N. 252 - Marzo 2021

Prezzo: 5.77 €

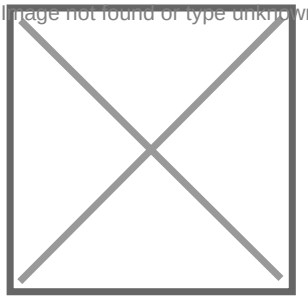
Tasse: 0.00 €

Prezzo totale (con tasse): 5.77 €

La sicurezza prima di tutto

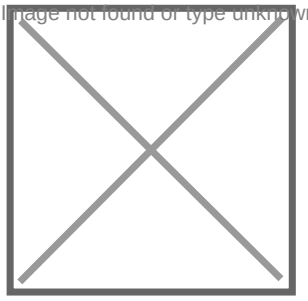
Basta un malware per dare modo agli hacker di infiltrarsi nei nostri dispositivi connessi
“Darcey Lee è una donna di 68 anni che vive sola con il suo gatto in un appartamento alla periferia di New York. Una sera di un’estate di qualche anno fa si vede piombare in casa dei poliziotti della

CISA (Cybersecurity and Infrastructure Security Agency). Incredula e spaventata urla e chiede spiegazioni. I poliziotti non le rispondo e continuano a perquisire la casa alla ricerca del computer. Ma Darcey non ha il computer. Eppure Tracerouter parla chiaro, l'attacco DDoS (Distributed Denial of Service) è partito da quell'abitazione. Ma come può una donna di 68 anni senza computer aver causato quell'attacco? Il router WiFi viene subito verificato. Tre i dispositivi connessi: un cellulare, uno smart speaker regalato dal figlio, e una telecamera WiFi che Darcey ha comprato in offerta per poter controllare il gatto dal suo cellulare. Che sia…? Impossibile… E invece sì. "Qualcuno" ha usato la telecamera di Darcey per instradare l'attacco... a sua insaputa..." Questa storia, ispirata da fatti realmente accaduti, mette in evidenza un aspetto molto trascurato: la sicurezza dei dispositivi connessi. Non è difficile trovare in rete storie di frigoriferi che inviano mail, telecamere accessibili da chiunque, router WiFi con backdoor ecc. Basta un malware infatti, per dare modo agli hacker di infiltrarsi nei nostri dispositivi connessi. Ma a volte è sufficiente l'ingenuità. Guardate ad esempio questo sito www.insecam.org: raccoglie le telecamere pubbliche, ma anche quelle le cui credenziali non sono state modificate. Oppure provate a navigare nel sito www.shodan.io: con qualche semplice ricerca si possono trovare router, webcam, NAS e sistemi aperti e gestibili da remoto senza la necessità di inserire credenziali o con i dati di autenticazione predefiniti. Il problema della sicurezza è spesso trascurato e con la grande disponibilità di moduli WiFi a basso costo è semplice per chiunque realizzare la propria applicazione, e spesso, spinti dall'entusiasmo di vedere il proprio progetto comunicare con il mondo, trascuriamo l'importanza di una comunicazione sicura. In questo numero analizziamo le principali modalità per rendere sicuri i vostri dispositivi IoT e iniziamo il corso di Azure Sphere, la soluzione di Microsoft nata per rendere invulnerabile la vostra applicazione. Articoli da leggere con attenzione. *Boris Landoni* **Sommario**



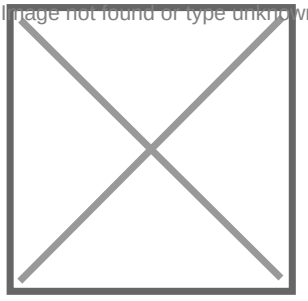
LoRa Edge LR1110 starter kit

Scopriamo LoRa Edge LR1110 di Semtech e il suo kit di sviluppo finalizzato alla produzione di dispositivi che coniugano le tecnologie LoRa, WiFi e GNSS per la geolocalizzazione.



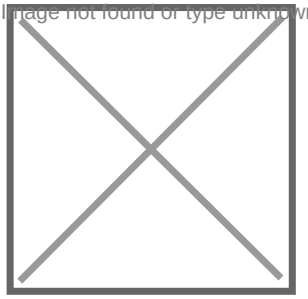
Smart sensor connesso a Blynk

Sviluppiamo un'applicazione IoT connettendo una scheda Fishino Guppy, equipaggiata con sensori di temperatura e umidità, alla piattaforma Blynk, che rende disponibili potenti widget per connettere il mondo dei sensori all'Internet of Things.



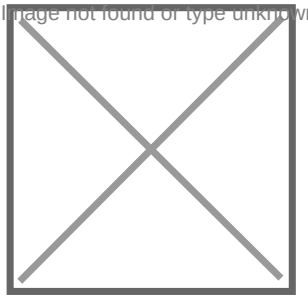
nvSRAM board

Aggiungiamo una RAM "non volatile" dove scrivere e mantenere, grazie a una pila tampone, dati permanenti.



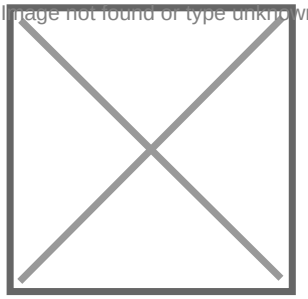
Monitoraggio ambientale con uChip

Dotato di scheda SD ed RTC, rileva e memorizza temperatura, umidità e pressione
touch.



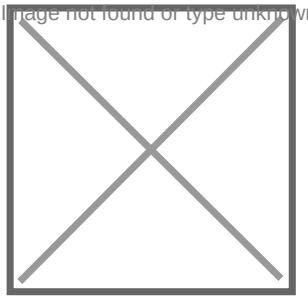
Interfaccia utente universale

Integra 8 display a 7 segmenti, 8 led e 8 pulsanti, che possono essere gestiti in lettu



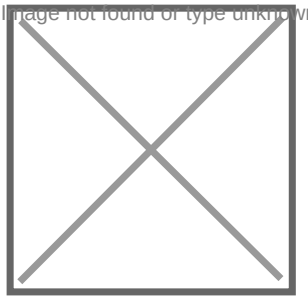
Riconoscimento targa da web

Usiamo il modulo ESP32-CAM per rilevare e riconoscere la targa di un
veicolo ed azionare un attuatore con cui aprire un garage, sollevare una
sbarra, attivare un allarme e altro ancora.



Sicurezza nell'IoT

L’immediato futuro vede ogni genere di dispositivo connesso e se questo può esser
nodi periferici rappresenta un’infinità di accessi disponibili per portare attacchi inform



Conoscere e usare Azure Sphere

Conosciamo la tecnologia di Microsoft per la creazione di applicazioni sicure, basate
scheda IoT.