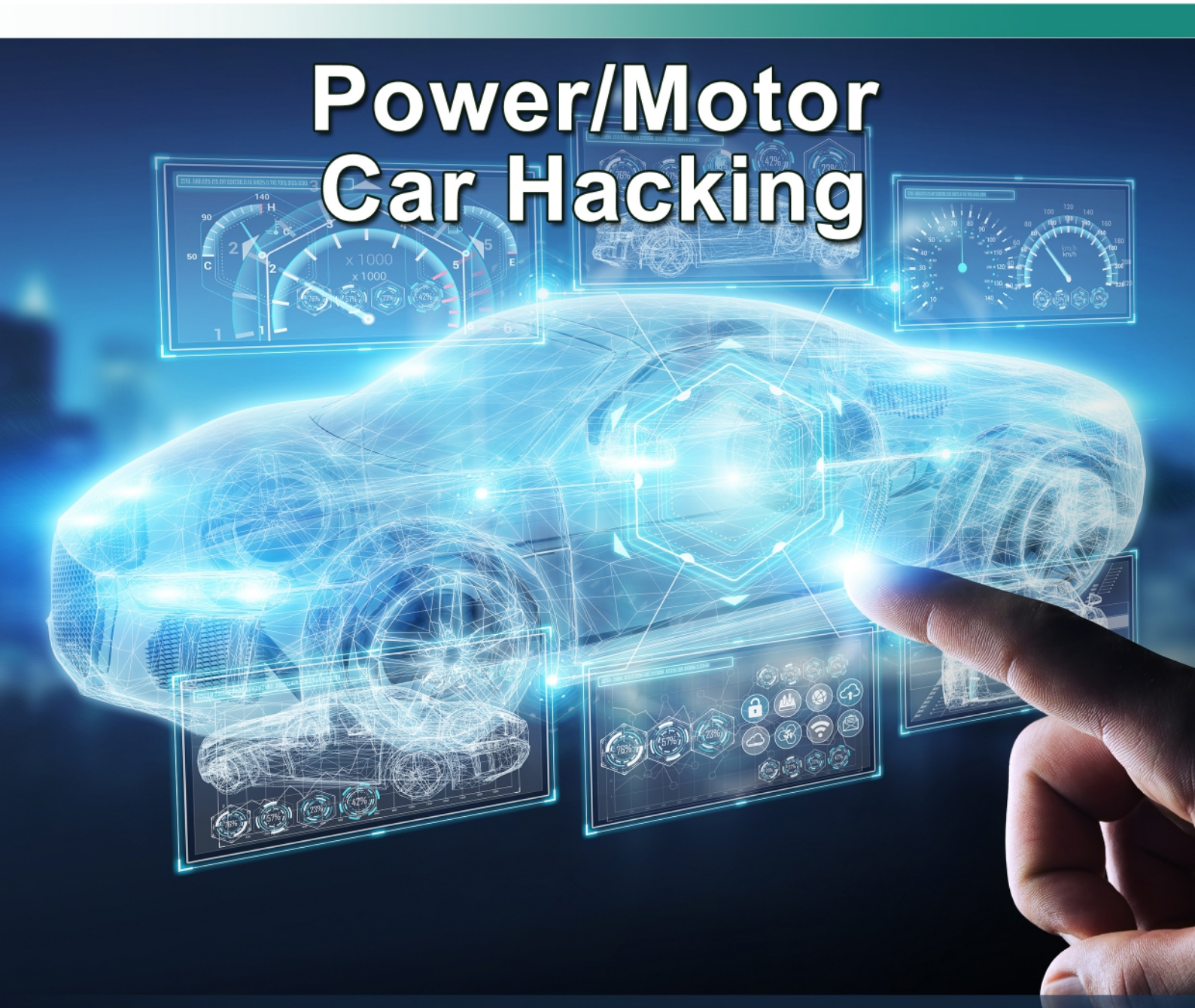
NUMERO 1 IN ITALIA SU ELETTRONICA EMBEDDED E SEMICONDUTTORI

Firmware 2.0

#45
Luglio 2024

Power/Motor Car Hacking



IN QUESTO NUMERO:

GLI SDR PER HACKERARE LO SPORTELLO DELL'AUTO

HACKRF ONE UNA GUIDA PRATICA: DALLA DECODIFICA DEI SEGNALI AL PENETRATION TESTING

CORSO DI ELETTRONICA PER RAGAZZI - PUNTATA 19

E MOLTI ALTRI ARTICOLI E PROGETTI!

it.emcelettronica.com

Elettronica Open Source

PROFESSIONAL & MAKER ZONE

PCBWay

CELEBRA 10 ANNI DI INNOVAZIONE

Un decennio di crescita e impegno costante all'eccellenza

10° ANNIVERSARIO DI PCBWAY

Unisciti a noi per celebrare il 10° anniversario di PCBWay. Da umili inizi nel 2014, PCBWay è diventata un leader globale nella produzione di elettronica, nota per prototipi di PCB di alta qualità e servizi di assemblaggio.

CRESCITA TECNOLOGICA

Nell'ultimo decennio, PCBWay ha ampliato la sua offerta per includere PCB avanzati come multistrato, flessibili e rigidi-flessibili. Il nostro continuo investimento in tecnologia all'avanguardia garantisce precisione e affidabilità per progetti elettronici complessi.

FOCUS SUL CLIENTE

Il successo di PCBWay deriva dal suo approccio centrato sul cliente. Con una piattaforma online facile da usare, preventivi istantanei e supporto completo, abbiamo attratto oltre 500.000 ingegneri ed appassionati di elettronica in tutto il mondo.

SOSTENIBILITÀ E COMUNITÀ

PCBWay si impegna per la sostenibilità e il coinvolgimento della comunità, supportando progetti educativi e favorendo l'innovazione nell'elettronica. Siamo all'avanguardia della tecnologia e dei servizi PCB, pronta ad esplorare nuove innovazioni.

www.pcbway.com

service@pcbway.com

Firmware 2.0 EDITORIAL PLAN 2024

COSA LEGGERAI NEL 2024?

TOPICS	MAKERS ZONE	DATA DI PUBBLICAZIONE
Wireless/RF	Audio/Video	1 Febbraio
PCB	PCB Design	1 Marzo
Artificial Intelligence	Robotics	1 Aprile
Arduino	Open Source Projects	1 Maggio
Medical	Wearable	1 Giugno
Power/Motor	Car Hacking	1 Luglio
IoT	MEMS&Smart Sensors	1 Settembre
Renewable Energy	Smart Projects	1 Ottobre
Industry 4.0	Remote control	1 Novembre
Test&Measurements	Analog&Digital Signals	1 Dicembre

Oltre il motore: hacking e innovazione nel mondo delle auto connesse

Cari lettori,

benvenuti al nuovo numero di Firmware 2.0, la vostra rivista di riferimento che vi consente di avere sempre a portata di mano un intero mondo di informazioni e nozioni tecniche, permettendovi di restare aggiornati sull'elettronica ovunque vi troviate e di portare l'innovazione sempre con voi. Questo mese ci addentriamo in un argomento di grande interesse e attualità: Power/Motor - Car Hacking. Il settore power sta attraversando una trasformazione straordinaria, spinto da innovazioni che mirano a rendere i veicoli non solo più efficienti, ma anche più sostenibili. Motori più potenti e sistemi di gestione energetica intelligenti stanno creando un'esperienza di guida più fluida e reattiva, trasformando il modo in cui percepiamo la mobilità. Tuttavia, questa rapida evoluzione tecnologica non è priva di sfide.

Con l'aumento della connettività nei moderni veicoli, emergono nuove vulnerabilità che richiedono la nostra attenzione. L'hacking automobilistico rappresenta una delle preoccupazioni principali in questo contesto. I veicoli odierni sono essenzialmente computer su ruote, dotati di una complessa rete di sistemi elettronici che gestiscono praticamente tutto, dalla navigazione al controllo del motore. La connettività offre innumerevoli vantaggi, come la possibilità di aggiornamenti software remoti, miglioramenti continui delle funzionalità e monitoraggio in tempo reale per garantire la sicurezza. Allo stesso tempo, apre la porta a potenziali minacce.

L'hacking automobilistico può manifestarsi in diverse forme. Potrebbe trattarsi di un'intrusione nel sistema di infotainment per accedere a dati personali o, in casi più estremi, di un attacco ai sistemi di controllo del veicolo. Nelle auto a guida autonoma queste minacce assumono una dimensione ancora più critica. Un hacker potrebbe teoricamente prendere il controllo del sistema di guida, mettendo a rischio non solo il veicolo stesso ma anche la sicurezza dei passeggeri e degli altri utenti della strada. Per tale motivo, è fondamentale che i produttori e gli sviluppatori implementino misure di sicurezza avanzate e rigide al fine di proteggere i veicoli da tali rischi. Nonostante queste preoccupazioni, l'hacking non è sempre sinonimo di pericolo, esiste infatti un lato positivo rappresentato dall'hacking etico che svolge un ruolo fondamentale nel rafforzare la sicurezza. Gli hacker etici lavorano incessantemente per identificare e correggere le vulnerabilità prima che possano essere sfruttate dai malintenzionati. Questo impegno costante da parte dei ricercatori della sicurezza contribuisce a rendere i sistemi automobilistici sempre più resilienti e sicuri.

In questo numero di Firmware 2.0 esploriamo in profondità tutte queste tematiche. Vi porteremo alla scoperta delle ultime innovazioni nel settore power, analizzando come le nuove tecnologie stiano plasmando il futuro della mobilità, e approfondiremo rischi, opportunità e sfide legate all'hacking automobilistico esaminando cosa ci riserva il domani in termini di sicurezza e sostenibilità. Grazie per essere parte della nostra grande community. Restate connessi per rimanere aggiornati sulle ultime novità del mondo elettronico e delle tecnologie emergenti.

Buona lettura!

Giordana Francesca Brescia

A tutta velocità

Affidatevi al leader nell'introduzione di nuovi prodotti™ per passare dall'idea al prototipo alla velocità della luce

mouser.it

MOUSER ELECTRONICS

Power/Motor Car Hacking

Founder&Editor
Emanuele Bonanni

CFO
Lidia Balica

Editorial Assistant
Maria Pisani

Maker in Chief
Giordana Francesca Brescia

Advertising & Marketing
Cristian Balica
cristian@contangosl.com

Graphic Designer
Marilde Mirra

Circulation
Users - 147.344
Social Network - 131.632

ABBONATI A

Firmware 2.0

PER AVERE **TUTTA L'ELETTRONICA A PORTATA DI CLICK** E RESTARE SEMPRE **AGGIORNATO SULL'ELETTRONICA EMBEDDED, I MICROCONTROLLORI** E **L'INNOVAZIONE TECNOLOGICA**

Elettronica Open Source

GLI SDR PER HACKERARE LO SPORTELLO DELL'AUTO

di **Andrea Garrapa**

Un sistema di accesso remoto senza chiave (Remote Keyless System - RKS) si riferisce semplicemente a qualsiasi serratura elettronica che funzioni senza l'uso di una chiave meccanica. Nel settore automotive, di solito, si presenta sotto forma di un portachiavi o di telecomando integrato nella chiave dell'auto, con pulsanti che comunicano utilizzando segnali a radiofrequenza (RF). I comandi vengono inviati verso il ricevitore integrato nel veicolo per eseguire una determinata azione, come bloccare o sbloccare la portiera. Per ovvie ragioni, i telecomandi per auto sono incredibilmente convenienti, ma questa comodità comporta un rischio, certamente piccolo, di pirateria informatica. In questo articolo, vedremo quali componenti hardware possono essere utilizzati dagli hacker per sbloccare lo sportello di un'auto.

INTRODUZIONE

Quando si preme il pulsante di sblocco della portiera di un'auto, dal telecomando viene inviato un segnale radio modulato che viene captato da un ricevitore nell'auto. Se il codice modulato corrisponde a quello dell'auto, lo sportello si sbloccherà. Ma sarebbe incredibilmente facile da hackerare senza alcuna sicurezza aggiuntiva. Tutto ciò che un hacker dovrebbe fare è registrare il segnale radio e riprodurlo in un secondo momento: un classico **attacco di replay**.
Per contrastare questa possibilità, i moderni telecomandi utilizzano un sistema a codice variabile, chiamato **rolling code**. Ogni volta che si preme il pulsante di sblocco, il telecomando utilizza un algoritmo per generare un nuovo codice. L'auto conosce lo stesso algoritmo e i vecchi codici vengono scartati ogni volta che ne viene generato uno nuovo. Ciò impedisce agli hacker di eseguire semplicemente un attacco replay, ma il sistema presenta ancora una vulnerabilità, che è ciò che sfrutta l'**attacco Rolljam**.

L'ATTACCO ROLLJAM

L'attacco Rolljam funziona registrando e bloccando il segnale radio proveniente dal telecomando. Poiché il segnale è stato bloccato, lo sportello dell'auto non si sblocca e il proprietario naturalmente riproverà premendo di nuovo il pulsante. Ciò crea un secondo segnale che viene anch'esso registrato e bloccato, ma in simultanea l'aggressore trasmette il primo codice per sbloccare la porta. Il proprietario non ne è consapevole, ma ora l'aggressore conosce il codice successivo nella sequenza (non ancora scaduto) e può usarlo per sbloccare l'auto a suo piacimento.
Per ricreare un attacco Rolljam bastano pochi semplici componenti hardware, un laptop e alcuni strumenti software open source. Uno dei componenti hardware richiesti è un dispositivo **SDR** (**Software-Defined Radio**) che viene utilizzato per registrare il segnale originale.

RADIO DEFINITA DAL SOFTWARE

Un SDR (radio definita dal software) è un sistema radio in cui componenti tradizionalmente implementati nell'hardware, come filtri e demodulatori, sono invece implementati nel software. La configurazione prevede in genere un front-end RF e un convertitore analogico-digitale, collegato a un computer tramite USB. Il computer esegue compiti complessi, come la demodulazione, che si riferisce all'estrazione del segnale originale da un'onda portante.

L'idea alla base di SDR è quella di avere un dispositivo in grado di ricevere e trasmettere diversi protocolli radio semplicemente configurando il suo software.
Un comune **dongle sintonizzatore TV USB** può essere utilizzato per inviare dati I/Q grezzi (in fase e quadratura, riferendosi alle componenti reale e immaginaria di un segnale RF) a un computer. Pertanto, è diventato conveniente per l'hobbista medio avere un analizzatore di spettro a banda larga. Inoltre, i progressi nell'hardware e nel software informatici hanno consentito l'analisi dei segnali complessi utilizzando software basati su grafici di flusso, come **GNURadio**, in grado di manipolare, decodificare e codificare dati da utilizzare con radio definite dal software.

ALCUNI SDR

Andremo ora a descrivere i principali hardware SDR presenti sul mercato, che possono svolgere le funzionalità richieste per hackerare la portiera di un'auto e non solo.

Figura 1: Il dispositivo SDR HackRF One

HACKRF ONE

HackRF One (in **Figura 1**) è un dispositivo SDR che consente agli utenti di trasmettere o ricevere segnali radio in una gamma di frequenze compresa tra 1 MHz e 6 GHz e larghezza di banda fino a 20 MHz. È una piattaforma hardware open source che funziona come periferica USB o la si può personalizzare per funzionare come soluzione autonoma.

HackRF One è uno dei dispositivi SDR più popolari sul mercato. La popolarità di HackRF One deriva da molti dei suoi vantaggi, come:

- La sua capacità di ricevere e trasmettere segnali radio nella gamma da 1 MHz a 6 GHz
- Compatibilità con software open source come GNURadio
- Avere una comunità notevole
- Documentazione ben scritta

Uno degli svantaggi di HackRF One è che ha una fascia di prezzo relativamente alta (300 euro), il che potrebbe renderlo inaccessibile ad alcuni studenti o autodidatti. Un altro aspetto negativo è che HackRF One richiede

funzionare ovunque in tutto il mondo.

Il dispositivo dispone di un'interfaccia basata su browser che consente di monitorare e controllare le cose sul proprio computer e device mobile. L'interfaccia ha un design piuttosto semplice in modo da poter controllare l'attività con pochi clic di un pulsante. La sua interfaccia consente anche connessioni web simultanee. Ogni connessione può sintonizzare un canale ricevitore indipendente su un intero spettro e ciò rende questo dispositivo abbastanza versatile.

Un'altra cosa impressionante di questo SDR è che ha la calibrazione automatica della frequenza tramite la temporizzazione GPS ricevuta, quindi non è necessario dedicare tempo alla calibrazione manuale. C'è anche un'interfaccia di estensione che consente di aggiungere decodificatori e utilità se si desidera fare ciò. Ha una gamma di frequenza compresa tra 10 kHz e 30 MHz.

NOOELEC NESDR

Il *NooElec NESDR* è un dongle USB DVB-T modificato e ottimizzato per l'utilizzo come SDR. Include condensatori e induttori selezionati che gli consentono di offrire

APACER: SOLUZIONI DI SUCCESSO PER LO STORAGE DIGITALE

di **Redazione**

Apacer è oggi una delle principali aziende nel settore della tecnologia dell'informazione e della comunicazione, specializzata nella produzione di dispositivi di memoria digitale e soluzioni di storage avanzate. Sin dalla sua nascita, Apacer ha puntato sull'innovazione e sulla qualità, offrendo una vasta gamma di prodotti che rispondono alle esigenze di un mercato in continua evoluzione, coprendo sia il segmento consumer che quello industriale.

Apacer si distingue nel settore della tecnologia dell'informazione e della comunicazione, con una particolare enfasi sui dispositivi di memoria digitale e soluzioni di storage. L'azienda è riconosciuta per la sua innovazione e qualità, offrendo una vasta gamma di prodotti che soddisfano le esigenze di consumatori, professionisti e aziende in tutto il mondo.
La serie dei suoi prodotti è vasta e diversificata, includendo moduli di memoria **DRAM**, **SSD** (**Solid State Drive**), **schede di memoria**, unità flash USB e soluzioni di storage industriali.

I moduli di memoria DRAM di Apacer sono progettati per offrire prestazioni elevate e affidabilità, risultando ideali per computer desktop, laptop e server. La gamma di SSD è particolarmente apprezzata per le sue elevate velocità di lettura e scrittura, la durata, la stabilità e l'efficienza energetica, rendendoli una scelta eccellente per migliorare le prestazioni dei sistemi informatici. Gli SSD (Solid State Drive) rappresentano un settore di eccellenza per Apacer, con prodotti che si distinguono per velocità di lettura e scrittura eccezionali, lunga durata ed efficienza energetica, ideali per incrementare le prestazioni di qualsiasi sistema informatico.
Nel segmento delle soluzioni di storage industriale, Apacer offre prodotti progettati per resistere a condizioni ambientali critiche.

Questi dispositivi sono costruiti per operare in ambienti difficili caratterizzati da temperature estreme, vibrazioni e altre condizioni avverse, garantendo un funzionamento affidabile anche nelle situazioni più impegnative. Le schede di memoria e le unità flash USB di Apacer sono conosciute per la loro robustezza, qualità costruttiva e alte prestazioni, e vengono ampiamente utilizzate da professionisti che necessitano di soluzioni di storage portatili, affidabili e sicure. Oltre all'hardware, Apacer sviluppa anche soluzioni software per la gestione e la sicurezza dei dati. Questi strumenti includono funzionalità di backup, recupero e sicurezza crittografica dei dati, progettati per integrarsi perfettamente con i prodotti hardware dell'azienda, offrendo un'esperienza utente completa e senza problemi.

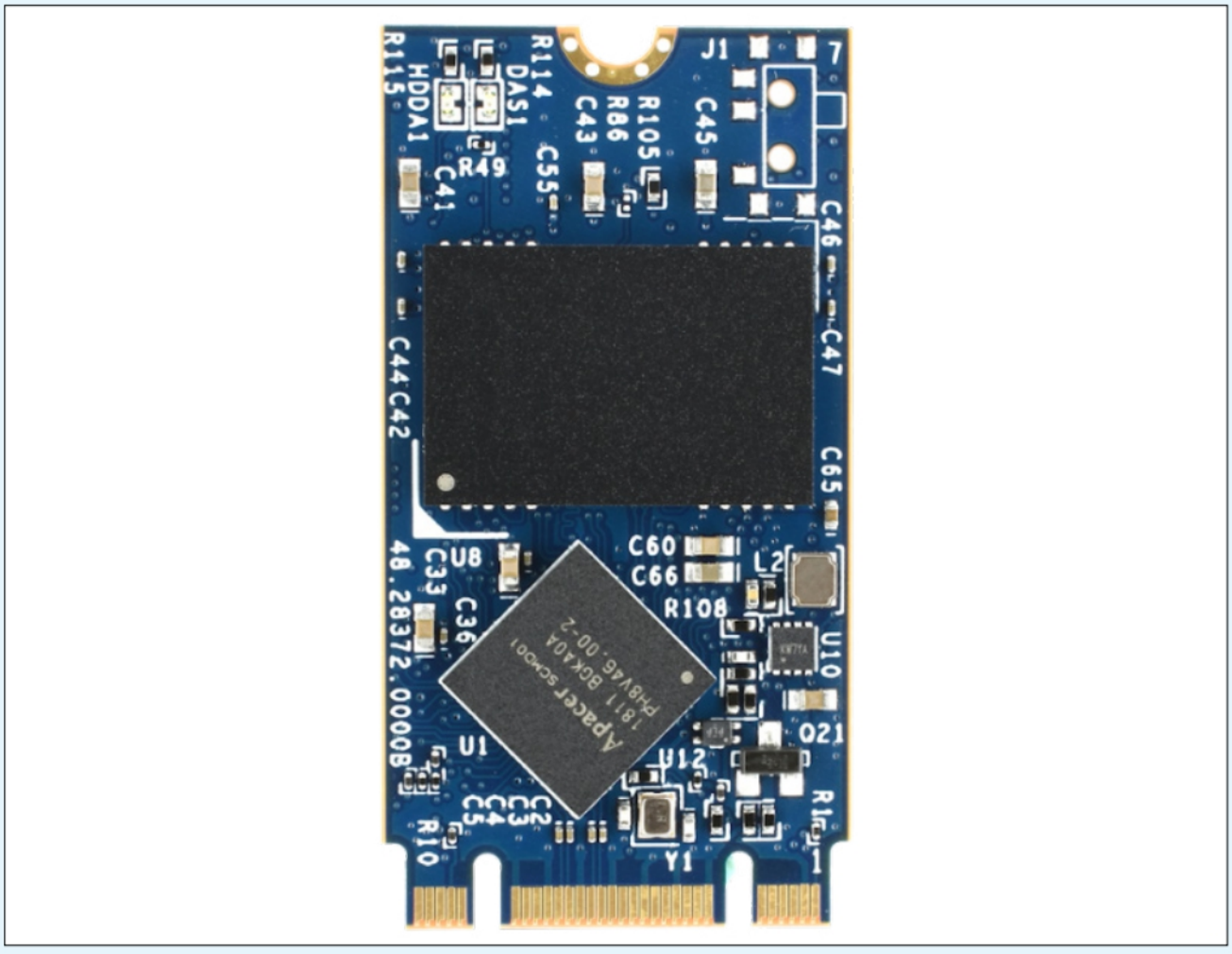
L'innovazione è al centro della filosofia aziendale di Apacer, che investe costantemente in ricerca e sviluppo per rimanere all'avanguardia della tecnologia. L'impegno profuso verso l'innovazione si riflette nei numerosi brevetti e nelle tecnologie proprietarie che l'azienda ha sviluppato nel corso degli anni, consentendo ad Apacer di anticipare le tendenze del mercato e rispondere prontamente alle nuove esigenze dei clienti. La qualità è un altro pilastro fondamentale.

Ogni prodotto è sottoposto a rigorosi test per garantire che rispetti gli elevati standard dell'azienda. Inoltre, Apacer offre un eccellente supporto post-vendita, con un team di esperti sempre pronti ad assistere i clienti, garantendo una soddisfazione completa, e si distingue anche per il suo approccio ecologico e sostenibile.

L'azienda adotta pratiche di produzione rispettose dell'ambiente, riducendo l'impatto ecologico e promuovendo un utilizzo responsabile delle risorse. Tale impegno nei confronti della sostenibilità riflette il livello di consapevolezza dell'azienda verso le responsabilità ambientali e sociali.

CASO STUDIO: POTENZIARE L'AUTOMAZIONE DELLA BIGLIETTERIA CON LE SOLUZIONI SSD AFFIDABILI DI APACER

Innovazione e ricerca sono al centro della filosofia di Apacer. L'azienda, infatti, investe costantemente in ricerca e sviluppo per rimanere all'avanguardia della tecnologia e soddisfare le mutevoli esigenze del mercato. Con il progresso tecnologico, l'**automazione della biglietteria** è diventata una caratteristica comune nelle città moderne.


R115
HDDA1
R114
DAS1
R49
C41
C55
R105
R86
C43
C45
J1
C46
C47
C44
C42
C65
C60
C66
R108
U8
C33
C36
48.28372.0000B
U1
U10
Q21
U12
Y1
R10
Apacer SCH001
PH8V46.00.2

Particolarmente nell'acquisto di biglietti per il trasporto pubblico, l'automazione è quasi onnipresente. Questa tecnologia non solo si allinea con le tendenze ESG (Environmental, Social, and Governance), sostituendo la carta con il digitale per ridurre gli sprechi, ma migliora anche l'esperienza utente per i consumatori. Inoltre, consente ai fornitori di servizi di incrementare l'efficienza operativa, risparmiare sui costi e rimanere operativi 24 ore su 24. Il cliente che collabora con Apacer in questo progetto è un integratore di sistemi di automazione di biglietterie all'avanguardia, specializzato nella fornitura di soluzioni per ferrovie locali o pubbliche. Assicurare la stabilità del sistema è fondamentale per il funzionamento dell'automazione della biglietteria. Apacer fornisce SSD di alta qualità, altamente stabili e su misura per soddisfare le esigenze del cliente, offrendo soluzioni ottimali.

Il cliente ha affrontato sfide significative a causa di improvvisi crash mentre utilizzava SSD di altre marche. Per affrontare questo problema e garantire una maggiore stabilità nelle operazioni successive, ha cercato fornitori di moduli di memoria in grado di soddisfare le loro specifiche e i requisiti di qualità. Il team tecnico professionale di Apacer ha analizzato l'ambiente di utilizzo del sistema del cliente e ha identificato che le temperature operative più alte del previsto stavano influenzando le prestazioni degli SSD. Di conseguenza, Apacer ha raccomandato SSD con operatività a temperatura ampia, garantendo funzionalità in un intervallo di temperature che vanno da -40 a 85 gradi Celsius.

L'SSD Apacer **SV250-M242**, sfruttando la tecnologia **3D NAND** per una capacità aumentata fino a 960GB e una maggiore efficienza energetica rispetto alla tecnologia 2D NAND, rappresenta la prossima generazione di unità a stato solido (SSD) con capacità di archiviazione compatte e ad alta velocità. Dotato di un robusto controller SATA che supporta l'ECC (*Error Correction Code*) sul modulo e un efficiente schema di livellamento dell'usura, insieme a un motore ECC LDPC (*Low Density Parity Check*), questo SSD estende la durata e migliora l'affidabilità dei dati.

Inoltre, il modello SV250-M242 è equipaggiato con un **sensore termico integrato** per monitorare la temperatura dell'SSD tramite comandi S.M.A.R.T., prevenendo efficacemente il surriscaldamento. Integra anche la più recente tecnologia S.M.A.R.T. di Apacer, principalmente orientata al monitoraggio e all'analisi della durata dell'unità. Fornisce agli utenti comandi e sottocomandi per accedere alle informazioni sullo stato dell'unità e anticipare potenziali guasti. Gli utenti possono utilizzare questi comandi/sottocomandi per monitorare la salute dell'SSD supportata dal firmware per controller SATA. Per applicazioni che richiedono un'intensità elevata, la protezione dei dati end-to-end garantisce l'integrità in più punti del percorso di trasferimento, facilitando una consegna affidabile dei dati. L'implementazione degli SSD ad ampio range di temperatura ha risolto i problemi del cliente, consentendo un'operatività fluida del sistema durante i test intensivi. Soddisfatto del miglioramento, il cliente sta considerando l'integrazione di altri SSD di Apacer con tecnologie a valore aggiunto da implementare nel prossimo prodotto.

Questo segna l'inizio di una relazione reciprocamente vantaggiosa. In definitiva, Apacer rappresenta un punto di riferimento nelle soluzioni di storage e delle memorie digitali, grazie alla sua vasta gamma di prodotti innovativi, alla qualità ineccepibile e all'impegno costante verso le esigenze e la completa soddisfazione del cliente.

La sua capacità di adattarsi rapidamente alle nuove tecnologie e di anticipare le esigenze del mercato lo rende una scelta privilegiata per chi cerca soluzioni di storage affidabili e performanti. L'azienda continua a crescere e ad evolversi, mantenendo salda la sua posizione di leader tecnologico e offrendo soluzioni affidabili e performanti in un mercato sempre più competitivo.

Apacer

L'autore è a disposizione nei commenti per eventuali approfondimenti sul tema dell'Articolo. Di seguito il link per accedere direttamente all'articolo sul Blog e partecipare alla discussione:
https://it.emcelettronica.com/apacer-soluzioni-di-successo-per-lo-storage-digitale

HACKRF ONE UNA GUIDA PRATICA: DALLA DECODIFICA DEI SEGNALI AL PENETRATION TESTING – PRIMA PARTE

di **William Thorossian**

Risalente al 2014, l'HackRF One è un dispositivo innovativo nel panorama della sicurezza informatica e delle radiofrequenze. Questo dispositivo open-source ha trasformato radicalmente l'approccio al penetration testing e all'hacking, offrendo un'opzione potente e accessibile. Operante su un'ampia gamma di frequenze, da 1MHz a 6GHz, l'HackRF One si distingue per la sua versatilità, consentendo agli utenti non solo di analizzare, ma anche manipolare e sperimentare con i segnali radio. Scopri in questo articolo come questo strumento è riuscito a democratizzare l'accesso alla tecnologia wireless avanzata, aprendo le porte ad una varietà di individui, dalla community degli hacker agli appassionati indipendenti. Attraverso la sua impronta indelebile nella sicurezza informatica, l'HackRF One continua a essere il punto di riferimento per chi cerca di esplorare le complesse reti delle comunicazioni wireless e affrontare le sfide della sicurezza nel mondo digitale sempre in evoluzione. In questa prima parte dell'articolo, affronteremo un viaggio attraverso l'HackRF One, presentando il dispositivo e le sue potenzialità.

L'HACKRF ONE: UNO STRUMENTO RIVOLUZIONARIO PER LA RICERCA IN CAMPO WIRELESS

L'**HackRF One** (vedi **Figura 1**) introdotto nel **2014**, e prodotto dalla **Great Scott Gadgets**, rappresenta un fondamentale punto di svolta nel panorama della sicurezza informatica e della radiofrequenza. Questo dispositivo open-source ha rivoluzionato la comunità dei professionisti del **penetration testing** e degli appassionati di hacking, fornendo un'opzione accessibile e potente per esplorare il vasto spettro delle radiofrequenze.

Con la capacità di operare su una gamma estesa da **1MHz** a **6GHz**, l'HackRF One si distingue per la sua versatilità. Gli utenti hanno la possibilità di ricevere segnali, decodificarli, apportare modifiche, riprodurli e trasmetterli, aprendo la strada ad una vasta gamma di applicazioni pratiche. Questo strumento non solo consente di analizzare e comprendere i segnali radio, ma offre anche la capacità di intervenire su di essi per scopi di sperimentazione, ricerca e sicurezza.

Oltre al suo ruolo cruciale nel campo della sicurezza informatica, l'HackRF One ha promosso la democratizzazione dell'accesso alla tecnologia RF avanzata. La sua accessibilità economica ha permesso a una gamma più ampia di individui, dai ricercatori indipendenti agli appassionati, di esplorare le potenzialità delle radiofrequenze e di contribuire allo sviluppo di nuove applicazioni e tecnologie.

L'impatto dell'HackRF One si estende ben oltre la sua data di lancio, poiché continua a essere una risorsa chiave per coloro che cercano di approfondire la comprensione delle comunicazioni wireless e delle possibili vulnerabilità. In un contesto in cui la sicurezza informatica è una priorità sempre crescente, dispositivi come l'HackRF One svolgono un ruolo cruciale nel potenziare la comunità globale della sicurezza informatica e nel promuovere l'innovazione nel campo della radiofrequenza.

FUNZIONALITÀ E VERSATILITÀ DELL'HACKRF ONE

L'HackRF One, con le sue capacità di ricetrasmissione **half-duplex** e la sua straordinaria copertura da **1MHz** a **6GHz**, si colloca al centro dell'innovazione nel campo della radiofrequenza. La sua larghezza di banda fino a **20MHz** fornisce una risoluzione dettagliata e una vasta gamma di opzioni per l'analisi dei segnali, rendendolo uno strumento versatile e potente per una varietà di applicazioni. In **Figura 2** potete vedere lo schema a blocchi di funzionamento della scheda.

La compatibilità dell'HackRF One con le principali

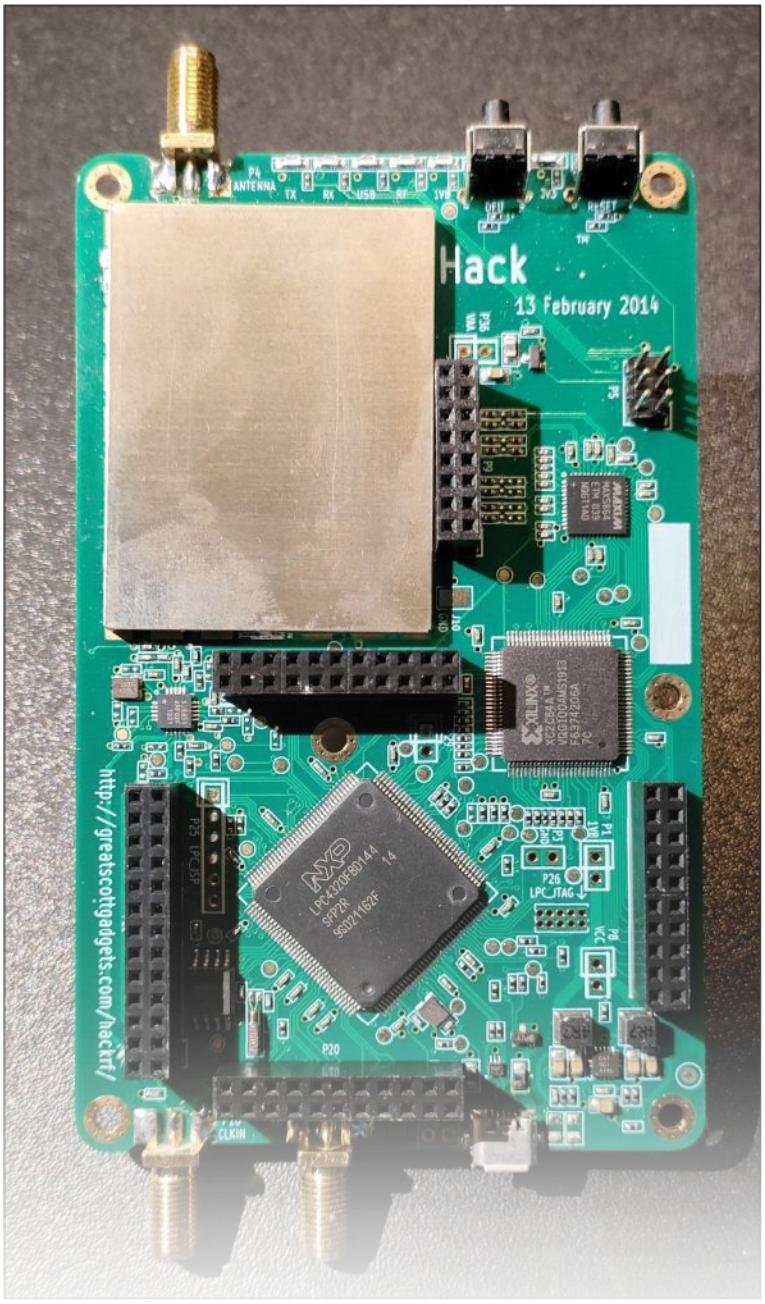


Figura 1: La scheda HackRF One

cità di ricevere e trasmettere su un'ampia gamma di frequenze offre agli scienziati e ai ricercatori uno strumento fondamentale per esplorare e sperimentare con le proprietà delle onde elettromagnetiche. Nell'ambito delle telecomunicazioni, l'HackRF One consente agli ingegneri di testare e ottimizzare le reti wireless, contribuendo così allo sviluppo di tecnologie di comunicazione sempre più efficienti.

Inoltre, la sua presenza nella comunità degli appassionati di radiofrequenza (Ham radio) ha aperto nuove opportunità per l'apprendimento e la creatività. Gli hobbisti possono esplorare il vasto mondo delle radiofrequenze, imparare a decodificare segnali e contribuire allo sviluppo di nuovi progetti e applicazioni.

In sintesi, l'HackRF One non è solamente uno strumento tecnologico avanzato, ma funge da ponte tra la teoria e la pratica in molteplici campi. La sua adattabilità e la vasta gamma di frequenze coperte lo rendono un alleato indispensabile per chiunque desideri esplorare, comprendere e sfruttare il potenziale delle radiofrequenze.

I MODULI DI ESPANSIONE: IL PORTAPACK

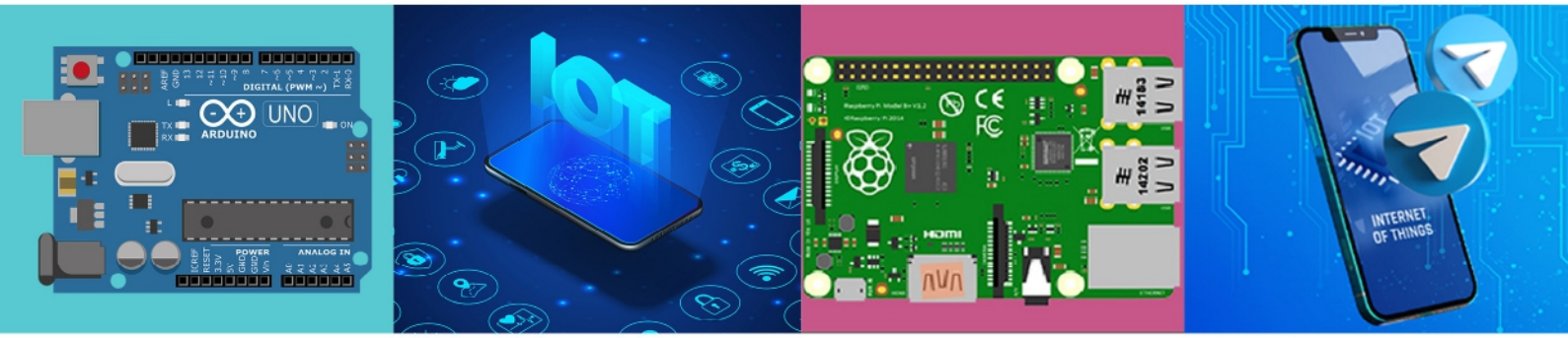
L'HackRF One è un dispositivo versatile e potente progettato per esplorare e sperimentare con le comunicazioni radio. La sua flessibilità è ulteriormente ampliata con l'aggiunta di schede Add-On come il **Portapack** (vedi **Figura 3**).

Il Portapack è un accessorio progettato appositamente per migliorare l'usabilità [illegible] trasformandolo in una

MY ACADEMY

La piattaforma di Elettronica Open Source dedicata ai corsi

SEI UN **MAKER** O UN **HOBBISTA** DELL'**ELETTRONICA**?



CON I CORSI **MAKERS ACADEMY** PUOI **MIGLIORARE LE TUE COMPETENZE ELETTRONICHE O ACQUISIRLE ANCHE PARTENDO DA ZERO**

MAKERS ACADEMY

SCOPRI I CORSI!

HACKRF ONE UNA GUIDA PRATICA: DALLA DECODIFICA DEI SEGNALI AL PENETRATION TESTING – SECONDA PARTE

di **William Thorossian**

Proseguiamo il nostro viaggio nell'universo dell'HackRF One. In questa seconda ed ultima parte dell'articolo, ci immergeremo in dettagli affascinanti e pratici, esplorando casi studio che evidenziano la potenza e la versatilità di questo dispositivo nella manipolazione dei segnali wireless. Nella seconda parte di questo approfondimento, ci concentreremo su tre ambiti chiave: Manipolazione GPS, Analisi RFID e Sniffing Bluetooth.

La Manipolazione GPS ci porterà nel cuore delle vulnerabilità legate alla geo localizzazione, rivelando come l'HackRF One possa essere utilizzato per alterare i dati GPS e, di conseguenza, influenzare la precisione e l'affidabilità dei dispositivi di navigazione satellitare. Successivamente, ci addentreremo nell'Analisi RFID, esaminando come l'HackRF One si riveli un alleato potente nella decodifica e manipolazione delle informazioni trasmesse dai sistemi RFID. Analizzeremo casi studio in cui la sua flessibilità apre nuove prospettive nella sicurezza degli accessi e nella gestione delle identità, svelando potenziali rischi e strategie di difesa. Infine, esploreremo il mondo dello Sniffing Bluetooth con l'HackRF One, rivelando come questo strumento consenta di scrutare le comunicazioni Bluetooth, aprendo scenari di potenziale vulnerabilità e dimostrando come possa essere utilizzato per migliorare la sicurezza di tali protocolli. Un'immersione approfondita in questi casi studio rivelerà la portata delle capacità dell'HackRF One nel contesto di sicurezza informatica, offrendo una prospettiva chiara su come questo dispositivo open-source continui a ridefinire il panorama della sicurezza wireless. Siate pronti a esplorare l'intricato intreccio tra sicurezza e sperimentazione, mentre ci addentriamo nella seconda parte di questo affascinante viaggio attraverso l'HackRF One.

CASO STUDIO 1: MANIPOLAZIONE GPS CON L'HACKRF ONE

Un esempio concreto e rivelatore delle potenziali implicazioni della manipolazione dei segnali GPS tramite l'HackRF One, è rappresentato dalla sua applicazione nell'analisi dei sistemi di navigazione veicolare, come abbiamo accennato in un precedente paragrafo. Immaginiamo un contesto in cui un ricercatore utilizza questo strumento per esaminare il traffico **GPS** di un veicolo. Attraverso l'interazione con i segnali GPS, l'HackRF One potrebbe consentire al ricercatore di individuare il segnale responsabile del blocco del sistema di navigazione del veicolo. Questa analisi approfondita potrebbe rivelare eventuali problemi di sicurezza nel sistema di navigazione o fornire informazioni preziose sulle modalità con cui potrebbe essere manipolato.

Da un punto di vista più critico, l'HackRF One potrebbe anche essere utilizzato malevolmente da un hacker per manipolare il segnale GPS di un dispositivo di localizzazione. Immaginiamo una situazione in cui un individuo malintenzionato utilizza lo strumento per alterare il segnale GPS di un veicolo o di un dispositivo di tracciamento personale. Questo potrebbe causare la scomparsa del dispositivo dal sistema di monitoraggio, nascondendo efficacemente la posizione del veicolo o dell'individuo. Un tale scenario solleva gravi preoccupazioni per la sicurezza, poiché potrebbe essere sfruttato per attività illegali, come il furto di veicoli o il monitoraggio non autorizzato delle persone.

La capacità dell'HackRF One di bloccare, manipolare o regolare i segnali GPS mette in luce la delicata intersezione tra la tecnologia e la sicurezza, richiamando l'attenzione sulla necessità di implementare misure robuste per proteggere i sistemi basati su GPS da potenziali minacce. Questi scenari illustrano chiaramente come l'utilizzo responsabile ed etico di strumenti quali l'HackRF One, sia essenziale per evitare abusi che potrebbero compromettere la sicurezza e la privacy delle persone.

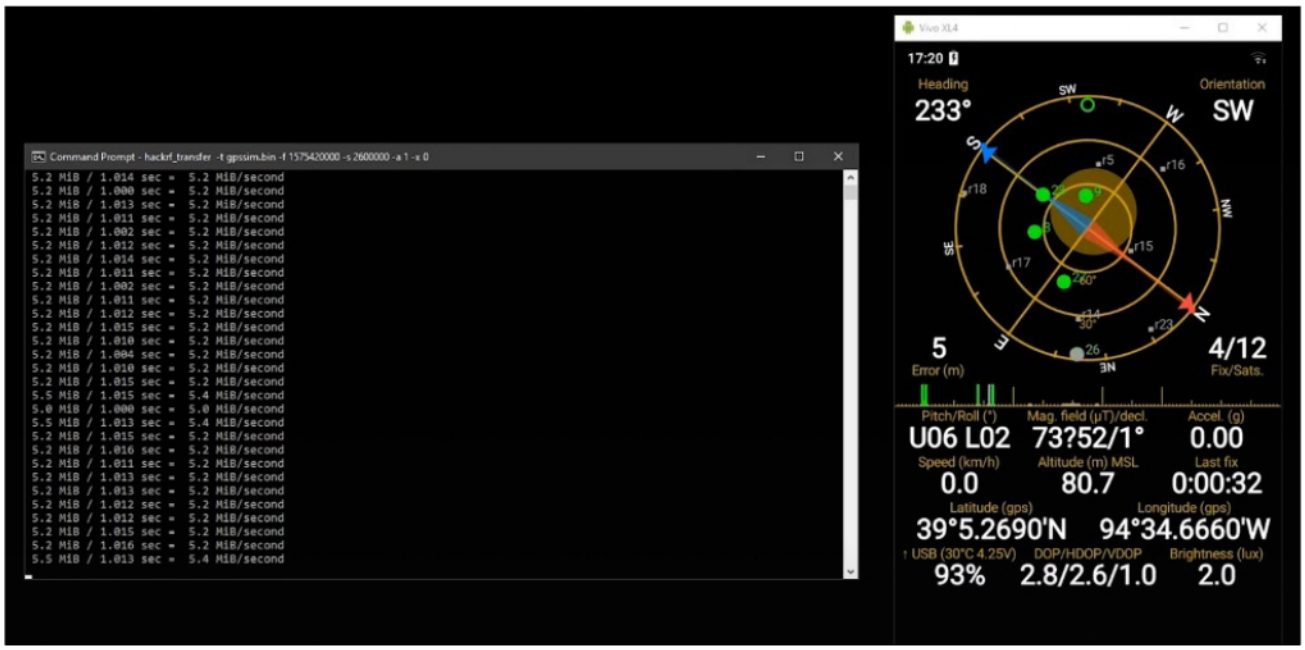


Figura 1: Esempio GPS SPoofing

CASO STUDIO 2: ANALISI RFID CON L'HACKRF ONE

Un ulteriore scenario di studio cruciale per l'HackRF One è l'approfondita analisi dei tag **RFID**, dispositivi ampiamente utilizzati nei contesti della sicurezza, della logistica e del Retail. La capacità di questo strumento di interagire con i tag RFID, offre una prospettiva dettagliata sul funzionamento di tali dispositivi, aprendo nuove vie di esplorazione e analisi nei settori in cui i tag RFID sono fondamentali.

Immaginiamo un contesto in cui un ricercatore sfrutta l'HackRF One per analizzare un tag RFID impiegato in un sistema di controllo dell'accesso. Come abbiamo accennato in un precedente paragrafo, attraverso l'interazione con il tag, il ricercatore può identificare potenziali vulnerabilità che, se sfruttate, potrebbero consentire

protezione avanzate per prevenire usi impropri e abusi di tali tecnologie.

La capacità dell'HackRF One di analizzare e comunicare con i tag RFID sottolinea l'importanza di esplorare la sicurezza di tali dispositivi in modo completo e responsabile. Gli scenari descritti mettono in risalto la duplice natura di questa tecnologia: uno strumento di indagine e miglioramento della sicurezza, ma anche un potenziale veicolo per minacce e attività malevole se utilizzato in modo scorretto. La consapevolezza di questi aspetti è essenziale per promuovere un utilizzo etico e sicuro delle tecnologie basate su RFID.

CASO STUDIO 3: SNIFFING BLUETOOTH E WI-FI CON L'HACKRF ONE

Oltre alle sue notevoli capacità nell'analisi di segna-

CORSO DI ELETTRONICA PER RAGAZZI – PUNTATA 19

di Fulvio De Santis

Nella precedente puntata abbiamo descritto e analizzato il funzionamento dell'amplificatore non invertente e dell'amplificatore invertente. Di questi amplificatori abbiamo spiegato come rappresentare l'amplificatore operazionale mediante i circuiti equivalenti e come calcolare le correnti, la tensione di uscita, l'amplificazione di tensione, la resistenza d'ingresso e la resistenza di uscita. In questa puntata, continueremo lo studio dell'amplificatore operazionale con altri due esempi di utilizzo di questo importante dispositivo nei circuiti elettronici: l'amplificatore sommatore e l'amplificatore differenziale.

L'AMPLIFICATORE SOMMATORE

Inizieremo lo studio di applicazioni dell'amplificatore operazionale con l'amplificatore sommatore. Nella **Figura 1** viene mostrato lo schema elettrico di un esempio di amplificatore sommatore.
L'amplificatore sommatore è un amplificatore invertente in grado anche di sommare più segnali applicati in ingresso. Come esempio, nello schema di **Figura 1** abbiamo collegato all'ingresso dell'amplificatore invertente tre generatori di tensione indipendenti V1, V2 e V3 collegati ai rispettivi terminali dei resistori R1, R2, e R3, mentre gli altri terminali sono collegati insieme al terminale negativo dell'operazionale.
Lo schema è già pronto per la nostra analisi, in quanto, come vedete sono indicate la tensione di uscita Vo, le correnti con il loro verso, I1, I2, e I3, confluenti in entrata nel nodo "a" e la corrente I somma delle tre correnti, uscente dal nodo "a" e diretta verso il resistore Rf di controreazione (in inglese "feedback"). Notate che il nodo "a" è in pratica coincidente con i due nodi inclusi nell'ellisse. Ora, applicheremo l'analisi nodale per calcolare le correnti considerando, come al solito, ideale l'amplificatore operazionale, a meno che venga dichiarato reale all'occorrenza.
Applichiamo la LKC al nodo "a" considerando positive le correnti entranti e negative le correnti uscenti dal nodo:

I1+I2+I3-I=0

Considerando che i due terminali d'ingresso dell'operazionale "+" e "-" sono in cortocircuito virtuale, e dato che il terminale positivo è a massa, il terminale negativo è a massa virtuale, applicando la legge di Ohm ricaviamo le correnti e le sostituiamo nell'equazione precedente delle correnti:

I1=V1/R1, I2=V2/R2, I3=V3/R3, I=-Vo/Rf
Quindi, tornando alla prima equazione si ha:

V1/R1+V2/R2+V3/R3+Vo/Rf=0

A questo punto, da quest'ultima equazione possiamo ricavare la tensione di uscita Vo:

Vo=-Rf*(V1/R1+V2/R2+V3/R3)

Si noti il segno negativo della tensione di uscita che sta ad indicare che l'amplificatore sommatore, essendo costituito dall'amplificatore operazionale invertente, inverte in uscita il verso del segnale d'ingresso.

Possiamo scrivere questa relazione anche così:

Vo=-(V1*Rf/R1+V2*Rf/R2+V3*Rf/R3)

In questo modo, vediamo più chiaramente che il valore di Vo per ogni segnale d'ingresso del generatore applicato dipende dal rapporto fra la resistenza di controreazione Rf e la resistenza collegata al rispettivo generatore. In pratica, definita Rx la resistenza collegata al generatore Vx, il rapporto Rf/Rx può essere considerato il coefficiente di amplificazione di tensione dell'amplificatore sommatore, ovvero, quando Rf>Rx l'amplificatore amplifica il segnale d'ingresso, mentre per Rf<Rx l'amplificatore attenua il segnale d'ingresso. Si ottiene il guadagno unitario e l'inversione del segnale d'ingresso per Rf=Rx, ossia Vo=-Vx.

L'AMPLIFICATORE DIFFERENZIALE

Un altro utilizzo dell'amplificatore operazionale è quello di realizzare un amplificatore differenziale. Il funzionamento di questo tipo di amplificatore è dedotto proprio dalla parola "differenziale": l'amplificatore differenziale effettua la differenza fra i segnali applicati ai due terminali d'ingresso "+" e "-"dell'operazionale.
Nella **Figura 2** viene mostrato lo schema teorico di un amplificatore differenziale.

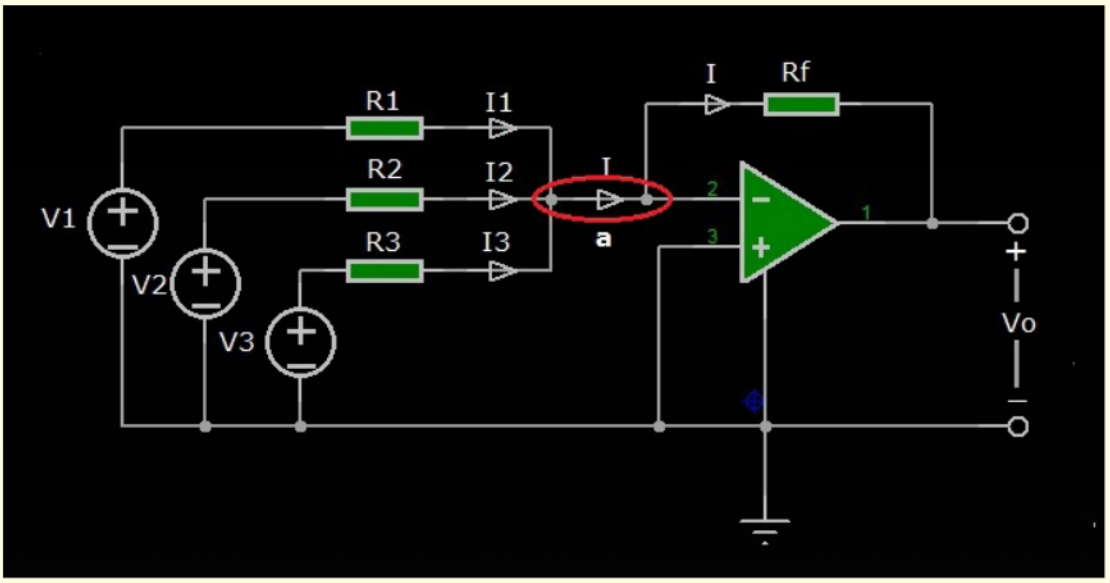


Figura 1: Schema elettrico di un amplificatore sommatore

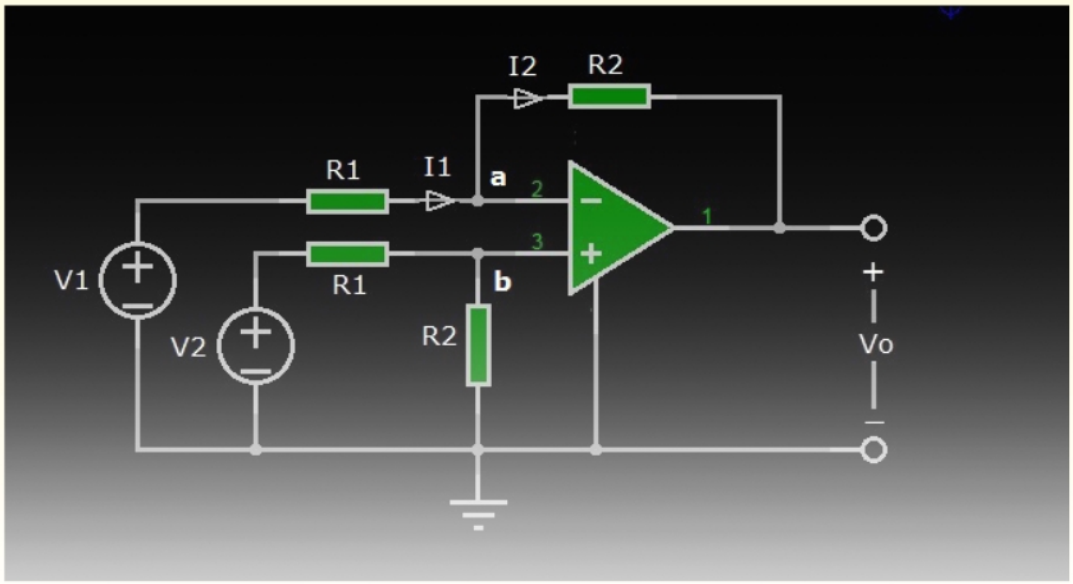


Figura 2: Amplificatore differenziale

+ 145.000
REGISTERED USERS

7.414 AVERAGE DAILY PAGEVIEWS (FEB2020)

830.610 2020 ANNUAL VISITORS

THE BIGGEST **EMBEDDED COMMUNITY** IN ITALY

SOCIAL CONNECTIONS

+ 83.000

+ 23.000

CATEGORIES

PROFESSIONALS
53 %

ACADEMICS/STUDENTS
25 %

MAKERS/HOBBYISTS
22 %

Elettronica Open Source