Cyber Security e Internet of Things

Date : 10 gennaio 2017

SICUREZZA IOT: UNA QUESTIONE DI VITA O DI MORTE?

Probabilmente negli ultimi mesi sarete stati inondati dall'enorme numero di incidenti di sicurezza pubblicati sui vari mezzi di informazione, digitali e cartacei.

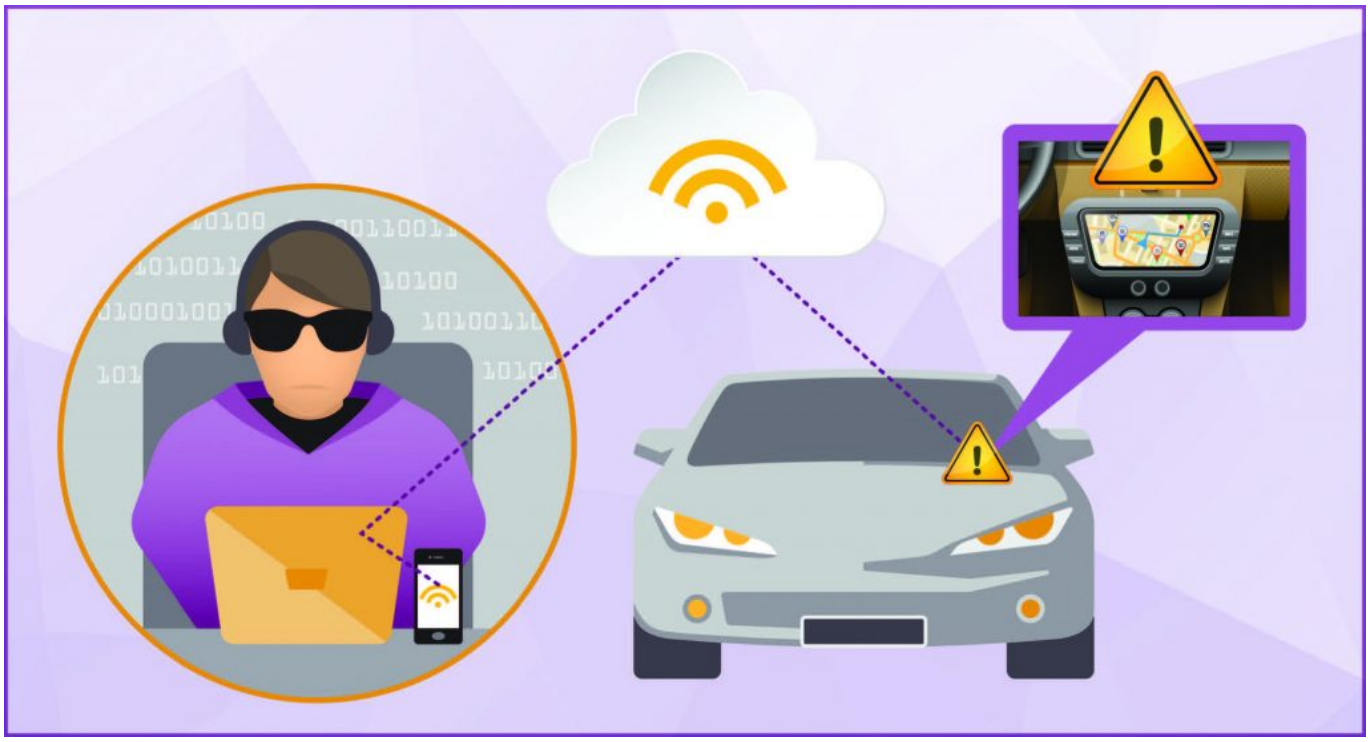
Abbiamo letto di attacchi mirati, APT (Advanced Persistent Threats), furti di indirizzi IP, di identità e informazioni protette da proprietà intellettuale che hanno portato a danni economici, licenziamenti dei responsabili (in alcuni casi anche del top management) e pubblicità negativa al brand dell'azienda.

Purtroppo conosciamo bene le conseguenze di un cyber attacco portato a buon fine. Sappiamo che le violazioni di sicurezza sono ormai frequenti, ma stiamo andando incontro ad una potenziale minaccia ancora più importante e di cui dobbiamo assolutamente tenere conto nell'immediato futuro: le vulnerabilità dell'Internet of Things (IoT), ovvero di tutti i dispositivi fisici e virtuali che oggi possono connettersi utilizzando qualunque tipologia di rete fissa e mobile, in generale via Internet.

Nel prossimo futuro violare la sicurezza di questi dispositivi potrà comportare non solo problemi di natura legale ed economica al produttore e/o gestore del dispositivo o servizio ma potrà avere impatti anche sulla vita delle persone.

Analizzeremo di seguito alcuni tra i più recenti e noti problemi di sicurezza IoT.

DALLE AUTO AI DISPOSITIVI MEDICI



Due ricercatori esperti di sicurezza, Charlie Miller e Chris Valasek, hanno dimostrato al Black Hat 2015 che è possibile compromettere la sicurezza di una Jeep Cherokee edizione 2014. In breve, i ricercatori hanno inizialmente verificato che il sistema proprietario di intrattenimento e navigazione Uconnect era pre-configurato per collegarsi automaticamente alla rete mobile dell'operatore di telecomunicazioni americano Sprint.

Attraverso una scansione delle vulnerabilità hanno rilevato che la porta TCP 6667 era inspiegabilmente aperta e consentiva un accesso senza autenticazione all'API (Application Programming Interface) del sistema di intrattenimento. Questo permetteva di modificare il sistema radio ed altre funzionalità.

Il sistema Uconnect era a sua volta collegato alla rete di comunicazione interna CAN (Controller Area Network) alla quale sono collegati i sottosistemi critici dell'auto, dal sistema frenante al volante.

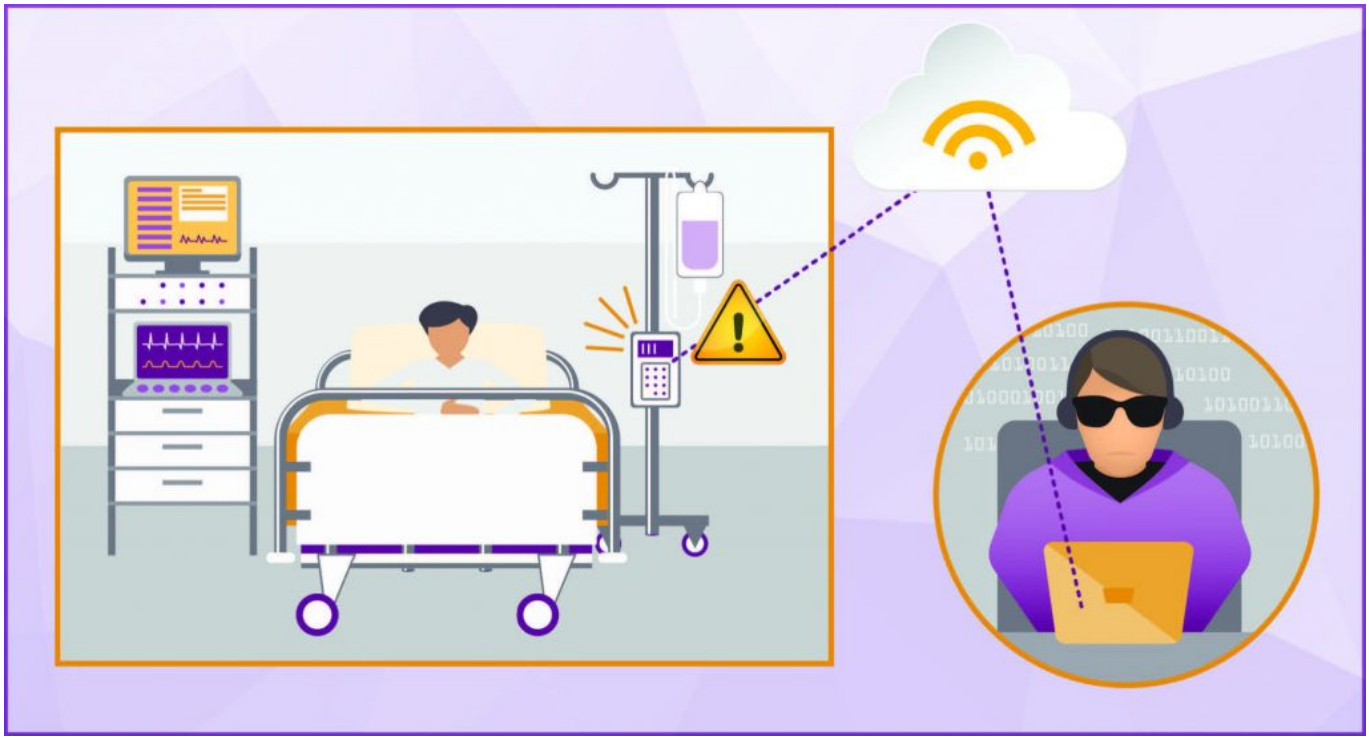
A questo punto i due ricercatori sono riusciti ad installare un firmware modificato nel microprocessore V850 della centralina Uconnect (quindi anche gli aggiornamenti software della centralina non venivano sufficientemente autenticati) che gli ha permesso di inviare dei comandi attraverso la rete CAN verso gli altri sottosistemi collegati (volante, freni, …).

La pubblicazione di questa scoperta ha costretto Fiat Chrysler Automobiles (FCA) a richiamare 1.4 milioni di autoveicoli per applicare le dovute patch.

Questa scoperta ha richiesto circa un anno di lavoro di analisi e sviluppo software da parte dei ricercatori ed ha portato all'attenzione dell'opinione pubblica mondiale un problema di sicurezza molto serio.

Può un hacker controllare da remoto, via internet, un’auto o, se fosse un cyber criminale, provocare incidenti, facilitare i rapimenti bloccando le porte dell’auto fino all’arrivo dei sequestratori, agevolare i furti?

Ma i problemi di sicurezza IoT che possono minacciare la libertà o addirittura la vita delle persone non si riscontrano soltanto nell’ambito dell’industria automobilistica.



Pochi mesi fà negli Stati Uniti la Food and Drug Administration (FDA) ha inviato un’informativa a tutti gli ospedali in cui metteva in evidenza dei problemi di sicurezza di una nota marca di dispositivi per la regolazione della somministrazione dei medicinali che avevano la caratteristica di poter essere controllati da remoto, ovvero via internet.

Nella segnalazione inviata si leggeva: “…un utente non autorizzato potrebbe acquisire il controllo del dispositivo e cambiare il dosaggio di somministrazione del medicinale, con potenziali gravi conseguenze per i pazienti sottoposti a particolari terapie…”

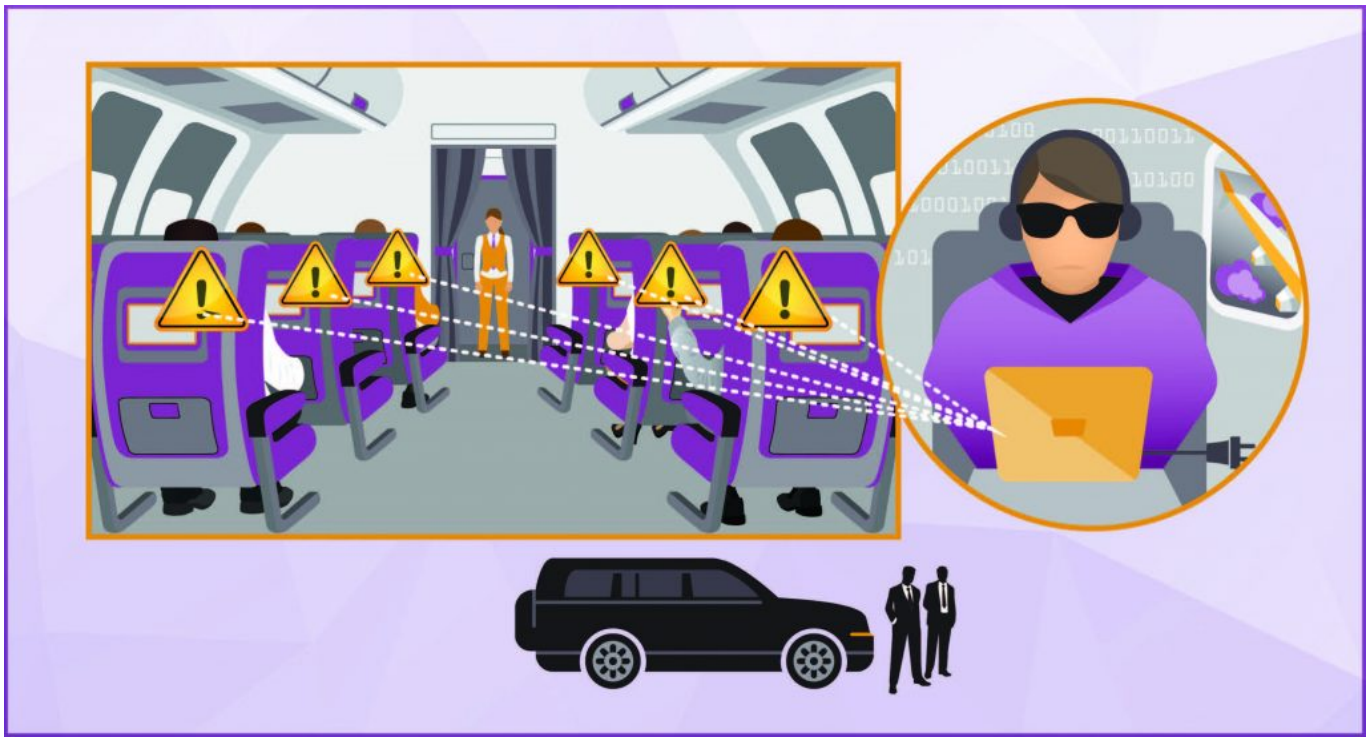
Non serve molta immaginazione per capire cosa poteva essere in grado di fare un hacker se avesse scoperto e sfruttato le vulnerabilità nei sistemi Hospira Symbiq Infusion (versione 3.13 e precedenti), Plum A+ Infusion (versione 13.4 e precedenti), e Plum A+ 3 Infusion (versione 13.6 e precedenti).

Un sicario avrebbe potuto facilmente controllare ed eventualmente uccidere la sua vittima e gli ospedali che utilizzavano questi sistemi potevano essere soggetti a forme di ricatto.

DAI FUCILI AGLI AEROPLANI

Ma i pericoli dell’IoT non finiscono qui. L’estate dello scorso anno veniva riportata sulla stampa la scoperta di due ricercatori esperti di sicurezza, Runa Sandvik e Michael Auger, i quali avevano scoperto un modo per introdursi via Wi-Fi nel sistema di puntamento per fucili Tracking Point, basato su Linux, attraverso la sua applicazione per smartphone (quindi una app) ShotView.

In tal modo un hacker poteva impedire al fucile di sparare o, peggio, indirizzare il sistema di puntamento su un altro bersaglio. Immaginiamo cosa poteva accadere se queste armi fossero state date in dotazione alle guardie del corpo di personaggi pubblici importanti (Presidenti, Ministri, VIP, ...).



Cosa può accadere, invece, quando siamo comodamente seduti in volo per un viaggio di affari o vacanza, magari ascoltando buona musica o vedendo un film con il sistema di intrattenimento di bordo?

Partiamo dalla considerazione che anche un aeroplano è dotato di una complessa rete di comunicazione interna che interconnette tutti i componenti elettronici di bordo e, oggi, offre anche un servizio internet ai passeggeri.

Un esperto di sicurezza, Chris Roberts, è stato fermato dall'FBI e accusato di aver manomesso il sistema di intrattenimento di un aereo durante la fase di volo. Sembra che il ricercatore sia riuscito ad avere accesso al computer di bordo (il Trust Management Computer) e, modificando opportunamente alcuni programmi, a cambiare la posizione dell'aereo in volo! Roberts ha dichiarato di aver raggiunto questi risultati lavorando in un ambiente di simulazione e non su di un vero aereo in quota. Boeing ha dichiarato successivamente pubblicamente che i propri sistemi di intrattenimento (IFE, In- Flight Entertainment) sono isolati dai sistemi di volo e navigazione.

Tuttavia il rischio di compromissione appare da quest'ultimo caso troppo reale per essere ignorato.

Dalla tragedia delle Torri Gemelle in New York dell'11 Settembre 2001 fino al disastro del volo Malaysian Airlines MH17 in Ucraina nel 2014, è ormai noto che i voli aerei sono un obiettivo importante dei terroristi, siano essi singoli individui, gruppi o stati.

I casi che abbiamo esaminato sono soltanto alcuni esempi dei potenziali problemi di sicurezza presenti in tanti dispositivi "intelligenti" (smart) sul mercato, connessi costantemente ad altri

dispositivi e sistemi online/cloud per offrire costantemente al consumatore diversi servizi (meteo, traffico, …).

Non sappiamo se le vulnerabilità esaminate sono state sfruttate da cyber criminali per compiere azioni criminose. Tuttavia siamo consapevoli che prima o poi le grandi risorse (finanziarie, computazionali,…) a disposizione dei cyber criminali saranno utilizzate per trovare delle vulnerabilità 0-day nei dispositivi del mercato IoT. La potenziale facilità di compromissione di alcuni sistemi e dispositivi visti precedentemente non potrà far altro che aumentare sia l'aspettativa di guadagno dei cyber criminali sia la gravità dei potenziali danni per gli utilizzatori finali

Le aziende che stanno investendo nel mercato IoT non potranno pertanto fare a meno di dotarsi nel prossimo futuro di esperti di sicurezza informatica e sviluppare codice sicuro per i propri dispositivi.

Riferimenti

- Definizione di IoT http://www.itu.int/rec/T-REC-Y.2060-201206-I
- https://en.wikipedia.org/wiki/Charlie_Miller_(security_researcher)
- http://chris.illmatics.com/about.html
- https://www.kb.cert.org/vuls/id/819439
- https://www.driveuconnect.eu/
- http://blog.fcanorthamerica.com/2015/07/22/unhacking-the-hacked-jeep/
- https://it.wikipedia.org/wiki/Patch_(informatica)
- https://it.wikipedia.org/wiki/Hacker
- http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm
- https://www.blackhat.com/docs/us-15/materials/us-15-Sandvik-When-IoT-Attacks-Hacking-A-Linux-Powered-Rifle.pdf
- http://www.cnet.com/news/fbi-pulls-computer-security-expert-off-flight-after-he-tweets-about-hacking-its-systems/

A cura di: **CESARE GARLATI,** *Chief Security Strategist in prpl Foundation e Co-chair del Mobile Working Group di Cloud Security Alliance*