analisi di sicurezza diventano sempre più importanti e complesse.

ATTENZIONE Il car hacking non va preso alla leggera. Giocare con la rete del vostro veicolo, le connessioni wireless, i computer di bordo o altri dispositivi elettronici può danneggiarlo o disabilitarlo. Siate molto prudenti nello sperimentare le tecniche di questo libro; la sicurezza deve essere sempre la vostra preoccupazione dominante. Come potete immaginare, né l'autore né l'editore di questo libro potranno essere ritenuti responsabili per eventuali danni che procuriate al vostro veicolo.

Che cosa si trova in questo libro

Questo libro vi guiderà nell'esplorazione di che cosa comporti il car hacking. Cominceremo con una rassegna delle norme relative alla sicurezza dei veicoli e poi entreremo nel dettaglio di come verificare se il vostro veicolo è sicuro e di come identificare le vulnerabilità nei sistemi hardware più sofisticati.
Ecco quello che troverete nei vari capitoli.

- **Capitolo 1: Comprendere i modelli di minaccia** mostra come valutare un veicolo. Imparerete come identificare le aree con i componenti a più alto rischio. Se lavorate nell'industria automobilistica, questa sarà una guida utile per costruire i vostri sistemi di modelli di minaccia.
- **Capitolo 2: Protocolli di bus** esamina in dettaglio le varie reti a bus che potrete incontrare nell'audit di un veicolo ed esplora cablaggi, tensioni e protocolli di ciascun bus.

- **Capitolo 3: Comunicazioni del veicolo con SocketCAN** mostra come usate l'interfaccia SocketCAN in Linux per integrare vari strumenti hardware CAN in modo da poter scrivere o usare uno strumento, indipendentemente dalle vostre apparecchiature.
- **Capitolo 4: Diagnostica e log** tratta di come leggere i codici del motore, gli Unified Diagnostic Services e il protocollo ISO-TP. Vedrete come funzionano i diversi servizi di modulo, quali sono le loro debolezze comuni e quali informazioni vengono registrate e dove vengono conservate.
- **Capitolo 5: Retroingegnerizzazione del bus CAN** spiega in dettaglio come analizzare la rete CAN, compreso come impostare ambienti virtuali di test e come usare strumenti e fuzzer relativi alla sicurezza CAN.
- **Capitolo 6: Hacking dell'ECU** si concentra sul firmware che gira sull'ECU. Scoprirete come accedere al firmware, come modificarlo e come analizzarne i dati binari.
- **Capitolo 7: Costruire e usare banchi di prova per ECU** spiega come smontare parti di un veicolo per creare un ambiente di test sicuro. Discute inoltre come leggere i diagrammi di cablaggio e come simulare componenti del motore per l'ECU, per esempio i sensori di temperatura e l'albero a gomiti.
- **Capitolo 8: Attaccare le ECU e altri sistemi embedded** tratta dei pin e delle metodologie per il debugging delle piastre circuitali. Esamina anche gli attacchi side-channel, come l'analisi della potenza differenziale e le imperfezioni del clock, con un esempio passo per passo.
- **Capitolo 9: Sistemi di infotainment di bordo** spiega nel dettaglio il funzionamento dei sistemi di infotainment. Poiché il sistema di infotainment di bordo ha probabilmente la superficie d'attacco più ampia, ci concentreremo su vari modi per arrivare al firmware e intervenire sul sistema. Questo capitolo esamina anche alcuni sistemi di infotainment di bordo open source, che possono essere utilizzati per i test.
- **Capitolo 10: Comunicazioni da veicolo a veicolo** spiega come è stato progettato il funzionamento della rete fra veicoli. Questo capitolo tratta della crittografia e dei diversi protocolli proposti in vari Paesi. Analizza anche alcuni dei potenziali punti deboli dei sistemi fra veicoli.
- **Capitolo 11: Trasformare in armi i risultati ottenuti da CAN** spiega nei dettagli come trasformare le ricerche in un exploit funzionante. Vedrete come convertire codice da prototipo in assembly e infine in shellcode e vedrete modi per raggiungere solo il veicolo obiettivo, fra cui i modi per sondare un veicolo senza farsi scoprire.
- **Capitolo 12: Attaccare sistemi wireless con WDR** tratta di come usare radio definita in software per analizzare le comunicazioni wireless, come TPMS, te-

lecomandi e sistemi immobilizer. Passeremo in rassegna gli schemi crittografici che potreste incontrare nell'affrontare gli immobilizer e i punti di debolezza noti.

- **Capitolo 13: Performance tuning** analizza le tecniche utilizzate per migliorare e modificare le prestazioni di un veicolo. Parleremo di messa a punto dei chip e di strumenti e tecniche comuni utilizzati per modificare un motore in modo che funzioni come volete.
- **Appendice A: Gli strumenti del mestiere** presenta un elenco di software e hardware che saranno utili per costruire il vostro laboratorio di sicurezza per auto.
- **Appendice B: Modalità e PID dei codici diagnostici** elenca alcune modalità comuni e alcuni comodi PID.
- **Appendice C: Creare un vostro Open Garage** spiega come partecipare alla comunità del car hacking e avviare un proprio Open Garage.

Al termine del libro, avrete una conoscenza molto più approfondita di come funzionano i sistemi informatici del vostro veicolo, dove sono più vulnerabili e come quelle vulnerabilità possono essere sfruttate.

Ringraziamenti

Grazie alla comunità Open Garages per il tempo, gli esempi e le informazioni che mi ha fornito e che hanno contribuito a rendere possibile questo libro. Grazie alla Electronic Frontier Foundation (EFF) per aver sostenuto il "Right to Tinker" e in generale per il suo favoloso lavoro. Grazie a Dave Blundell per il contributo a molti capitoli del libro, e a Collin O'Flynn per aver creato ChipWhisperer e per avermi permesso di utilizzare i suoi esempi e le sue illustrazioni. Infine, grazie a Eric Evenchick per aver rivisto da solo tutti i capitoli del libro, e un grazie speciale alla No Starch Press per aver migliorato di gran lunga la qualità dei miei sproloqui di partenza.

1

Comprendere i modelli di minaccia

Se provenite dal mondo dei test di penetrazione del soft_ ware, conoscete già le superfici di attacco. Per tutti gli altri, superficie d'attacco è un termine che indica tutti i modi possibili di attacco a un obiettivo, dalle vulnerabilità nei singoli componenti a quelle che influenzano l'intero veicolo.

Quando parliamo di superficie d'attacco, non ci interessa come si effettua un exploit su un obiettivo, ma solo quali siano i punti di ingresso a quell'obiettivo. Potete pensare la superficie di attacco come l'area superficiale di un oggetto (rispetto al suo volume). Due oggetti possono avere lo stesso **volume**, ma aree superficiali radicalmente diverse. Quanto maggiore è l'area superficiale, tanto più elevata l'esposizione al rischio. Se equipariamo il volume di un oggetto al suo valore, il nostro obiettivo, nel rafforzare la sicurezza, è arrivare a un rapporto basso fra rischio e valore.

Trovare le superfici d'attacco

Quando valutate la superficie d'attacco di un veicolo, dovete immaginarvi di essere una spia malvagia che si propone di fare qualcosa di brutto al veicolo. Per trovare le debolezze nella sicurezza del veicolo, valutatene il perimetro e documentate il suo ambiente. Prestate attenzione a considerare tutti i modi in cui possono arrivare dati al veicolo, che sono tutti i modi in cui il veicolo può comunicare con il mondo esterno. Esaminando l'esterno del veicolo, ponetevi queste domande:

- Quali segnali vengono ricevuti? Onde radio? Telecomandi? Sensori di distanza?

- Esiste un accesso mediante tastierino fisico?
- Ci sono sensori a sfioramento o di movimento?
- Se il veicolo è elettrico, come si carica?

Esaminando l'interno, invece, ponetevi queste domande:

- Quali sono le opzioni di input audio: CD? USB? Bluetooth?
- Esistono porte per la diagnosi?
- Quali sono le capacità del cruscotto? C'è un GPS? Bluetooth? Internet?

Come potete vedere, sono molti i modi in cui dei dati possono entrare nel veicolo: se qualcuno di quei dati è malformato o è intenzionalmente maligno, che cosa succede? Qui entra in scena la modellizzazione delle minacce.

Modellizzazione delle minacce

Sono stati scritti interi volumi sulla modellizzazione delle minacce, ma qui faremo solo un rapido riassunto, in modo che possiate costruire i vostri modelli di minacce. (Se avete domande o se questa sezione vi suscita qualche curiosità, trovate un buon libro sull'argomento!)

Nel costruire modelli di minacce per un'automobile, si raccolgono informazioni sull'architettura dell'obiettivo e si crea un diagramma per illustrare come comunichino fra loro le varie parti dell'auto. Poi si usano queste mappe per identificare gli input a più alto rischio e per mantenere una lista di controllo delle cose da tenere sotto osservazione; questo aiuterà a stabilire una graduatoria, in cui ai primi posti saranno i punti di ingresso che potrebbero dare un rendimento migliore.

I modelli delle minacce normalmente vengono preparati durante il processo di sviluppo o progettazione di prodotto.

Se l'azienda che realizza un particolare prodotto ha un buon ciclo di vita dello sviluppo, crea il modello delle minacce all'inizio dello sviluppo di prodotto e aggiorna continuamente il modello, a mano a mano che il prodotto percorre le diverse fasi del ciclo di sviluppo. I modelli delle minacce sono documenti "vivi" che mutano al modificarsi del bersaglio e in funzione delle conoscenze che si acquisiscono su quel bersaglio, perciò dovrete aggiornare spesso il vostro modello.

Il vostro modello delle minacce può essere costituito da più livelli diversi; se un processo nel modello è complicato, dovete prendere in considerazione la possibilità di disaggregarlo ulteriormente, aggiungendo ulteriori livelli ai vostri diagrammi. All'inizio, però, il livello 2 sarà il massimo a cui riuscirete ad arrivare. Analizzeremo i vari livelli nei paragrafi che seguono, a partire dal Livello di minaccia 0.

Livello 0: vista "a volo d'uccello"

A questo livello, utilizziamo le liste di controllo costruite nel considerare le superfici d'attacco. Pensate a come i dati possono entrare nel veicolo. Disegnate il veicolo al centro, poi etichettate gli spazi interno ed esterno. La Figura 1.1 mostra un possibile diagramma di Livello 0.

Le caselle rettangolari sono gli input, il cerchio centrale rappresenta l'intero veicolo. Nel loro tragitto verso il veicolo, gli input superano due linee tratteggiate, che rappresentano minacce esterne e interne.

Il cerchio del veicolo non rappresenta un input, bensì un processo complesso, ovvero una serie di attività che potrebbero essere ulteriormente disaggregate. I processi sono numerati e, come potete vedere, questo è il numero 1.0. Se nel modello delle minacce fossero presenti più oggetti complessi, li si numererebbe in successione: per esempio, un secondo processo sarebbe il 2.0, un terzo il 3.0 e così via. Ciò che sapete delle caratteristiche del veicolo aumenterà progressivamente e dovrete aggiornare il diagramma di conseguenza. Non preoccupatevi se la maggior parte degli acronimi nel diagramma non vi dice nulla: chiariremo quale sia il loro significato tra breve.

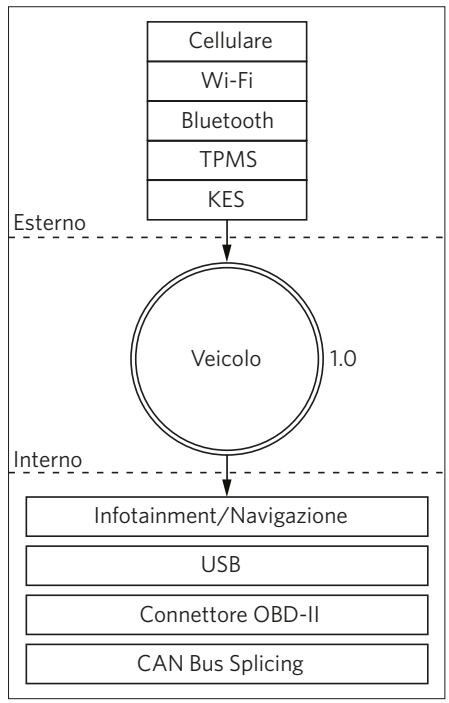


Figura 1.1 - Input di Livello 0.

Livello 1: ricevitori

Per passare al diagramma di Livello 1, scegliete un processo da esplorare. Nel nostro diagramma abbiamo un solo processo, perciò scaviamo nel processo veicolo e focalizziamo la nostra attenzione su ciò a cui "parla" ciascun input.

La mappa del Livello 1 presentata nella Figura 1.2 è quasi identica a quella del Livello 0: l'unica differenza è che qui specifichiamo le connessioni del veicolo che ricevono l'input di Livello 0. Per il momento non esamineremo in profondità i ricevitori: stiamo solo identificando il dispositivo o l'area di base a cui parla l'input.

Nella Figura 1.2, notate che ciascun ricevitore è stato numerato. La prima cifra rappresenta l'etichetta del processo ricavata dal diagramma del Livello 0 nella Figura 1.1,

mentre la seconda cifra è il numero del ricevitore. Poiché l'unità di infotainment è sia un processo complesso sia un input, la rappresentiamo con un cerchio di processo. Ora abbiamo tre altri processi: immobilizer, ECU e Ricevitore TPMS.

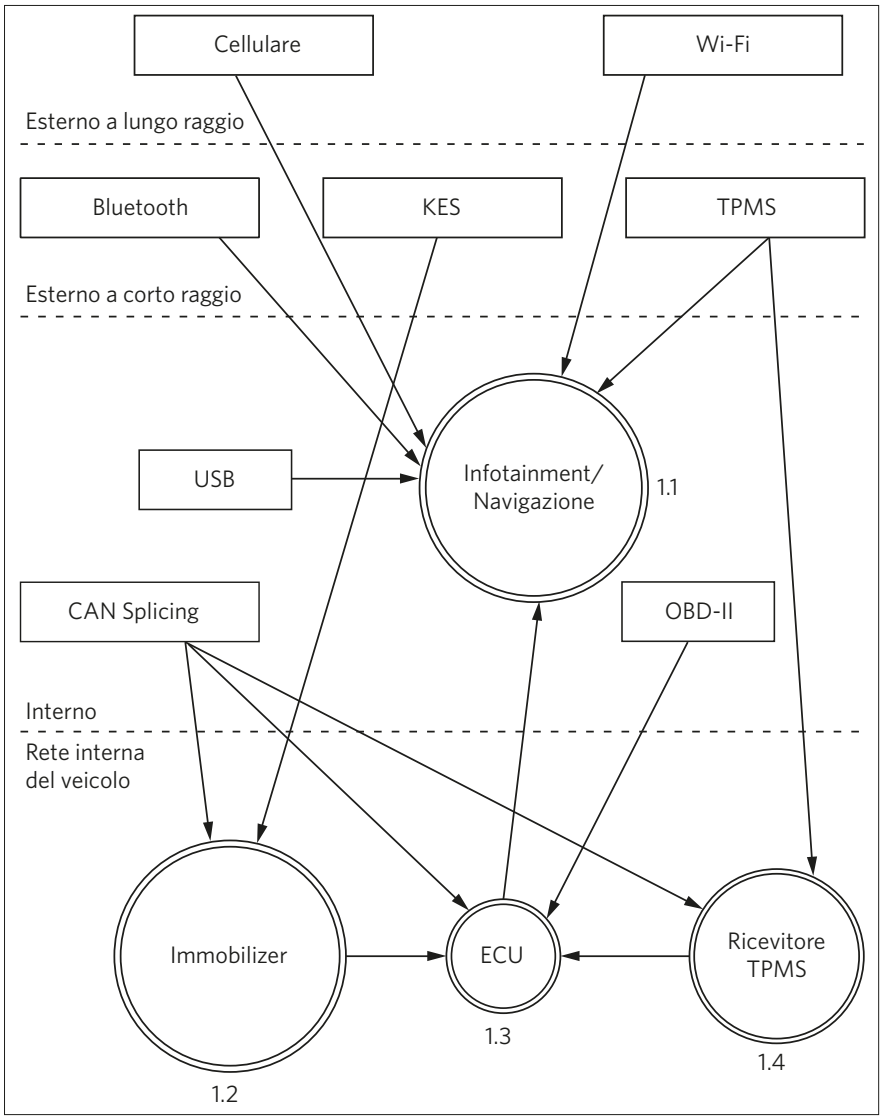


Figura 1.2 - Mappa di Livello 1 degli input e delle connessioni del veicolo.

Le linee tratteggiate nella mappa del Livello 1 rappresentano divisioni fra livelli di fiducia. Glil input nella parte alta del diagramma sono i meno fidati, quelli in basso i più

fidati. Il livello di rischio di un canale di comunicazione aumenta con l'aumentare dei confini di fiducia che attraversa.

Livello 2: disaggregazione del ricevitore

Al Livello 2, esaminiamo le comunicazioni che avvengono all'interno del veicolo. Il nostro diagramma di esempio (Figura 1.3) si concentra su una console di infotainment basata su Linux, il ricevitore 1.1. Questo è uno dei ricevitori più complicati, ed è spesso collegato direttamente con la rete interna del veicolo.

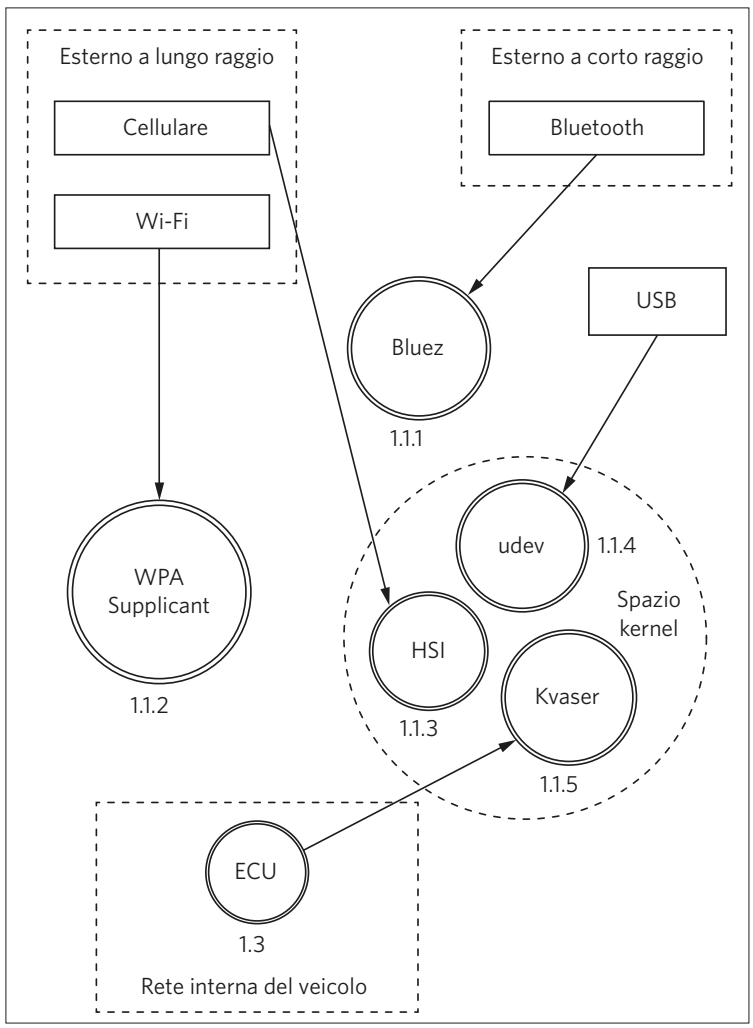


Figura 1.3 - Mappa di Livello 2 della console di infotainment.

Nella Figura 1.3, raggruppiamo i canali di comunicazione in riquadri a linee tratteggiate per rappresentare ancora una volta i confini della fiducia. Ora c'è un nuovo confine di fiducia all'interno della console di infotainment, denominato **spazio kernel**. I sistemi che parlano direttamente con il kernel presentano un rischio più elevato di quelli che parlano alle applicazioni del sistema, poiché possono aggirare tutti i meccanismi di controllo dell'unità di infotainment. Perciò il canale cellulare è a rischio più elevato del canale Wi-Fi perché attraversa un confine di fiducia entrando nello spazio kernel; il canale Wi-Fi, invece, comunica con il processo WPA Supplicant nello spazio utente.
Questo sistema è un **sistema di informazione e intrattenimento di bordo** (**IVI**, *In-Vehicle Infotainment*) e usa parti comuni a un ambiente Linux. Nello spazio kernel, si vedono riferimenti ai moduli kernel udev, HSI e Kvaser, che ricevono input dal nostro modello di minaccia. Il modulo udev carica i dispositivi USB, HSI è un driver seriale che gestisce le comunicazioni cellulari e Kvaser è il driver della rete del veicolo.
Lo schema per la numerazione del Livello 2 ora è del tipo *X.X.X*, e il sistema di identificazione è lo stesso di prima. Al Livello 0, abbiamo preso il processo veicolo che era 1.0 e siamo scesi in profondità; poi abbiamo identificato tutti i processi del Livello 1 come 1.1, 1.2 e così via. Poi, abbiamo selezionato il processo infotainment identificato come 1.1 e lo abbiamo ulteriormente disaggregato per il diagramma del Livello 2. A Livello 2, quindi, abbiamo etichettato tutti i processi complessi come 1.1.1, 1.1.2 e così via. (Potete estendere il medesimo schema di numerazione, scendendo ancora più in profondità nei processi. Lo schema di numerazione è a fini di documentazione; permette di fare riferimento a un processo ben definito al livello appropriato.)

NOTA

Idealmente, a questo stadio, si riporterebbe nella mappa quali input siano gestiti dai diversi processi, ma per il momento dovremo fare delle congetture. Nel mondo reale, dovreste retroingegnerizzare il sistema di infotainment per trovare queste informazioni.

Quando si costruisce o si progetta un sistema per autoveicoli, si deve continuare a scavare in profondità in tutti i processi complessi possibili. Riunitevi con il team di sviluppo e cominciate a discutere i metodi e le librerie utilizzati da ciascuna applicazione, in modo da poterli incorporare nei relativi diagrammi di minaccia. Probabilmente scoprirete che i confini di fiducia al livello delle applicazioni si trovano per lo più fra l'applicazione e il kernel, fra l'applicazione e le librerie, fra l'applicazione e altre applicazioni, e addirittura fra funzioni. Mentre esplorate questi collegamenti, evidenziate i metodi che hanno privilegi più elevati o che gestiscono informazioni più delicate.

Identificazione delle minacce

Ora che siamo scesi di due livelli all'interno delle nostre mappe di modellizzazione delle minacce, possiamo iniziare a identificare le potenziali minacce. L'identificazione delle minacce spesso è più divertente con un gruppo di persone e una lavagna bianca, ma potete condurla anche da soli, come esercizio di riflessione.

Proviamo a svolgere questo esercizio insieme. Partiamo dal Livello 0, la "vista a volo d'uccello" e valutiamo quali possano essere i problemi di alto livello relativi a input, ricevitori e confini di minaccia. Ora elenchiamo tutte le potenziali minacce con i nostri modelli di minaccia.

Livello 0: vista a volo d'uccello

Nel determinare le potenziali minacce al Livello 0, cercate di rimanere al livello alto. Alcune di queste minacce possono sembrare poco realistiche, perché sapete dell'esistenza di ulteriori ostacoli o di protezioni, ma è importante includere in questo elenco tutte le possibili minacce, anche se alcune sono state già affrontate. La cosa importante qui è stabilire tutti i rischi a cui può andare incontro ciascun processo e ciascun input.

Le minacce di alto livello al Livello 0 sono legate al fatto che un attaccante potrebbe:

- assumere il controllo del veicolo da remoto;
- spegnere un veicolo;
- spiare le persone a bordo del veicolo;
- sbloccare un veicolo;
- rubare un veicolo;
- tracciare un veicolo;
- aggirare i sistemi di sicurezza;
- installare malware sul veicolo.

A tutta prima, può essere difficile immaginare una serie completa di scenari di attacco. Spesso è bene far partecipare a questa fase anche persone che non sono tecnici, perché, come sviluppatori o tecnici, siete tendenzialmente così coinvolti nei meccanismi interni di funzionamento che può risultarvi naturale non attribuire alcun credito a certe idee, senza nemmeno averne l'intenzione.

Siate creativi; cercate di formulare gli attacchi più da cattivi dei film di James Bond che vi possono venire in mente. Magari pensate ad altri scenari di attacco e alla possibilità che si applichino anche ai veicoli. Per esempio, prendete in considerazione il ransomware, un software maligno che può cifrare o impedirvi l'accesso al computer o al telefono fino a che non pagate una certa cifra a qualcuno che controlla il software

da remoto. Questa tecnica potrebbe essere utilizzata anche per i veicoli? La risposta è sì. Quindi, scrivete *ransomware* nel vostro elenco.

Livello 1: ricevitori

L'identificazione delle minacce al Livello 1 si focalizza sulle connessioni di ciascun elemento più che sulle connessioni che possono essere effettuate direttamente con un input. Le vulnerabilità che evidenziamo a questo livello sono a vulnerabilità che influenzano ciò che si collega ai dispositivi in un veicolo.
Le suddivideremo in gruppi di minacce che si riferiscono rispettivamente a cellulare, Wi-Fi, telecomandi (KES), sensori di controllo della pressione degli pneumatici (TPMS), console di infotainment, USB, Bluetooth e connessioni al bus CAN (Controller Area Network, rete dell'area di controllo). Come potete vedere nell'elenco che segue, sono molte le vie per entrare in un veicolo.

Cellulare

Un attaccante potrebbe sfruttare la connessione cellulare in un veicolo per:

- accedere da qualunque luogo alla rete interna del veicolo;
- penetrare l'applicazione, nel sistema di infotainment, che gestisce le chiamate in arrivo;
- accedere al modulo **SIM** (*Subscriber Identity Module*, modulo dell'identità dell'abbonato) attraverso l'unità di infotainment;
- usare una rete cellulare per collegarsi al sistema diagnostico remoto (**onStar**);
- ascoltare le comunicazioni cellulari;
- disturbare le chiamate d'emergenza;
- tracciare i movimenti del veicolo;
- creare una finta stazione **GSM** (*Global System for Mobile Communications*).

Wi-Fi

Un attaccante potrebbe sfruttare la connessione Wi-Fi per:

- accedere alla rete dei veicolo da una distanza fino a 300 metri e più;
- trovare un exploit per il software che gestisce le connessioni in arrivo;
- installare codice maligno sull'unità di infotainment;
- individuare la password Wi-Fi;
- creare un falso punto d'accesso da concessionario per far credere al veicolo di essere sottoposto a manutenzione;
- intercettare le comunicazioni che passano attraverso la rete Wi-Fi;
- tracciare il veicolo.

Chiavi telecomando (key fob)

Un attaccante potrebbe sfruttare la connessione key fob per:

- inviare richieste key fob malformate che mettano l'immobilizer del veicolo in uno stato non noto. (L'immobilizer dovrebbe mantenere il veicolo bloccato, in modo che non possa essere avviato mettendo in contatto i fili. Dobbiamo fare in modo di garantirci che mantenga intatte le sue funzioni);
- sondare attivamente un immobilizer per scaricare la batteria dell'auto;
- rendere impossibile l'uso di una chiave;
- catturare informazioni crittografiche che sfuggano dall'immobilizer durante il processo di handshake;
- trovare a forza bruta l'algoritmo del key fob;
- clonare il key fob;
- disturbare il segnale del key fob;
- scaricare il key fob.

Sensore di controllo della pressione degli pneumatici

Un attaccante potrebbe sfruttare la connessione **TPMS** (*Tire Pressure Monitor Sensor*, sensore di controllo della pressione degli penumatici) per:

- inviare una condizione impossibile all'unità di controllo del motore (**ECU**, *Engine Control Unit*), provocando un guasto che poi possa essere sfruttato;
- trarre in inganno l'ECU perché effettui una correzione eccessiva per condizioni dissestate della strada;
- portare il ricevitore TPMS o l'ECU in uno stato non recuperabile, il che potrebbe far sì che il guidatore accosti per verificare uno pneumatico dichiarato a terra dal sistema, o che potrebbe addirittura far spegnere il veicolo;
- tracciare un veicolo sulla base degli ID univoci dei TPMS;
- sostituire il segnale TPMS in modo da attivare segnali d'allarme interni.

Console di infotainment

Un attaccante potrebbe sfruttare la connessione alla console di infotainment per:

- mettere la console in modalità debug;
- modificare le impostazioni diagnostiche;
- trovare un bug di input che provochi risultati inattesi;
- installare malware sulla console;
- usare un'applicazione maligna per accedere alla rete del bus CAN interna;
- usare un'applicazione maligna per spiare le azioni degli occupanti del veicolo;
- usare un'applicazione maligna per falsificare i dati visualizzati all'utente, per esempio la posizione del veicolo.

USB

Un attaccante potrebbe usare una connessione a una porta USB per:

- installare malware nell'unità di infotainment;
- sfruttare una falla nello stack USB dell'unità di infotainment;
- collegare un dispositivo USB maligno con file opportunamente predisposti per penetrare elementi di importazione nell'unità di infotainment, come la rubrica degli indirizzi e i decodificatori MP3;
- installare aggiornamenti software modificati sul veicolo;
- mettere in corto circuito la porta USB, danneggiando di conseguenza il sistema di infotainment.

Bluetooth

Un attaccante potrebbe usare una connessione Bluetooth per:

- eseguire codice sull'unità di infotainment;
- sfruttare una falla nello stack Bluetooth dell'unità di infotainment;
- caricare informazioni malformate, per esempio una rubrica indirizzi corrotta progettata in modo tale da eseguire del codice;
- accedere al veicolo da breve distanza (meno di 100 metri);
- disturbare il dispositivo Bluetooth.

CAN (Controller Area Network)

Un attaccante potrebbe sfruttare la connessione al bus CAN per:

- installare un dispositivo dianostico maligno in grado di inviare pacchetti al bus CAN;
- inserirsi direttamente in un bus CAN per cercare di mettere in moto un veicolo senza disporre di una chiave;
- inserirsi direttamente in un bus CAN per caricare malware;
- installare un dispositivo diagnostico maligno per tracciare il veicolo;
- installare un dispositivo diagnostico maligno per consentire comunicazioni da remoto direttamente con il bus CAN, trasformando quello che normalmente sarebbe un attacco interno in una minaccia esterna.

Livello 2: disaggregazione del ricevitore

Al Livello 2, possiamo parlare maggiormente di identificazione di minacce specifiche. Esaminando quali applicazioni esattamente gestiscano le diverse connessioni, possiamo iniziare a effettuare una convalida sulla base delle possibili minacce.
Suddivideremo le le minacce in cinque gruppi: Bluez (il daemon Bluetooth), wpa_applicant (il daemon Wi-Fi), HSI (modulo kernel cellulare dell'interfaccia sincrona ad

alta velocità), udev (gestore dei dispositivi kernel) e il driver Kvaser (driver del ricetrasmettitore CAN). Negli elenchi che seguono, ho specificato le minacce per ciascun programma.

Bluez

Versioni vecchie o senza patch del daemon Bluez:

- potrebbero essere oggetto di exploit;
- potrebbero non essere in grado di gestire rubriche indirizzi corrotte;
- potrebbero non essere configurate in modo da garantire un'adeguata cifratura;
- potrebbero non essere configurate in modo da gestire un handshaking sicuro;
- potrebbero usare passkey di default.

wpa-applicant

- Versioni più vecchie potrebbero essere oggetto di exploit;
- potrebbero non applicare una adeguata cifratura wireless in stile WPA2;
- potrebbero connettersi a punti di accesso maligni;
- potrebbero lasciar sfuggire informazioni sul driver via BSSID (interfaccia di rete).

HSI

- Versioni più vecchie potrebbero essere oggetto di exploit;
- potrebbero essere suscettibili a comunicazioni seriali iniettabili (attacchi del tipo "man-in-the-middle", in cui chi attacca inserisce comandi seriali nel flusso di dati.

udev

- Versioni più vecchie o senza patch potrebbero essere suscettibili ad attacchi;
- potrebbero non avere una "lista bianca" aggiornata dei dispositivi, consentendo a un attaccante di caricare driver o dispositivi USB aggiuntivi non testati o che non dovrebbero poter essere usati;
- possono consentire a un attaccante di caricare dispositivi estranei, per esempio una tastiera, per accedere al sistema di infotainment.

Driver Kvaser

- Versioni più vecchie o senza patch potrebbero essere oggetto di exploit;
- potrebbero consentire a un attaccante di caricare firmware maligno nel dispositivo Kvaser.

Questi elenchi di potenziali vulnerabilità non sono affatto esaustivi, ma dovrebbero essere sufficienti a darvi un'idea di come funzioni la sessione di brainstorming. Se fosse

opportuno passare a una mappa delle potenziali minacce al vostro veicolo di Livello 3, dovreste scegliere uno dei processi, per esempio HSI, e iniziare a esaminare il sorgente del suo kernel per identificare metodi e dipendenze sensibili vulnerabili agli attacchi.

Sistemi di valutazione delle minacce

Avendo documentato molte delle nostre minacce, ora possiamo valutarle, attribuendo loro un livello di rischio. Sistemi di valutazione molto usati sono DREAD, ASIL e MIL-STD-882E. DREAD si usa comunemente nel Web testing, mentre il settore degli autoveicoli e quello governativo utilizzano rispettivamente ISO 26262 ASIL e MIL-STD-882E. Purtroppo, questi due standard sono focalizzati sui guasti di sicurezza e non sono adeguati alla gestione delle minacce maligne. Trovate maggiori informazioni su questi standard all'indirizzo *http://opengarages.org/index.php/Policies_and_Guidelines*.

Il sistema di valutazione DREAD

DREAD è un acronimo che sta per:

- **Damage potential** (potenziale di danno): quanto è grande il danno?
- **Reproducibility** (riproducibilità): quanto è facile riprodurlo?
- **Exploitability** (sfruttabilità): quanto è facile da attaccare?
- **Affected users** (utenti influenzati): quanti utenti ne sono influenzati?
- **Discoverability** (scopribilità): quanto è facile trovare la vulnerabilità?

La Tabella 1.1 elenca i livelli di rischio da 1 a 3 per ciascuna categoria di valutazione.

Tabella 1.1 - Sistema di valutazione DREAD.

	Categoria	Elevato (3)	Medio (2)	Basso (1)
D	Damage potential	Potrebbe modificare il sistema di sicurezza e guadagnarsi la fiducia totale, per prendere infine il controllo di tutto l'ambiente	Potrebbe lasciar sfuggire informazioni delicate	Potrebbe lasciar sfuggire informazioni banali
R	Reproducibility	È sempre riproducibile	Si può riprodurre solo se vale una condizione specifica o entro una certa finestra temporale	È molto difficile da riprodurre, anche avendo informazioni specifiche sulla vulnerabilità

	Categoria	Elevato (3)	Medio (2)	Basso (1)
E	Exploitability	Permette a un attaccante alle prime armi di eseguire l'exploit	Consente a un attaccante esperto di creare un attacco che potrebbe essere usato più volte	Consente di portare a termine l'attacco solo a un attaccante esperto con conoscenze approfondite
A	Affected users	Influenza tutti gli utenti, compreso l'utente e i clienti chiave del setup di default	Influenza alcuni utenti o alcuni specifici setup	Influenza una percentuale molto piccola di utenti; normalmente colpisce una caratteristica poco nota
D	Discoverability	Si può trovare facilmente in una spiegazione pubblicata dell'attacco	Influenza una parte usata di rado, il che significa che un attaccante dovrebbe essere molto creativo per scoprirne un uso maligno	È una minaccia poco chiara, il che significa che è improbabile che un attaccante trovi un modo per sfruttarla

Ora possiamo applicare ciascuna categoria DREAD della Tabella 1.1 a una minaccia identificata in precedenza in questo capitolo e attribuirle una valutazione di rischio, da basso (1) a elevato (3). Per esempio, se prendiamo le minacce HSI del Livello 2 analizzate in "Livello 2: disaggregazione del ricevitore" a pagina 10, possiamo determinare valutazioni delle minacce come quelle indicate nella Tabella 1.2.

Tabella 1.2 - Minacce HSI di Livello 2 con punteggi DREAD.

Minacce HSI	D	R	E	A	D	Totale
Una versione vecchia, senza patch di HSI che può essere oggetto di exploit	3	3	2	3	3	14
Una HSI che può essere suscettibile a comunicazioni seriali iniettabili	2	2	2	3	3	12

Possiamo stabilire la valutazione complessiva utilizzando i valori nella colonna del Totale, come indicato nella Tabella 1.3.

Tabella 1.3 - Punteggi di rischio DREAD.

Totale	Livello di rischio
5-7	Basso
8-11	Medio
12-15	Elevato

Quando si esegue una valutazione di rischio, è buona pratica visualizzare i risultati in forma di punteggio, in modo che chi legge possa capire meglio i rischi. Nel caso delle minacce HSI, possiamo attribuire un rischio elevato a tutte, come nella Tabella 1.4.

Tabella 1.4 - Minacce HSI di Livello 2 con punteggi DREAD.

Minacce HSI	D	R	E	A	D	Totale	Rischio
Una versione vecchia, senza patch di HSI che può essere oggetto di exploit	3	3	2	3	3	14	Elevato
Una HSI che può essere suscettibile a comunicazioni seriali iniettabili	2	2	2	3	3	12	Elevato

Entrambi i rischi sono elevati, ma si può vedere che la versione obsoleta del modello HSI presenta un rischio leggermente più elevato degli attacchi seriali iniettabili, perciò si può decidere di affrontare per prima cosa quel rischio. Si può anche vedere che il motivo per cui il rischio della comunicazione seriale iniettabile è più basso è che il danno e meno grave e l'exploit è più difficile da riprodurre di quello relativo a una versione vecchia di HSI.

CVSS: un'alternativa a DREAD

Se DREAD non è abbastanza dettagliata per voi, potete prendere in considerazione una metodologia di rischio più particolareggiata, nota con il nome di **CVSS** (*Common Vulnerability Scoring System*, sistema di valutazione comune della vulnerabilità).
CVSS offre molte categorie in più e consente di tener conto di molti più dettagli, rispetto a DREAD; si articola in tre gruppi: di base, temporale, ambientale. Ciascun gruppo a sua volta è suddiviso in sottoaree (sei per il gruppo base, tre per il temporale, cinque per l'ambientale), per un totale di 14 aree di valutazione!

NOTA

Per informazioni dettagliate su come funziona CVSS, vedete all'indirizzo *http://www.first.org/cvss/cvss-guide*.

NOTA

Potremmo usare gli standard ISO 26262 ASIL o MIL-STD-882E, nel valutare le minacce, ma vogliamo un livello di dettaglio maggiore che non il semplice Rischio = Probabilità x Gravità. Se dovete scegliere uno di questi due sistemi per una analisi di sicurezza, scegliete MIL-STD-882E del Dipartimento della Difesa (DoD). Il sistema Automotive Safety Integrity Level (ASIL) molto spesso ha una caduta del rischio nella classificazione QM, il che in sostanza lascia con un grosso punto interrogativo. Il sistema del DoD tende a dare una classificazione più elevata, il che equivale ad attribuire un valore più elevato al costo di una vita. Inoltre, MIL-STD-882E è nato in vista di un'applicazione a tutto il ciclo di vita di un sistema, incluso il suo smaltimento, il che si adatta bene a un ciclo di vita sicuro per lo sviluppo.

Lavorare con i risultati del modello delle minacce

A questo punto abbiamo una serie di mappe delle molte potenziali minacce al nostro veicolo e le abbiamo classificate per livello di rischio. E adesso?

Dipende da qual è l'obiettivo del vostro team. Per usare gergo militare, gli attaccanti sono la "squadra rossa" e i difensori la "squadra blu". Se fate parte della squadra rossa, per voi il passo successivo è iniziare ad attaccare le aree a più alto rischio che è probabile offrano anche le migliori possibilità di successo. Se fate parte della squadra blu, tornate al vostro diagramma dei rischi e intervenite su ciascuna minaccia con una contromisura.

Per esempio, se dovessimo prendere i due rischi visti nel paragrafo su "Il sistema di valutazione DREAD" a pagina 12, potremmo aggiungere a ciascuno una sezione di contromisure.

La Tabella 1.5 include la contromisura per il rischio di esecuzione di codice HSI e la Tabella 1.6 presenta la contromisura per il rischio di intercettazione HSI.

Tabella 1.5 - Rischio di esecuzione di codice HSI.

Minaccia	Esecuzione di codice nello spazio kernel
Rischio	Elevato
Tecnica di attacco	Sfrutta la vulnerabilità nelle versioni vecchie di HSI
Contromisure	Il kernel e i moduli del kernel devono essere aggiornati con le versioni più recenti

Tabella 1.6 - Intercettazione di comandi HSI.

Minaccia	Intercetta e inietta comandi dalla rete cellulare
Rischio	Elevato
Tecnica di attacco	Intercetta le comunicazioni seriali via HSI
Contromisure	Tutti i comandi inviati via rete cellulare sono con firma cifrata

Ora avete un elenco documentato di vulnerabilità ad alto rischio con le relative soluzioni. Potete stabilire un ordine di priorità per le soluzioni non ancora implementate, sulla base del rischio implicito nel non implementarle.

Riepilogo

In questo capitolo avete visto quanto sia importante usare modelli delle minacce per identificare e documentare le vostre condizioni per quanto riguarda la sicurezza, e far partecipare sia tecnici sia non tecnici alle sedute di brainstorming per immaginare i possibili scenari. Poi siamo scesi in profondità in questi scenari per identificare tutti i rischi potenziali. Grazie a un sistema di valutazione, abbiamo classificato e categorizzato ciascun rischio potenziale. Dopo aver valutato le minacce in questo modo, ci siamo ritrovati con un documento che definiva la situazione del nostro prodotto attuale per quanto riguarda la sicurezza, le eventuali contromisure già applicate e un elenco di compiti ad alta priorità che attendono ancora di essere affrontati.