Hacking delle colonnine: il pericolo è reale?

TRA LE STAZIONI DI RICARICA E IL VEICOLO ELETTRICO NON PASSA SOLO CORRENTE. L'EV-CHARGER È ANCHE UN DISPOSITIVO TECNOLOGICAMENTE ATTREZZATO PER GESTIRE PAGAMENTI CON RFID CARD, VIA POS OPPURE ATTRAVERSO IL PLUG&CHARGE: STRUMENTI CHE PREVEDONO SCAMBI DI DATI SENSIBILI E CHE LO RENDONO UN POTENZIALE BERSAGLIO. ECCO QUALI SONO I PERICOLI E GLI STRUMENTI MESSI IN CAMPO DALL'INDUSTRIA PER PROTEGGERE UTENTI E GESTORI

DI FEDERICA MUSTO

Secondo l'enciclopedia Treccani, con il termine hacker si intende un "esperto di programmazione e di reti telematiche che, perseguendo l'obiettivo di democratizzare l'accesso all'informazione e animato da princìpi etici, opera per aumentare i gradi di libertà di un sistema chiuso e insegnare ad altri come mantenerlo libero ed efficiente". Il termine, nato a cavallo degli anni 1960 al MIT di Boston, non ha dunque di per sé la connotazione negativa che ha sviluppato nell'opinione comune. I cosiddetti "pirati informatici", il cui scopo è danneggiare un sistema informatico, sono invece chiamati "crackers", o "black hat Hacker" nel momento in cui l'obiettivo sia la violazione illegale dei sistemi informatici, con o senza vantaggi personali. Questa distinzione tra pirati informatici e "white hacker", hacker bianchi, è fondamentale per comprendere al meglio il fenomeno di hacking dell'infrastruttura di ricarica e più in generale nel settore dei veicoli elettrici, dal momento che, a oggi, la maggior parte degli attacchi informatici di cui si ha prova sono stati effettuati, in effetti, con l'obiettivo di dimostrare delle falle nella sicurezza informatica dell'infrastruttura e dei veicoli "a spina" – oggi fortemente interconnessi –, con l'obiettivo di spingere verso maggiori investimenti e ricerca nel settore della cyber security. Spoiler: molte delle soluzioni ai problemi che affronteremo in questo articolo - lo vedremo - sono già disponibili sul mercato. Il discrimine sta nella loro applicazione, o meno.

Alcuni casi di hacking recenti

Nelle prime settimane dopo lo scoppio della guerra in Ucraina si è verificato un attacco hacker di protesta ad alcune stazioni di ricarica dislocate sull'autostrada russa che collega Mosca a San Pietroburgo, ripreso da un gruppo di elettromobilisti fermati a caricare le loro auto. Dapprima sullo schermo della colonnina colpita è stato visualizzato un messaggio di errore: "Call service, no plugs available"; subito dopo sono apparsi una serie di insulti verso Putin e messaggi pro Ucraina.
All'incirca nello stesso periodo nel Regno Unito, in particolare sull'Isola di Wight in Inghilterra - come riporta un video trasmesso dalla BBC - tre punti di ricarica sono stati hackerati per mostrare sui propri display video osceni, anche in questo caso rendendo inutilizzabili le colonnine per la ricarica per tutto il corso dell'attacco.
Al di là del tipo di messaggio mostrato sui display,

ciò che è da ritenersi rilevante per questi attacchi è la capacità da parte degli autori di prendere il controllo della stazione di ricarica - di una o più colonnina - e di renderle inutilizzabili. Se "in piccolo" tale situazione può arrecare danno al malcapitato che necessita di caricare durante l'attacco, guardando il problema da un punto di vista più ampio si può immaginare cosa potrebbe accadere nel momento in cui le colonnine venissero bloccate in un momento di pericolo, creando di fatto difficoltà a soccorsi o forze dell'ordine, o qualora l'attacco non riguardasse solo poche colonnine ma tutti i charging point presenti in un'intera area, bloccando l'erogazione di energia o magari avviando in contemporanea il rifornimento di tutti i veicoli connessi, di fatto sbilanciando in modo colposo la rete elettrica locale. C'è da specificare che le reti elettriche - almeno in Italia - sono sempre dimensionate in maniera da sopportare i picchi di richiesta dell'infrastruttura locale, specialmente dove si parla di colonnine HPC e dunque allacciate direttamente in media tensione e aventi potenza dedicata.

Tipologie di attacchi

Non tutti gli attacchi informatici sono uguali. Ne esistono di diverso tipo, con strumenti, scopi e punti di accesso differente. Uno dei più noti è il cosiddetto man-in-the-middle, in cui l'autore dell'attacco riesce a interporsi nel mezzo di una comunicazione tra due parti, intercettando per apprendere informazioni e di conseguenza anche potenzialmente manipolando il traffico diretto verso la parte ricevente. Nel caso di attacchi a colonnine per la ricarica, questo tipo di hackeraggio potrebbe ad esempio manipolare le informazioni che l'auto trasferisce alla colonnina su account e riferimenti per il pagamento, dando così accesso a frodi di pagamento o alla duplicazione delle informazioni bancarie dell'utente. Un'altra possibilità è quella in cui la parte malintenzionata va ad agire sui dati relativi alla potenza di ricarica, per cui l'informazione sulla potenza richiesta dal BMS dell'auto viene manipolata verso la colonnina e dunque la colonnina fornisce più potenza di quella accettabile dal veicolo, andando a sovraccaricare la batteria, danneggiandola, o bloccare il flusso, di fatto impedendo il rifornimento. Un altro attacco hacker possibile in questo ambito è quello definito spoofing, e si verifica quando un hacker si "maschera" da fonte attendibile accedendo in tal modo a dati o informazioni riservate. In ambito EV, un attacco spoofing si verifica, ad esempio, quando la comunicazione tra colonnina e veicolo non è sufficientemente sicura e l'hacker riesce a fingersi il server - lato colonnina - con il quale il veicolo dialoga nel momento in cui viene connessa la presa e comincia il processo di ricarica. In questo modo l'hacker può manomettere l'ID del veicolo, rubandolo o sostituendolo al reale ID di un altro veicolo: sarà possibile così usufruire, ad esempio, delle informazioni di fatturazione di qualcun altro per caricare il veicolo manomesso.

LE TESSERE RFID DI ULTIMA GENERAZIONE SONO STRUMENTI DI ATTIVAZIONI PIUTTOSTO SICURI. MENTRE I SISTEMI POS SOFFRONO LE STESSE CRITICITÀ DI QUELLI PRESENTI NEI COMUNI BANCOMAT E POSSONO ESSERE A RISCHIO SOPRATTUTTO NEI LUOGHI MENO SORVEGLIATI

Lo standard ISO 15118

Dunque cosa si può fare per evitare il verificarsi di attacchi informatici alle colonnine di ricarica? Come dicevamo all'inizio, molte delle soluzioni sono già disponibili e vanno solo implementate correttamente. La più promettente è quella portata dal cosiddetto Standard ISO 15118, ovvero uno standard internazionale che delinea il protocollo di comunicazione digitale che un veicolo elettrico (EV) e una stazione di ricarica dovrebbero utilizzare per ricaricare la batteria ad alta tensione del veicolo elettrico. Lo standard copre tutti i casi d'uso relativi al recharging in tutto il mondo, per cui include applicazioni di ricarica cablata (AC e DC), wireless e anche i pantografi utilizzati per caricare veicoli più grandi come gli autobus. Inoltre lo standard copre anche la comunicazione tra veicolo a rete (il cosiddetto V2G, vehicle to grid) con cui il veicolo sarà in grado di comunicare con la rete elettrica per quanto concerne il trasferimento di energia elettrica (in entrambe le direzioni).
Lo standard si compone di una serie di documenti che definiscono tutte le operazioni e le autenticazioni che il collegamento deve soddisfare perchè la ricarica vada a buon fine. In parole semplici, qualora tutte le "sezioni" dello standard siano rispettate e attivate, il livello di crittografia e sicurezza tramite certificati digitali è sufficiente perchè i tentativi di hackeraggio – di cui sopra sono stati portati alcuni esempi – siano sventati. Ad esempio, l'ISO 15118 prevede che sia creato un canale sicuro di comunicazione tra colonnina e veicolo tramite TLS, ovvero un "protocollo di creazione di canali sicuri". Semplificando, il TLS utilizza una combinazione di crittografia e autenticazione attraverso certificati digitali per garantire che un canale sia protetto contro possibili attacchi. Per intenderci è lo stesso protocollo che viene utilizzato in Https per garantire che il traffico che scorre tra un client e un server su Internet sia protetto. Ma esistono dei casi in cui l'autenticazione tramite TLS non è ritenuta obbligatoria dal sistema, ovvero quando viene utilizzata un qualche tipo di autenticazione esterna e dunque la colonnina viene considerata come disponibile per un gruppo chiuso di utenti. È il caso delle tessere RFID.

Le Rfid card sono sicure?

Quando un utente utilizza una Rfid card per autenticarsi e avviare una ricarica presso una colonnina, il sistema tralascia la comunicazione di dati relativi all'autenticazione del veicolo che generalmente passa tramite il connettore, per dare priorità all'autenticazione e ai dati di fatturazione della tessera. Il sistema riconosce tale autenticazione come avvenuta in un ambiente sicuro e dunque non usufruisce del canale crittografato TLS per lo scambio dei dati, aprendo a potenziali manomissioni da parte di black hat hacker. C'è poi da considerare che, almeno ipoteticamente, una tessera Rfid è un oggetto più semplice da clonare rispetto che violare il sistema di una colonnina. Fortunatamente le ultime Rfid card hanno utilizzato sempre più diffusamente la crittografia DES per il tag NFC - Near-Field-Communication - che è associato al token ID dell'utente e dunque al suo sistema bancario.

Violare il gestionale: sicurezza dell'OCPP

Un aspetto ancora debole dei punti di ricarica che non attuano nella sua totalità lo standard ISO 15118 di ultima generazione è il protocollo Open Charge Point Protocol (OCPP). Si tratta del protocollo standard che regola la comunicazione tra le singole colonnine di ricarica per veicoli elettrici e il sistema di gestione centrale – il backend – ovvero il software che permette agli operatori di monitorare, autorizzare o interrompere la ricarica, e che dunque riceve i dati di autenticazione di tutti gli utilizzatori della rete di colonnine. Quando questo protocollo resta aperto, potrebbe esporre il sistema ad attacchi, ad esempio, di tipo man-in-the-middle, in grado di entrare e corrompere – con informazioni manipolate – non solo la singola colonnina, ma l'intera rete dell'infrastruttura.

Pagamento via POS: comodità o falla nella sicurezza?

L'ultimo punto riguarda una previsione. Ad oggi la ricarica in Italia può essere avviata tramite Rfid card, app - e qui è d'obbligo sottolineare l'importanza di preservare in sicurezza i dati di accesso, che restano il modo più semplice per accedere ad un account da parte di un malintenzionato - e, laddove disponibile, il Plug&Charge supportato dallo standard ISO 15118. Ma l'elettromobilista attento avrà notato che molte delle stazioni di ricarica recentemente installate sono state predisposte per supportare il POS, l'hardware per il pagamento con carta di credito e bancomat. Sono tristemente note le varie tipologie di hackeraggio e clonazione dei nostri sistemi di pagamento con "fake-POS" sovrapposti all'hardware di pagamento originale. Sebbene dunque l'introduzione del pagamento della ricarica con carta possa essere considerata una comodità, va valutato il fattore di rischio del fatto che spesso le colonnine sono collocate in luoghi poco sorvegliati in cui è più semplice avere accesso e manomettere fisicamente la colonnina.