Io non ho nulla da nascondere, che mi importa della sicurezza IT?

Disclaimer

SARO’ POLEMICO.

Sicurezza IT

- Serve^Hirebbe sui server pa, bancari, assicurativi, ospedalieri, degli studi legali …
- Serve^Hirebbe sui ‘sistemi grossi e costosi’
- Serve^Hirebbe sui ‘sistemi a servizio della collettività’

Ma sui piccoli sistemini di uso quotidiano?

- Automobile?
- Termosifone ?
- Antifurto ?
- Termometro (interno/esterno)?
- Apricancello ?

Non scherziamo !

- Ma non ci dirai che queste cose hanno a che fare con l’informatica !!!!!
- Auto: tpms, aperture porte e accensione...
- Termosifone: contabilizzazione, accensione e spegnimento
- Antifurto: lettura dei sensori

Continuiamo a scherzare

- Il termometro e l’apricancello sono per fortuna vulnerabili, il primo vista la possibile utilità sociale di un monitoraggio delle temperature interne, e l’apricancello per la facilità di trovare ricambi non originali …
- Ci sarebbero anche altri oggettini ma forse e’ meglio lasciarli stare.

SDR

- Software defined radio
- Radio che hanno le loro funzionalità non solo definite principalmente in digitale ma spesso le modalità di funzionamento son definite da software.
- Una sorta di fusione di radio e un PC.
- Ottima cosa per implementare trasmissioni di dati da/per IoT

Bande radio libere

- Le bande radio sono regolamentate a livello Europeo, Nazionale e a volte locale.
- Le bande di ns interesse sono ISM (wifi, bluetooth) CB, PMR (walkie talkie), LPD (low power device) e altre ancora.
- Altre bande, oltre I 2.5 GHz hanno rilevanza per radar e satelliti.

Esempi d’uso

- Wifi e bluetooth non han bisogno di presentazioni come la CB e la PMR (Private Mobile Radio).
- Arriviamo alla LPD, Low Power Device. Ovvero frequenze per uso libero, in europa sulla frequenza 433 MHz. ATTENZIONE ALLE BANDE MILITARI. SONO PROIBITE.
- Sulla 433 si trova letteralmente di tutto. Molti prodotti dell’est usano questa banda e altre per trasmettere di tutto, a volte in fonia e in chiaro.

Tecnicalità

- Sulla freq, 433 MHz abbiamo detto. Ovviamente non tutti trasmettono digitalmente sullo stesso ‘numero’ di Hertz. Ci si sposta di qualche decina di Khz nello spazio tra tra 433 e 434 MHz. Ci si sposta a passi di 25Khz (o altri) e la potenza di trasmissione è limitata (sarebbe) sotto I 10mW milliWatt... Le modalità di trasmissione sarebbero FM.

Strumenti

- Una radio sdr (tv dongle)
- Linux, e rtl_433
- OPPURE:
- http://websdr.org/

Ovvero un

sito dove usare una sdr da un altro paese … Alcuni danno accesso anche alla 433MHz

Possibili abusi sulla privacy?

- Google è nostro amico e ci mostra molte ‘robe’ che trasmettono su 433 e simili. Contabilizzatori di calore, TPMS (pneumatici), Sistemi di allarme, apricancello, stazioni meteo e altro.
- Tutta questa roba, visto l’affollamento, della frequenza, trasmette per un istante e, HA UN ID.

Possibili abusi sulla privacy...

- Se ha un ID potrà esser tracciato. Rivisto. E le sue letture potranno esser usate nel dominio del tempo e dello spazio.
- Prendiamo a esempio un Pneumatico che, viene visto in X, poi in Y e in Z...
- Prendiamo un termostato o un contabilizzatore di calore che mostra variazioni di lettura.

Ma che ci ……. del calore ?

- Dopo I cookie ora il calore ?
- Beh se il ‘contatore’ scorre o sei a casa e hai I soldi, o non sei a casa, o non hai I soldi... Potrebbe essere una informazione interessante per un impiccione, un malvivente o altro ancora.

Possibili vantaggi per la collettività

- In tempi di green deal e problemi energetici avere una possibilità di conoscere I consumi energetici e le temperature ‘localissime’ è di evidente beneficio.
- Idem la lettura in tempo reale magari al semaforo di quanti pneumatici passano …

howto

- Esistono molti howto su come cominciare. A mio avviso la prima cosa è il dongle tv o websdr e poi con rtl_433 ove applicabile mostrare il tutto in un formato testuale.
- Il sito rtl-sdr.com ha molti tutorial.
- A me piace usare mqtt. Un broker di messaggi. Quindi potreste avere più ricevitori afferenti nel vostro dataset.

Ma che dati girano?

- Sicuramente un identificativo.
- Spesso una descrizione dell’apparato in forma testuale.
- I dati importanti: pressione, calore, temperatura, flussi etc.
- Normalmente, secondo la documentazione di questi apparati, e, del codice, E’ TUTTO IN CHIARO.

Ma perchè sarebbe pericoloso? (avere I dati in chiaro)

- Mettiamo che qualcuno vuole creare disturbo e comincia a trasmettere dati ‘farlocchi’ di pressione o temperatura a una centralina.
- Oppure a un possibile allarme
- OPPURE A UN APPARATO ELETTROMEDICALE.

Conclusioni

Mi sembra che:

- le normative abbiano imposto la presenza sul mercato di dispositivi non adeguatamente pensati
- Le aziende non chiedessero altro che poter inondare il mercato di nuovi prodotti.
- I cittadini non siano stati per nulla informati.

Rischi

- Sicuramente per la privacy, I rischi sono il possibile tracciamento (dipende dalla potenza di trasmissione del pneumatico/device) che collocherei un livello medio basso.
- Certo se si parla di sistemi di allarme o biomedicale le cose cambiano*

  *sul secondo ho trovato valutazioni di antenne e sistemi, non ho evidenze documentali di uso.

Bibliografia

- https://github.com/merbanan/rtl_433
- https://atc.mise.gov.it/index.php/tecnologie-delle-comunicazioni/gestione-spettro-radio/piano-nazionale-di-ripartizione-delle-frequenze (leggete le note con la massima attenzione)
- https://en.wikipedia.org/wiki/LPD433
- https://en.wikipedia.org/wiki/ISM_radio_band

Domande ?

- Ma io posso ascoltare tutte le bande ISM (Industrial, Scientific, Medical) ?
- Ripeto: leggete il piano delle frequenze del vs paese e attenzione a dispositivi/frequenze ffoo/ffaa. Sicuramente potete ascoltare I vostri apparati che sono a norma. Controllate PRIMA la normativa vigente.