UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

Domotica
Rischi e Tecnologie

Relatore:

Mauro Migliardi

Tesista:

Gabriele Romano

Anno 2021/2022

Dipartimento dell'ingegneria dell'informazione

Laurea in Ingegneria Informatica

Sommario

Acronimi e Abbreviazioni

AWS = Amazon Web Service

DNS = Domain Name Server

GDPR = General Data Protection Regulation

HTTP = Hyper Text Transfer Protocol

IFTTT = If This Then That

IoT = Internet of Things

IRC = Internet Relay Chat

MITM = man-in-the-middle

RFID = Radio Frequency Identification

SOHO = Small Office Home Office

TLS/SSL = Transport Layer Security/Secure Sockets Layer

UPnP = Universal Plug and Play

WiFi = Wireless Fidelity

ZC = ZigBee Coordinator

ZED = ZigBee End Device

ZR = ZigBee Router

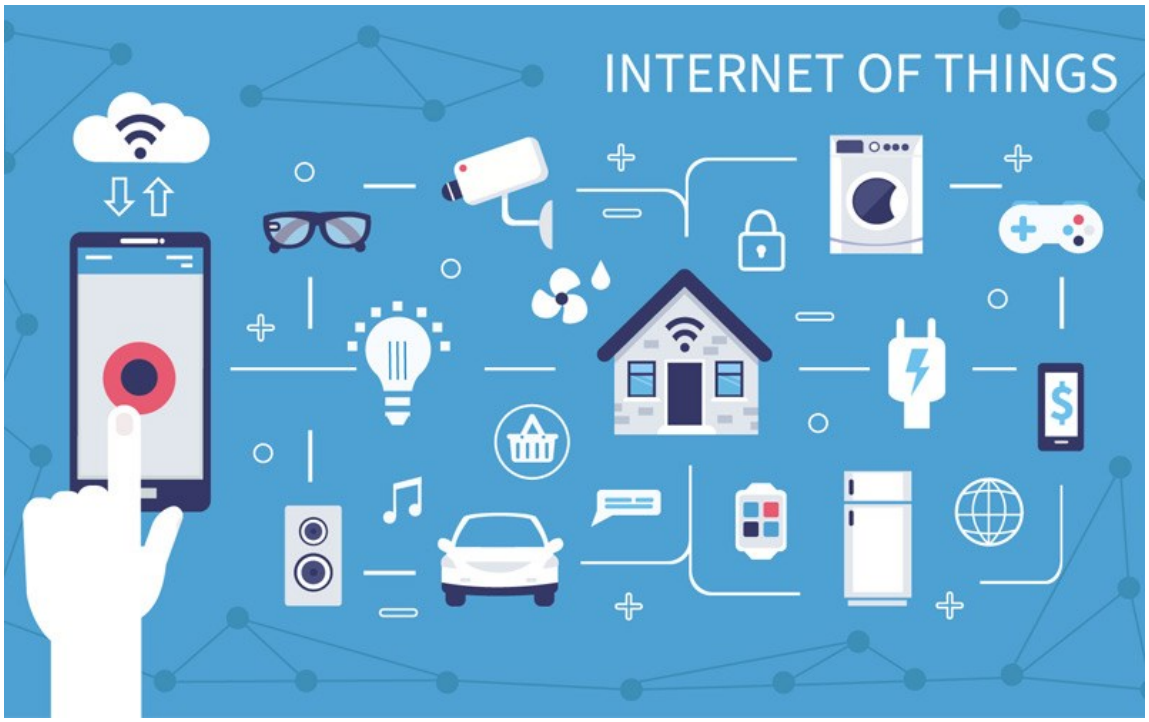
Introduzione

Domotica, Automazione, Smart Home sono tutte denominazioni dello stesso concetto, ovvero la possibilità, in un'abitazione o edificio, di poter controllare remotamente tutti i dispositivi connessi ad internet, utili per vivere quotidianamente in casa. Che sia un piccolo assistente virtuale, come Google Home, o qualsiasi altro dispositivo smart, come condizionatori, forni, televisioni, lavatrici, persino caffettiere e spazzolini, tutti totalmente controllabili da un semplice comando vocale, accessibile da IOS e Android, e rimanendo seduti comodamente sul divano. Oltretutto, l'intero ecosistema può anche essere automatizzato, portando dunque a non compiere quasi nessuna azione da parte dell'utente, dato che il sistema è già al corrente di tutto.

Il concetto

IoT e Smart Device

Innanzitutto, è necessario definire cosa siano questi dispositivi tecnologici che appartengono a quell'assioma che è conosciuto come ***internet of things*** (IoT) **– internet delle cose**. Termine coniato da Kevin Ashton, ingegnere inglese e ricercatore presso il *MIT*, che la usò la prima volta nel 1999.



L'IoT designa una molteplicità di oggetti, materiali, strumenti, apparecchiature, che grazie alla loro connessione alla rete internet, possono "dialogare" tra loro, scambiandosi messaggi, comprese informazioni su dati personali. L'obiettivo dell'internet delle cose è semplificare la vita di tutti i giorni, **migliorare la salute, l'ambiente, la mobilità e di conseguenza il tempo libero.** L'IoT consiste dunque in una rete di infrastrutture nelle quali innumerevoli sensori sono progettati per registrare, processare, immagazzinare dati localmente o interagendo tra loro sia nel medio raggio, mediante l'utilizzo di tecnologie a radio frequenza (per esempio Rfid, bluetooth ecc.), sia nel lungo raggio tramite una rete di comunicazione elettronica.

L'architettura dei sistemi si basa su un **network** che mette in comunicazione componenti fisiche intelligenti con una parte logica di gestione di dati, azioni e controlli. La parte concreta del sistema si compone di **smart devices** (come frigoriferi, TV e lavatrici) e di

sensori (ad es. di movimento, di temperatura e umidità) che eseguono comandi e monitorano l'ambiente.

Di questo ecosistema si identifica una branca denominata Domotica

Cos'è la domotica

Etimologia

Dall'unione del termine *domus*, che in latino significa "casa", e del suffisso greco *ticos*, che indica le discipline di applicazione. **È la scienza interdisciplinare che si occupa dello studio delle tecnologie adatte a migliorare la qualità della vita nella casa.**

Storia

Negli anni immediatamente successivi al 1940, ovvero l'invenzione del computer elettronico digitale, si ha avuto un grande incremento del settore in questione. Nel 1966, l'ingegnere Jim Sutherland crea il **ECHO IV**, che è stato il **primo dispositivo della home automation**, controllava temperature ed elettrodomestici, permetteva di inserire liste della spesa, ricette e altri promemoria di famiglia. Nel 1969 viene inaugurato ARPAnet, il precursore del moderno Internet, rendendo poi possibile lo sviluppo dell'IoT, offrendo a sempre più dispositivi di connettersi ad internet, il che ha portato allo sviluppo di ulteriori tecnologie raggiungendo i giorni nostri.

Applicazione

La domotica svolge un ruolo importantissimo nel rendere "intelligenti" apparecchiature, impianti e sistemi.

Con **smart home** (casa intelligente**)** si indica un ambiente - opportunamente progettato e tecnologicamente attrezzato - il quale mette a disposizione dell'utente impianti dove apparecchiature e sistemi sono in grado di svolgere funzioni parzialmente autonome (in grado di attivarsi in seguito ad un comando da parte dell'utente e svolgere anche funzioni non esplicitate) o completamente autonome (ovvero agiscono solo se si verificano determinate condizioni).

In alcuni casi si parla di **building automation**. L'edificio intelligente, con il supporto delle nuove tecnologie, permette la gestione coordinata, integrata e computerizzata degli impianti tecnologici (climatizzazione, distribuzione acqua, gas ed energia, impianti di sicurezza), delle reti informatiche e delle reti di comunicazione, allo scopo di migliorare la flessibilità di gestione, il comfort, la sicurezza e per migliorare la qualità dell'abitare e del lavorare

all'interno degli edifici. Da notare che la domotica non sempre consente di ottenere risparmi energetici in abitazioni private, infatti, il consumo stesso del sistema domotico potrebbe aumentare il fabbisogno energetico dell'abitazione.

Un'altra applicazione di largo utilizzo è legata alla videosorveglianza e alla gestione di accessi e presenze (in particolare mediante il monitoraggio di porte e finestre). Ambiti attualmente meno diffusi riguardano i sistemi di irrigazione intelligenti, le soluzioni SOHO e le applicazioni intelligenti per la salute, la cura e l'assistenza di anziani e malati.

Utilizzo

Le applicazioni domotiche legate alla sicurezza sono quelle che a oggi rappresentano la quota maggiore del **mercato delle smart houses**. Infatti, i sistemi di videosorveglianza, i sensori di movimento e antintrusione si attestano come il 35% del mercato globale.

Se si parla di domotica, il primo marchio che spicca inizialmente è **Google**, il colosso della Mountain View, con il suo smart speaker (si intende un dispositivo in grado di riconoscere la voce dell'umano ed effettuare azioni all'interno dell'ecosistema smart) ormai presente sul mercato da qualche anno, Google Home, ha conquistato molteplici abitazioni nel mondo. Più recentemente, anche Amazon, un altro colosso dell'economia globale, ha lanciato Alexa, con l'obiettivo di rivaleggiare con Google, sfruttando la possibilità di vendere il proprio smart speaker su Amazon ed eliminando il prodotto del rivale dal proprio magazzino.

Esistono ulteriori smart speaker di altri marchi famosi come HomePod della Apple e il prodotto della Xiaomi che sfrutta al suo interno l'assistente Google.

In ogni caso è proprio Google che ha fatto il primo passo nel mondo della domotica **implementando** su Google Home un software già presente nei telefoni Android, ovvero **Assistente Google**. L'utente, sfruttando l'assistente vocale, era in grado di eseguire azioni sul telefono come, ad esempio, alzare o abbassare il volume, attivare la modalità aereo, impostare sveglie, eventi, ed inviare messaggi. Ciò ha permesso di testare le funzionalità dell'assistente negli anni precedenti al lancio del Google Home, rendendolo già inizialmente ad essere quasi pronto per essere un dispositivo autonomo. Oggi è stato migliorato e apprende alcune abitudini dell'utente che ne sta facendo uso, e ciò combinato al sistema Google, sincronizzazioni ed elevata reperibilità nei servizi online, da origine ad una sorta di sistema multifunzione, in grado di adattarsi alle situazioni, per quanto possibile.

Tuttavia, non è, a livello di performance, come la nota Siri di Apple, di fatto si contraddistingue per alcune funzionalità che Siri non può avere, come ad esempio dettare un messaggio ed inviarlo tramite WhatsApp.

Le motivazioni sono essenzialmente questioni di privacy e accesso ai dati remoto. Se la Apple è una grande fortezza all'interno di un fossato (o almeno così appare), Android lo si può paragonare ad un castello sopra una collina, il quale è difficile da raggiungere ma che una volta superata la foresta il castello è del tutto scoperto.

Detto ciò, quasi tutti oggi stanno sempre di più avvicinandosi alla domotica, che sia solo lo smart speaker o un frigo smart, che sia un privato o un'azienda, in qualche modo, tutti hanno almeno un prodotto che permette di interfacciarsi nel mondo dell'IoT.

Infatti, come dimostra uno studio dell'osservatorio IoT della School of Management del Politecnico di Milano, il mercato delle smart houses in Italia ha raggiunto i **380 milioni di euro** nel 2018, con una crescita del 52% rispetto al 2017. Il trend positivo è uno dei più alti in Europa (solo la Spagna segna una crescita del +59%) ma, in termini assoluti di diffusione, il divario con gli altri paesi europei è ancora considerevole. Basti pensare che paesi come il Regno Unito e la Germania hanno mercati da 1,7-1,8 miliardi di euro. Oltre alla diffusione, anche il grado di conoscenza degli oggetti smart e connessi sta migliorando. Infatti, il 41% degli italiani possiede almeno un oggetto smart a casa, di cui la maggior parte sono correlati all'ambito della sicurezza. Tuttavia, le potenzialità di questi oggetti spesso non vengono

sfruttate appieno perché i consumatori non le ritengono utili o non sono in grado di usarle a causa dell'eccessiva complessità. Un altro aspetto che tende a frenare gli utenti sia nell'utilizzo sia nell'acquisto di smart device riguarda gli aspetti legati alla **privacy**. Infatti, è cresciuta la diffidenza dei consumatori nel condividere i dati personali, passando dal 27% al 51%.

Uno dei fattori che avvantaggia questo business sempre in crescita, è che la possibilità di controllare l'abitazione da remoto conferisce un certo senso di dominio da parte persona che ne sta facendo uso, un aspetto seppur molto inconscio, ma che pian piano accresce di continuo la convinzione che si possa controllare sempre al meglio la propria casa. Si inizia acquistando alcune lampadine per l'illuminazione interna, poi esterna, poi si prosegue comprando qualsiasi interruttore remoto comprese tapparelle, e prese. Alcuni accrescono il proprio controllo con la videosorveglianza, la climatizzazione, l'irrigazione, e solo una minima parte di persone in Italia, ma notevolmente più elevata in America, ha la propria rete wi-fi gestita dal modem di Google.

Molte compagnie sfruttano questa ambizione di controllo dei consumatori per essere maggiormente visibili all'interno del marketing, ed esistono infatti software e servizi di terze parti, tra cui **IFTTT** (If This Then That), Zapier e Zoho Flow che permettono la comunicazione e relativa automazione di dispositivi che non hanno particolare affinità con Google Home o Alexa. Ad esempio, la possibilità di accendere all'alba, automaticamente, i condizionatori, comandi che con il solo collegamento ai servizi Google non è possibile realizzare.

In altre parole, questi software facilitano l'utente, il quale può essere principiante o esperto, nella possibilità di automatizzazione di alcuni dispositivi.

Un ulteriore esempio, utilizzando Arlo, brand che si occupa di smart device relativi a campanelli e videosorveglianza, e mediante l'ausilio di IFTTT si può schedulare la seguente **automazione**:

"Se Arlo riceve un evento del campanello suonato, allora Google Home annuncia che qualcuno ha suonato alla porta"

Un altro esempio, stavolta con Tado, azienda che si occupa di termostati e condizionatori:

"Se la temperatura esterna in questo indirizzo raggiunge i 25 °, allora Google Home accende i condizionatori"

Ci sono molti altri esempi di questo genere, le possibilità sono quasi illimitate.

Un altro utilizzo può avvenire mediante l'hub (un dispositivo responsabile della comunicazione tra la rete Wi-Fi e i dispositivi di quell'ecosistema). Un esempio è l'ecosistema HUE, della Philips, che mediante l'hub HUE, connesso alla rete internet usando il cavo ethernet, e sfruttando il protocollo **ZigBee**, di cui parlerò in seguito, ha le potenzialità per eseguire comandi quasi istantaneamente. Una prova lampante è appunto la possibilità di poter sincronizzare un dispositivo di illuminazione con il proprio contenuto dello schermo del desktop. Ciò deve avvenire in tempo reale e con un ritardo trascurabile, un tempo era impensabile da realizzare, a causa di interferenza o colli di bottiglia della rete stessa, invece la coppia ethernet-protocollo ZigBee lo rende possibile.

Protocollo ZigBee

Zigbee è un protocollo standard utilizzato per **collegare in una rete wireless dispositivi domotici** come lampadine, prese, interruttori, serrature, sensori.

Normalmente si collega la rete ad un hub/gateway che supporta la tecnologia ZigBee, collegando poi alla rete tutti i dispositivi che rientrano nel raggio. I restanti dispositivi verranno controllati ugualmente ma attraverso un controllo indiretto ("di passaggio").

Struttura

La rete creata dall'insieme dei dispositivi imita proprio la struttura di un alveare, e da qui infatti che ne viene il nome. Al suo interno ospita tre diverse tipologie di api (dispositivi):

- **ZigBee Coordinator** (ZC): vi è un solo nodo che può agire da coordinatore, deve essere attivato per primo, funziona da tramite con gli altri nodi ed è il responsabile della formazione della rete e della sua sicurezza, spesso è l'hub gateway (cioè il ponte verso Internet).
- **ZigBee Router** (ZR): possono essercene più di uno, permette di estendere la copertura della rete e lo scambio di dati fra i diversi dispositivi trovando il percorso migliore. Può eseguire tutte le funzioni del nodo coordinatore tranne la formazione della rete.

- **ZigBee End Device** (ZED): sono dispositivi semplici, inviano e ricevono informazioni ma non possono eseguire altre funzioni nella rete. Ogni end device può essere connesso a un router o al coordinatore. Solitamente sono dotati di batteria e consumano energia solo in fase di trasmissione dati.

Molto spesso, il ZC è compreso nello smart speaker o nell'hub, mentre gli ZED sono dispositivi non presenti in tutti le case e sono vicini alle pareti, ad esempio dei sensori (che siano di movimento o di temperatura). Gli ZR invece sono tutti i dispositivi restanti che si trova sparsi in tutta la casa, come l'illuminazione o elettrodomestici.

Gli interruttori invece sono una via di mezzo e dipende dalla casa produttrice come identificarlo.

Differenze con le altre tecnologie

In questa tabella sono elencati i principali vantaggi e svantaggi delle diverse tecnologie

	WiFi	Bluetooth LE (Low Energy)	Zigbee
Lancio	1997	2010	2003
Standard	IEEE 802.11.1	IEEE 802.15.1	IEEE 802.15.4
Banda	2,4 GHz	2,4 GHz	2,4 GHz
Copertura	100 m	30 m	10÷100 m
Velocità	54 Mb/s	1 Mb/s	250 kb/s
Topologia	Star	Scatternet	Mesh
Consumo	Alto	Basso	Basso

Figura 1 Star Topology

La topologia Star è quella più comune, ed è quella utilizzata nella rete Wi-Fi. Nella quale ogni dispositivo è connesso con il dispositivo centrale, che gestisce tutte le comunicazioni.

La ScatterNet è una topologia di rete nella quale più PicoNet, ovvero una connessione che si instaura tra due o più dispositivi Bluethooth, internamente può essere composta da tre tipi di dispositivi:

- Master → Pallini Rossi
- Slave → Pallini Viola

Ogni dispositivo può sia master che slave, l'unione di queste PicoNet rendere possibile una ScatterNet da nove o più dispositivi.

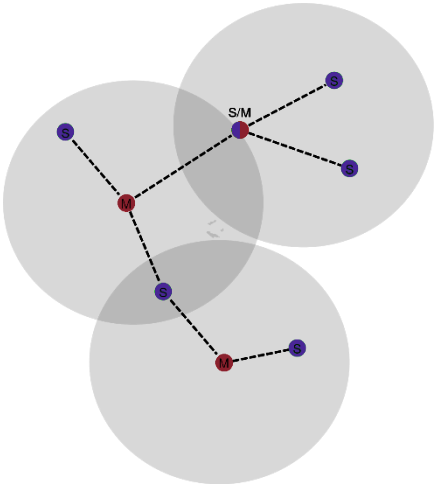


Figura 2 ScatterNet Topology

Nella Topologia Mesh solo alcuni dispositivi sono interconnessi, mentre la restante parte sono dispositivi finali, ciò permette di dividere il lavoro del gateway, ovvero se esso non raggiunge il dispositivo finale ci i dispositivi intermedi svolgeranno il lavoro.

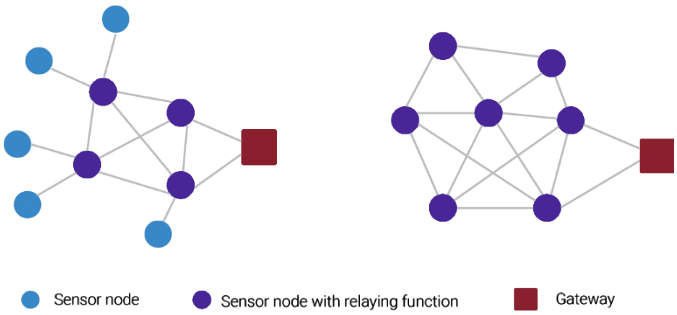


Figura 3 Partial and Full Mesh Topology

Differenze tra Bluetooth e Bluetooth low Energy

Le ultime due tecnologie differiscono sostanzialmente nell'utilizzo che ne viene fatto, il primo è comunemente sfruttato nella comunicazione tra telefoni e altri tipi di dispositivi, mentre il secondo è sfruttato nelle comunicazioni tra dispositivi dello stesso tipo, come ad esempio degli smart device. Inoltre, consuma un quantitativo di energia irrisorio.

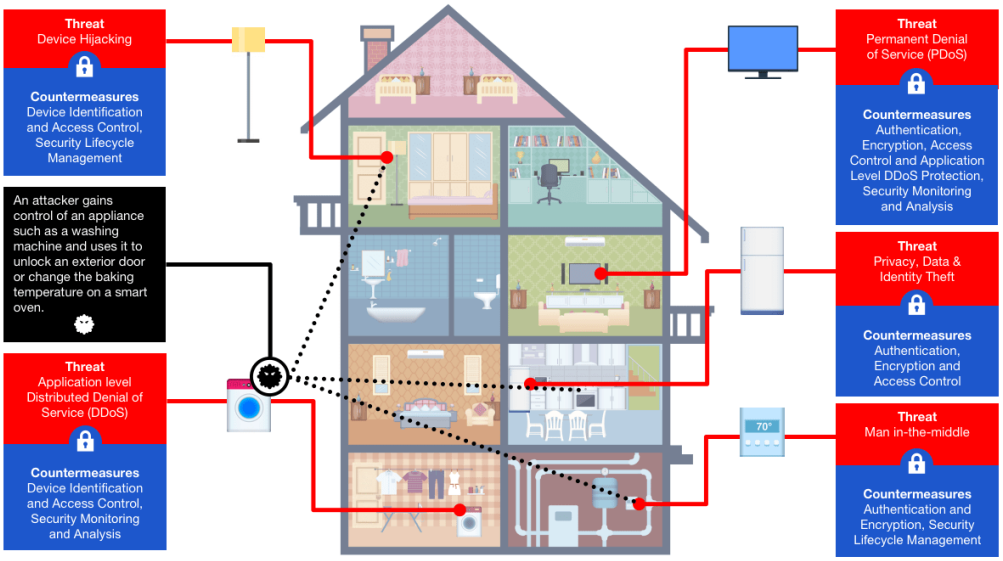
Sicurezza e Condivisione dati

Il Concetto

Tuttavia, come sempre, esiste un'altra faccia della medaglia, e questa riguarda la sicurezza dei nostri preziosi dati personali.

Molti utenti accettano senza pensare le **condizioni di utilizzo**, azione spesso necessaria durante la creazione di molti account di diverse piattaforme online, il più delle volte nascondono postille nelle quali è indicato che alcuni dei nostri dati saranno utilizzati a scopo pubblicitario per altre aziende o per "**profilare**" le nostre attività ed abitudini. Quale è il significato di quanto detto sopra? Sostanzialmente qualsiasi cosa diciamo o cerchiamo sul web, la ritroviamo sott'occhio qualche minuto dopo sugli Ads presenti nei siti web nelle applicazioni. Ed è qui che inizia la polemica sui dati personali che ormai, non sono più tanto personali.

Purtroppo, è una realtà che molta gente ha accettato da tempo, perché ormai qualsiasi iniziativa per evitare ciò sarebbe superflua, ad oggi internet è ovunque ed è sufficiente



accedere al browser Google, che magicamente la nostra posizione (approssimativa) viene regalata a qualche grande società.

Allo stesso modo i dispositivi IoT che dialogano con noi e tra di loro ricevono e scambiano ingenti quantità di dati e informazioni personali, spesso anche dati più sensibili come quelli riguardanti la salute.

Oggi con il **nuovo Regolamento europeo sulla privacy (GDPR)** non si parla più propriamente di “dati sensibili” ma di “categorie particolari di dati personali”, ed è proprio questo documento che sancisce i limiti nei quali la “vendita” dei nostri dati deve essere rispettata.

Il GDPR è il regolamento istituito dall’Unione Europea nel 2016/18 per fornire le direttive base riguardanti la gestione dei dati sensibili di ogni individuo.

Dato Personale → “S’intende come dato personale qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato») attraverso dati quali il nome, il cognome, un codice identificativo on line, dati relativi all’ubicazione nonché tutti i dati indicanti le sue caratteristiche fisiche, fisiologiche, genetiche, psichiche, economiche, culturali o sociali”.

Vulnerabilità e Soluzioni

Molti esperti concordano nell'affermare che, quando si parla di dispositivi IoT, **non dobbiamo chiederci "se" ma "quando" verranno attaccati**, perché si tratta di dispositivi estremamente vulnerabili e con livelli di protezioni minimi. Non è raro che molti dati di un determinato server subiscano un attacco hacker, nel caso dell’IoT e della domotica i nostri dati sono ricavati direttamente da noi in tempo reale e anche usando le nostre registrazioni vocali (ad esempio i comandi lanciati da Google Home o Alexa).

Dato che ormai il rapporto vocale tra le persone e l’apparecchio è possibile perché il dispositivo è dotato della capacità di ascolto di tutto ciò che accade nell’ambiente e non solo del comando vocale che di volta in volta gli possa essere impartito**. Inoltre, esso è, per un periodo di tempo limitato, in attività e dunque in grado di ascoltare ed elaborare i suoni che percepisce nell’ambiente** (e anche, attraverso i rumori i comportamenti di chi li produce). Proprio a causa di ciò molte persone non si sentono sicuri nel possedere uno di questi dispositivi in casa.

È altresì vero che nelle nuove versioni degli smart speaker è presente anche un interruttore che consente di disattivare i microfoni, e quindi anche la capacità di ascolto dell’apparato, ma ovviamente questo significa rinunciare, per il tempo della disattivazione, a ogni funzionalità dell’apparato stesso.

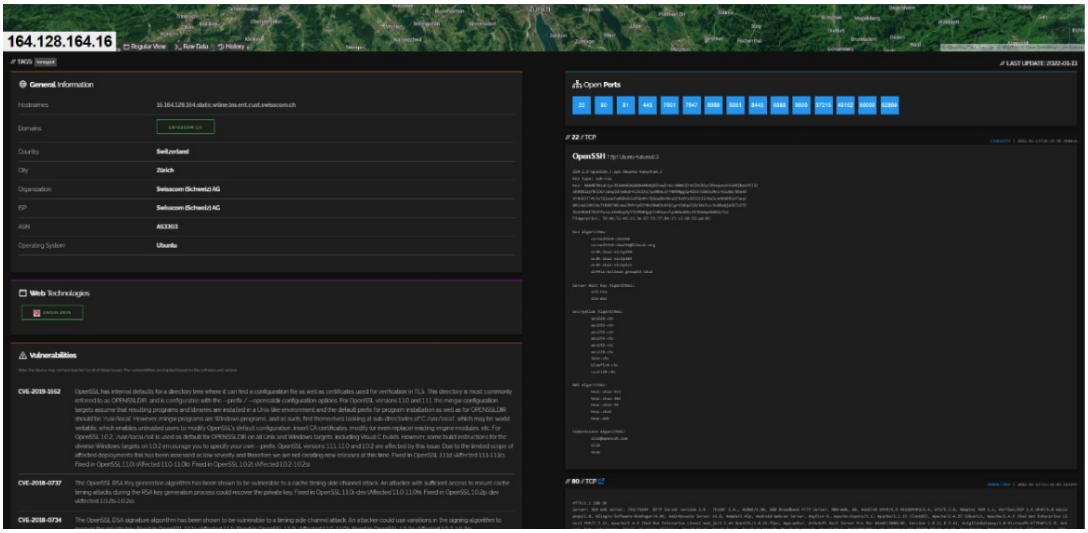
Va tenuto presente che l’apparecchio, esattamente come gli smartphone, resta comunque **sempre in collegamento con il sistema** Google e con gli apparecchi della casa ai quali è

stato connesso. Ciò significa che anche quando non viene usato, esso trasmette continuamente messaggi al server della casa madre.

Insomma, queste nuove forme di Assistenti Intelligenti studiati per la casa possono anche essere definite, se si vuole, come i moderni maggiordomi dell'era digitale, ma, esattamente come i maggiordomi vittoriani, sanno tutto di ciò che accade nella casa ed inoltre registrano e ritrasmettono.

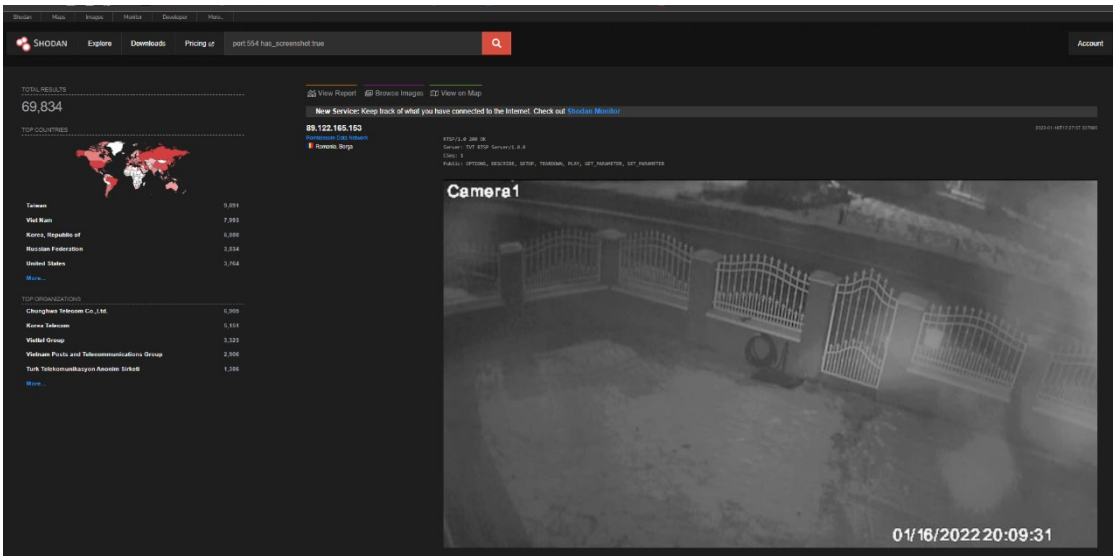
Se ci pensiamo bene le piccole ipCam che distribuiamo all'interno delle nostre case, banalmente per tenere sotto controllo il bebè, sono dotate di un sistema operativo che, seppur minimale, è connesso ad Internet ed è quindi **soggetto ad attacchi di tipo informatico.** Questo può avvenire sfruttando qualche "falla" lasciata intenzionalmente dagli sviluppatori, con l'obiettivo di monitorare il funzionamento, ma che, utilizzato per fini criminosi, potrebbe dare la possibilità di ottenere informazioni come la presenza in casa dell'utente o meno.

Relativamente alle ipCam, esiste un "motore di ricerca", **Shodan.io**, che permette di accedere a qualsiasi sia connessa ad internet ad eccezione dei siti web. Mediante numerosi metadata, Shodan è in grado di catalogare tutti gli indirizzi IP in categorie (webcam, database, server). Cliccando l'indirizzo corrispondente è possibile visualizzare informazioni generali, le porte accessibili e le vulnerabilità del dispositivo.

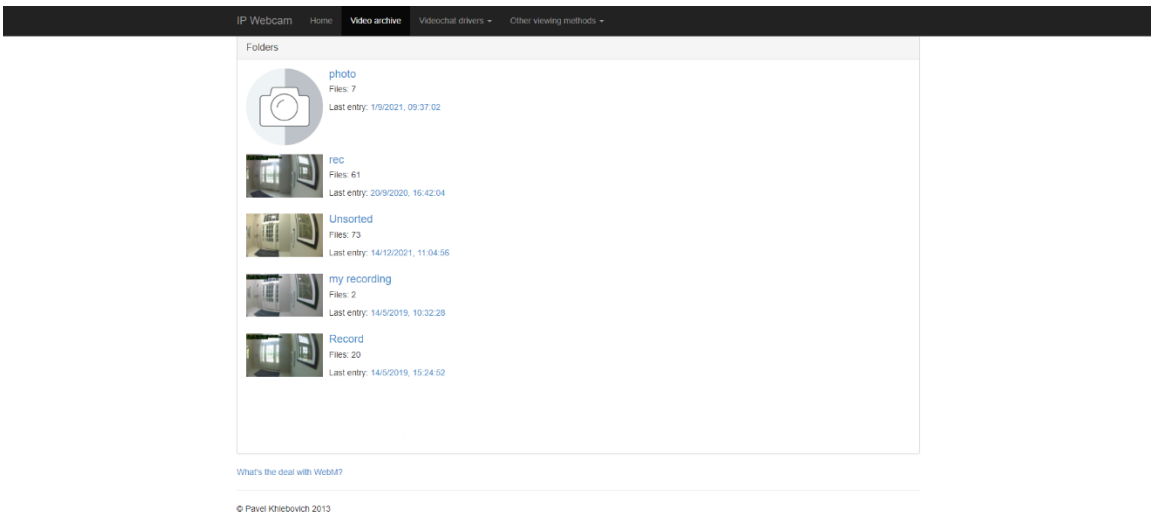


Questo sito è altrettanto potente quanto spaventoso dato che mette in evidenza il modo per accedere a quel determinato indirizzo IP, ciò ci fornisce una nuova prospettiva di quanto spesso siano inaffidabili i sistemi in cui riponiamo la nostra fiducia e consegniamo inavvertitamente i nostri dati sensibili.

Ad esempio, con una semplice query *"port:554 has_screenshot:true"* è possibile ottenere tutti gli indirizzi IP che hanno la porta 554 aperta, e concedono di salvare alcuni screenshot di ciò che registrano. Mediante questa semplice ricerca è possibile vedere una moltitudine di screenshot di ipCam in tutto il mondo senza alcuna difficoltà, scoprendone luogo e orario.



Un ulteriore prova è la ricerca, *"webcam port:8080"*, la quale mostra una moltitudine indirizzi IP di webcam nei quali la porta 8080 è aperta, ciò ci consente di accedere alla pagina di configurazione del dispositivo, alterare le impostazioni o, addirittura accedere alle registrazioni archiviate, tutto ciò in pochi clic.



Nel complesso, **è legale? SI**. Sostanzialmente Shodan provvede a raccogliere dati presenti sulla rete (IoT) e renderli disponibili. Essi contengono già strutture e sono già leggibili. Quindi non fa altro che rendere accessibili informazioni già presenti in rete. Ovviamente è dell'utente la responsabilità delle proprie azioni.

La domanda più corretta sarebbe, **è pericoloso? Dipende**, come si può facilmente intuire eventuali hacker possono ricavare informazioni di vitale importanza e successivamente attaccare il proprio obiettivo. Tutte le possibili vittime dovrebbero difendersi nel miglior modo possibile, nei prossimi paragrafi vengono spiegati nel dettaglio tecniche di attacco e di difesa online.

Uno smart device ha quattro componenti principali:

1. **Il dispositivo** → hardware acquistato (Google home, Alexa)
2. **L'applicazione mobil**e → l'applicazione che interagisce con il dispositivo
3. **Cloud end point** → i servizi Internet utilizzati dal dispositivo e dall'applicazione mobile
4. **Network communication** → traffico di rete di ogni componente (Locale e di Internet)

Ognuna di queste componenti ha le proprie minacce e vulnerabilità. Queste possono essere sfruttate dai criminali della rete per estorcere informazioni senza che noi ne veniamo a conoscenza. I possibili attaccanti sono:

A. **Attaccante Esterno** (Internet)

   L'Attaccante esterno non ha bisogno di un diretto accesso alla connessione nella quale i dispositivi sono collegati e può utilizzare tutte le vulnerabilità e i bug conosciuti per infettare il dispositivo. questo tipo di attaccanti è il più pericoloso per la sua capacità di infettare un gran numero di dispositivi.

B. **Attaccante Interno** (Local Network)

   Questo attaccante è presente all'interno della rete alla quale sono connessi i dispositivi e può effettuare attacchi diretti.

C. **Attaccante vicino geograficamente** (Vicino di Casa)

   Questo tipo di attaccante è presente fisicamente vicino alla rete alla quale sono connessi i dispositivi e può avviare attacchi durante il setup del

dispositivo oppure utilizzando le low-energy network (Bluetooth, Zigbee, or ZWave).

Il dispositivo

Alcuni dispositivi IoT per uso domestico sono stati commercializzati molto velocemente e le loro misure di sicurezza non sono state adeguatamente verificate. In alcuni casi, i manuali per l'utente non si dilungano sui problemi di privacy e non forniscono informazioni sufficienti a garantire la sicurezza del dispositivo. Ad esempio, i baby monitor e le telecamere di sicurezza possono essere attaccati semplicemente, offrendo ai criminali informatici la possibilità di vedere l'interno della casa.

Di seguito i momenti critici e le possibilità di attacco:

- **Accoppiamento Internet** - configurazione delle credenziali per connettere il dispositivo a Internet
  - ✗ Un attaccante vicino può fisicamente dirottare la configurazione sfruttando la scarsa sicurezza del Wi-Fi o delle tecnologie low-energy.
  - ✓ Una connessione Internet cablata o un input manuale delle credenziali risolverebbe il problema.
- **Configurazione** - configurazione delle impostazioni, creare un account durante la fase di setup
  - ✗ Un attaccante interno o esterno è a conoscenza delle deboli configurazioni di default del dispositivo durante la fase di setup e le potrebbe sfruttare a suo vantaggio.
  - ✓ Una preconfigurazione più efficace risolverebbe il problema. La criticità in questa soluzione è che purtroppo sono le case costruttrici dei prodotti che dovrebbero agire in questa fase.
- **Aggiornabilità** - Possibilità del dispositivo di aggiornarsi automaticamente o manualmente
  - ✗ Qualsiasi tipo di attaccante può scegliere come bersaglio un dispositivo “out of date” (non aggiornato), e quindi sfruttarne vulnerabilità o bug presenti in quella versione.
  - ✓ L'aggiornamento automatico permetterebbe di risolvere il problema.

- **Servizi a rischio** - Servizi del dispositivo attivi visibili a chiunque (Non criptati, come UPnP, mDNS, HTTP server, etc...

  ✗ Un attaccante interno o esterno ha una maggiore superficie di attacco, perché può scegliere uno dei qualsiasi servizi che non possiedono criptazione e di conseguenza otterrebbe tutti i dati in chiaro

  ✓ Un dispositivo che utilizza servizi criptati è più sicuro (es: HTTPS).

- **Vulnerabilità** - Eseguire servizi sul dispositivo che contengono vulnerabilità

  ✗ Qualsiasi attaccante può sfruttare uno di questi servizi per infettare e dirottare il dispositivo, più dispositivi dirottati potrebbero dar luogo ad una botnet (una collezione di computer compromessi che stanno eseguendo programmi malevoli e controllati remotamente da cybercriminali. I cyber criminali agiscono remotamente attraverso processi automatici (bot) in canali pubblici (IRC)).

  ✓ Assicurarsi che la fonte di questi servizi sia attendibile e riconosciuta da qualche ente.

Sono state fornite delle soluzioni specifiche per ogni problema, di seguito propongo una soluzione più generica ma che garantisce un adeguato stato di sicurezza, **isolare una rete dedicata**. Permette di separare la rete dedicata ai dispositivi IoT dalle altre reti. Si tratta di un'operazione piuttosto semplice, perché basta configurare una rete guest dalla homepage di configurazione del router e connettere solamente i dispositivi IoT di uso domestico.

Per fare un esempio, se il frigorifero dovesse subire un attacco ed essere trasformato nel componente di una **botnet** che invia spam o ricerca criptovalute, collegandolo a una rete guest, esso viene estraniato dalla rete in cui principalmente accediamo ai nostri account più a rischio, come quello bancario, permettendoci di salvaguardarli.

L'applicazione mobile

Molti utenti controllano la loro Smart Home tramite un’applicazione sullo smartphone, trasformando quest'ultimo in un preziosissimo database per chiunque desideri intromettersi nella vita privata del proprietario.

Purtroppo, la stessa App potrebbe non salvaguardarci adeguatamente. Ci sono molti brand IoT in commercio, perché affidarsi al più costoso se è presente una sottomarca che svolge la

stessa funzione? Sostanzialmente il più delle volte un brand ha un costo maggiorato non solo perché è migliore esteticamente o è semplicemente più noto, il vero motivo è dato dalla grande efficienza ed efficacia del Backend (ovvero l'infrastruttura che l'utente finale non vede e non controlla, ma che permette lo svolgimento dei compiti richiesti), vale a dire che è ben progettato e poco vulnerabile contro eventuali attacchi esterni.

Di seguito i momenti critici e le possibilità di attacco:

- **Dati sensibili** - include come le chiavi API, le password e le chiavi crittografate che andrebbero codificati nell'applicazione
  - ✗ non essendo codificate un attaccante potrebbe estrarle e utilizzarli a proprio piacimento, senza che l'utente se ne accorga.
  - ✓ Una buona regola è quella di criptare questi codici.
- **Errori di programmazione** - l'implementazione di errori o uso incorretto delle librerie include vettori di crittografia deboli e seeds facilmente indovinabili (Utilizzati nei generatori di numeri pseudo randomici)
  - ✗ Qualsiasi attaccante può sfruttare l'inizializzazione scorretta di un protocollo crittografico per ricavare informazioni sensibili.
  - ✓ Utilizzare pratiche di uso comune garantirebbe una maggior sicurezza, ad esempio informarsi adeguatamente sull'uso di una determinata libreria per poterla sfruttare al meglio e nel modo corretto.
- **Over-privileged** (sovra privilegiato) - le applicazioni richiedono più privilegi di quelli che necessitano.
  - ✗ Un attaccante interno può utilizzare i permessi concessi per ricavare informazioni sensibili sugli utenti finali. Principalmente gli utenti vittima di ciò sono uomini e donne che hanno poca dimestichezza con il proprio smartphone e non hanno la capacità di comprendere cosa l'applicazione stia richiedendo.
  - ✓ Consentire l'accesso solo ai permessi necessari ed incentivare l'istruzione di tutte quelle persone che hanno poca dimestichezza con questo mondo.

Come per il precedente punto dell'elenco una soluzione generica è di assicurarsi che i dispositivi di accesso, controllo e distribuzione della rete siano protetti da password, o un qualsiasi **metodo di autenticazione**. Sembra banale come raccomandazione, ma molte

persone oggi non comprendono appieno cosa hanno tra le loro mani, non è un semplice giocattolo per chiamare ma è molto di più.

Cloud end point

La rete domestica potrebbe anch'essa non essere affidabile e i dati conservati al suo interno potrebbero essere soggetti a violazioni. Un cybercriminale potrebbe monitorare gli schemi di utilizzo dei vari dispositivi, e ottenere da ciò le tue routine quotidiane. Il cloud è il luogo nel quale vanno a finire i nostri dati personali e qualsiasi dato riguardante, poter entrare in uno dei essi ed estrapolarne informazioni non è un'operazione semplice, tuttavia neanche impossibile.

- **Categorie di dominio** - definisco tre tipi di categorie di domini: principale, di terze parti, ibrido. Il primo è posseduto e gestito dal venditore del prodotto, il secondo, sono end-point usati da servizi esterni come Google Maps, mentre il terzo sono end-point eseguiti su un'infrastruttura Cloud come AWS ma gestiti dal venditore del dispositivo.
    - ✗ Un attaccante ha più probabilità di attacco, tante quanto il numero di end-point presenti. Inoltre, se si utilizzano domini di terze parti il rischio aumenta. Gli end-point ibridi corrono il rischio di esporre informazioni dell'utente ai provider dei Cloud.
- **Configurazione TLS** - si riferisce alla configurazione del livello TLS/SSL, ed include l'uso di un valido e affidabile certificato, in modo da evitare le vulnerabilità dovute alle versioni del livello TLS/SSL
    - ✗ Un attaccante può sfruttare le debolezze usando la chiave pubblica delle comunicazioni che utilizzano l'infrastruttura in modo tale da compromettere l'integrità dello scambio di messaggi.
    - ✗ Certificati self-signed possono rischiare l'impersonazione da parte dell'attaccante, specialmente se non implementano un controllo dei certificati.
    - ✗ Un errore tra i nomi dei certificati può indicare l'incorretta configurazione del TLS/SSL e ciò può essere poi sfruttato dall'attaccante.

- ✗ Le versioni più vulnerabili del TSL/SSL possono perdere informazioni a proposito del contenuto criptato che poi può essere usato dall'attaccante per modificare la comunicazione tra i due interlocutori.

- **Servizi vulnerabili** - il rilascio di servizi vulnerabili sul Cloud include l'uso di autenticazione in chiaro, configurazioni errate e servizi dirottabili.

  - ✗ Un attaccante può sfruttare le vulnerabilità dei servizi del Cloud per avere controllo sui dispositivi. Principalmente i sistemi operativi più vecchi dato che non hanno più il supporto degli aggiornamenti possono essere i principali target.

  - ✗ Gli attaccanti interni ed esterni possono sfruttare le autenticazioni in chiaro per guadagnare l'accesso alla rete.

Dopo aver protetto le reti per assicurarti che nessuno dei tuoi dispositivi IoT possa accedere ai tuoi dati personali o controllare la rete, è necessario continuare a **monitorare ciò che succede** all'interno di essa, ed essere costantemente vigili, periodicamente adottare strategie di cambiamento password e, per gli utenti più esperti, assicurarsi sempre che i servizi che vengono utilizzati siano affidabili.

Network communication

Quest'ultima sezione invece si riferisce ai collegamenti locali tra dispositivi smart e il loro interfacciamento con il server esterno

- **Protocolli** → l'uso di servizi DNS di terze parti, HTTP, UPnP o protocolli personalizzati può intaccare la sicurezza della connessione

  - ✗ DNS di terze parti → questo tipo di DNS può memorizzare pattern dell'utente e causare problemi di privacy ad esso.

  - ✓ è meglio utilizzare i DNS locali.

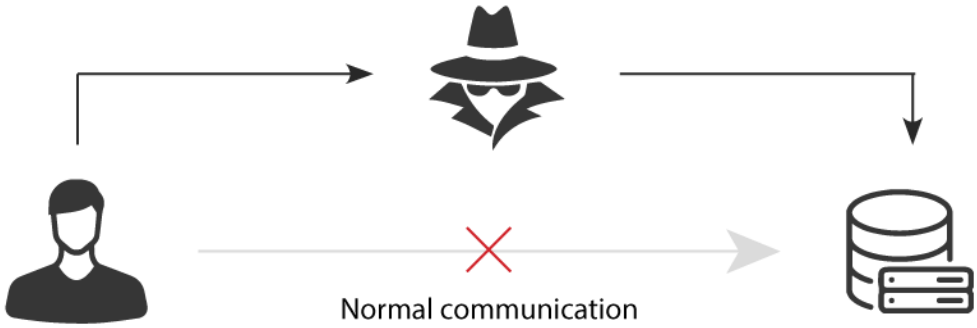
  - ✗ HTTP → un attaccante può curiosare connessioni HTTP dato che non offrono integrità e confidenzialità.

  - ✓ Usare HTTPS risolverebbe il problema.

  - ✗ UPnP → un attaccante interno può inviare comandi e controllare i dispositivi che usano questo protocollo, dato che esso non include l'autenticazione.

- ✓ Utilizzare gli stessi comandi ma con HTTPS è più sicuro.
- ✗ NTPv3 → Un attaccante interno ha la possibilità di fare breccia pur essendoci dei certificati, perché questo protocollo non garantisce l'integrità dei certificati.
- ✓ Usare NTPv4 è più sicuro, essendo una versione più aggiornata.
- ✗ Protocolli Personalizzati → questi protocolli non sono standard e quindi non possedere misure di sicurezza adeguate, dato che potrebbero non avere rispettato le misure standard.
- ✓ Utilizzare protocolli standard garantisce più sicurezza.

- **Man-In-The-Middle** → un attaccante può intercettare la comunicazione tra i componenti del dispositivo e modificarne il contenuto, compromettendo così la comunicazione.



- ✗ Non è raro che all'interno di una comunicazione via internet, l'attaccante cerchi in ogni modo di ottenere più dati possibili, ed il problema più grosso è che chi subisce l'attacca non ha praticamente mezzi a disposizione per sapere se lo scambio di dati avviene in modo sicuro e corretto
- ✓ Componenti che verificano endpoint e certificati sono più sicuri, quindi comunicazioni mediante il SSL che sfruttano la potenzialità dei certificati ci permettono di avere maggiore controllo

- **Criptazione** → se i dati non vengono criptati, un attaccante può curiosare sulla comunicazione tra i componenti della smart home e trarne delle informazioni significative.

✗ Direttamente correlato al MITM, non utilizzare la criptazione permette all'attaccante, non solo di vedere il contenuto senza problemi, ma anche di poterlo alterare a proprio vantaggio

✓ Componenti che usano la criptazione su tutta la comunicazione sono più sicuri.

Da queste vulnerabilità scienziati ricercatori ed esperti in networking ha prodotto una tabella che rappresenta una classifica per i dispositivi IoT più conosciuti, di seguito ve ne mostro alcuni:

Device	Device Grade	Mobile Grade	Cloud Grade	Network Grade
Google Home	78.57% (C)	69.23% (D)	94.57% (A)	53.57% (F)
Amazon Echo	88.1% (B)	46.15% (F)	69.57% (D)	78.57% (C)
Apple HomePod	85.71% (B)	100% (A)	56.52% (F)	89.29% (B)
Philips HUE Hub	90.48% (A)	61.54% (D)	95.65% (A)	75.0% (C)
Samsung SmartTV	66.67% (D)	69.23% (D)	79.35% (C)	75.0% (C)

Osservando dalla tabella, il Cloud Google potrebbe essere il più affidabile; tuttavia, i metodi di comunicazione tra dispositivi e Cloud e l'applicazione stessa non è dei migliori. D'altra parte, se osserviamo la Apple, la comunicazione e l'applicazione mobile gode di un ottimo grado di affidabilità ma il Cloud non è per nulla all'altezza.

Realtà e contromisure

Il caso Xiaomi-Google

Dalla tabella nel precedente capitolo possiamo ricavare su quali aspetti quel dispositivo defice, essi possono causare dei problemi concreti nell'uso quotidiano, un esempio realmente accaduto riguarda le **Xiaomi Mijia 1080p Smart IP** (un modello di videocamere per la smart home).

La vicenda è salita alla ribalta il 2 gennaio del 2020, quando un utente sul popolare social **Reddit** ha postato un intervento in cui veniva evidenziato come le videocamere in questione stessero, sì effettivamente riprendendo l'ambiente circostante, però sullo smart display comparivano immagini appartenenti ad altri ambienti e persone.

Prima di approfondire la questione però, è essenziale chiarire bene ed esaustivamente quali siano i componenti in gioco. Da una parte abbiamo le **videocamere Xiaomi** e dall'altra un **Google Nest Hub**.

Un Google Nest Hub può essere considerato come uno schermo intelligente mediante cui avere la possibilità di vedere video su **Youtube** o i nostri programmi preferiti in streaming o anche ascoltare della musica tramite l'integrazione con l'app dedicata, come **Spotify**. Oltre all'aspetto puramente ludico però, un Google Nest Hub può essere anche impiegato per prendere il **controllo degli aspetti gestionali della domotica** con un semplice tocco sullo schermo. Inoltre, può anche ricevere comandi vocali. È una sorta di dispositivo multifunzione, in quanto tale può anche fungere da **schermo per mostrare le immagini** in tempo reale acquisite dalle videocamere o dal sistema di videosorveglianza presente in casa, ed ecco quindi che arriviamo al secondo elemento in gioco, le videocamere Xiaomi.

La videocamera risultava effettivamente funzionante, solo che le immagini visualizzate sullo schermo del Google Nest Hub erano quelle di altri utenti in possesso del medesimo modello.

Si può quindi facilmente immaginare il disorientamento nello scoprire come una videocamera potesse aver trasmesso immagini e fotogrammi personali e intimi a dei perfetti

sconosciuti, con tutti i rischi per la sicurezza e la privacy che questo comportava. **Non è solo una mera questione di violazione della privacy**, seppure questa sia indiscutibilmente fondamentale e un diritto garantito, quanto il potenziale rischio derivante dal fatto che immagini simili potessero essere acquisite da malintenzionati o hacker. L'intera faccenda ha suscitato immediatamente le reazioni più disparate, inizialmente si è anche pensato che fosse un malfunzionamento legato a un mancato aggiornamento o a degli apparati non aggiornati o fuori produzione, ma tutti i dispositivi coinvolti nel caso erano nuovi e aggiornati all'ultima versione del firmware.

Immediatamente Google e Xiaomi hanno cercato di comprendere i motivi di questo disguido tecnico, per così dire, e in data 17 gennaio 2020 Xiaomi ha annunciato di aver risolto con successo il bug responsabile dell'interferenza ed estromissione delle loro videocamere Mi dal sistema proprietario di Google.

Sono ovviamente seguite delle scuse dovute, in cui la società ha espresso il proprio disappunto per l'accadimento dichiarando come la tutela della privacy e della sicurezza degli utenti sia uno degli obiettivi dichiarati aziendali. Report successivi hanno messo in evidenza come il bizzarro fenomeno fosse stato causato dall'implementazione di una nuova funzionalità nelle videocamere e come avesse colpito poco più di un migliaio di utenti.

Si tratti di numeri che forse per un'azienda possono essere poco significativi, se si tengono conto dei milioni di prodotti immessi sul mercato, però la corsa nel cercare di risolvere l'increscioso incidente e le dovute scuse hanno messo ancora più in evidenza come la privacy e la sicurezza siano tematiche quanto mai degne di considerazioni oggigiorno.

Il caso dell'ascolto prolungato

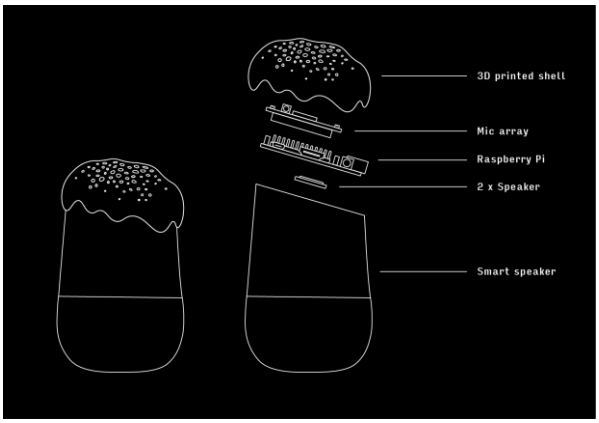
Un altro recente scandalo coi Google Nest porta in primo piano la possibilità che il microfono, utilizzato per impartire comandi all'assistente vocale, rimanga attivo svariati minuti anche dopo la fine del comando. Un evento correlato a ciò, riguarda Alexa. Un uomo aveva richiesto al proprio Echo Dot la sua cronologia delle tracce audio relative ai comandi impartiti, ed in aggiunta alle proprie, riceve anche la cronologia dei comandi di un altro utente, totalmente sconosciuto, Amazon si è subito attivata giustificandosi, assicurando che fosse un caso isolato e che il bug è stato immediatamente risolto. Errare è umano, ma siamo davvero sicuri di lasciare i nostri dati personali in balia di errori umani? Un errore di questo genere combinato alla questione del prolungato ascolto indesiderato dell'assistente virtuale, potrebbe portare a situazioni in cui le nostre conversazioni, probabilmente private, come

questioni lavorative, ad esempio progetti futuri per un'azienda che si stavano anticipando in buona fede alla propria famiglia, potrebbero girare in rete ed arrivare in casa di uno sconosciuto, che malauguratamente potrebbe essere un addetto di un'azienda rivale.

Il Parassita

Alcune volte la soluzione è più immediata di ciò che si pensi, noi non possiamo controllare i dati in rete ma possiamo limitare i dati che inviamo, un esempio molto innovativo è questo "parassita" dell'assistente vocale, denominato **Progetto Alias**.(Ideato da Bjørn Karmann)

Questo piccolo dispositivo permette di evitare l'ascolto indesiderato da parte dello smart device. Il metodo di funzionamento è relativamente semplice, appena l'utente pronuncia la parola chiave impostata su Alias (es: Hey Alias), il parassita smette di trasmettere il rumore bianco e trasmette "Ok Google o Alexa" all'assistente. Ciò permette di ascoltare ciò che noi diremo e successivamente eseguire il comando. Nel momento in cui abbiamo terminato di parlare Alias riprenderà a trasmettere rumore bianco all'assistente. Una soluzione semplice, e a basso prezzo, dato che basta un Raspberry Pi per tutto ciò. In questo modo si possono limitare i danni di eventuali bug causati da errori commessi dall'uomo, concedendoci più protezione.



Conclusione

Come potrebbero evolversi tutti questi dispositivi in futuro? Come si evolveranno i possibili attaccanti? E come cambierà il concetto di privacy? Le ricerche oggigiorno si concentrano verso un mondo più automatizzato, più controllato, con il minor numero di rischi possibili, specie su Internet, ma si riuscirà veramente in tutto ciò?

Molti film e serie tv cercano di dare la loro opinione riguardo questo aspetto, ad esempio un episodio della famosa serie di Netflix **Love Death + Robots** ci fornisce una visione di come potrebbe essere in futuro una casa domotica, nella quale qualsiasi oggetto è parte dell'IoT, che sia una maniglia, una finestra, il lavandino, delle foto, il tutto è interconnesso. Nell'episodio in questione il robot responsabile della pulizia cercava di correggere la posizione di una foto e la proprietaria continuava a contrastarlo, il tutto si conclude con la proprietaria che cerca di scappare, dato che aveva innescato involontariamente un sistema di eliminazione del proprietario, dal robot, e così tutto l'ecosistema interconnesso si rivolta verso di lei.

Ovviamente questo è un caso estremo, ma cosa impedisce che diventi effettivamente così, il call center chiamato dalla proprietaria era anch'esso un bot, inoltre non è riuscito a fornire supporto necessario, ciò non significa che era stato mal programmato, ma che l'intervento umano deve esserci sempre.

In una casa del genere, i possibili attaccanti saprebbero tutto di colui che vive nella casa, e proprio per questo motivo che ci vorranno sempre più misure di difesa per contrastare qualsiasi genere di attacco in rete.

Sitografia

https://www2.keil.com/iot

https://it.wikipedia.org/wiki/Security_Information_and_Event_Management

https://questionidiarredamento.it/domotica-il-futuro-e-oggi/

https://www.kaspersky.com/blog/guest-wifi/23843/

https://www.kaspersky.it/resource-center/threats/how-safe-is-your-smart-home

https://www.safety.com/google-home-safety/

https://it.wikipedia.org/wiki/Domotica

https://www.iusinitinere.it/

https://www.rambus.com/iot/smart-home/

https://lamiacasaelettrica.com/domotica-zigbee/

https://yourthings.info/

https://www.domotica.it/2015/05/domotica-e-sicurezza-ai-tempi-di-internet-things/

https://www.agendadigitale.eu/sicurezza/privacy/lintelligenza-artificiale-che-ci-spia-a-casa-quali-rischi-e-soluzioni-per-la-privacy/

https://money.cnn.com/2013/04/08/technology/security/shodan/index.html

https://securitygladiators.com/what-is-shodat/

https://zeusintegrated.com/blog/item/a-brief-history-of-smart-home-automation

https://www.washingtonpost.com/technology/2018/12/20/amazon-alexa-user-receives-audio-recordings-stranger-through-human-error/?noredirect=on

https://homesmarthome100057497w.altervista.org/la-sicurezza-di-una-smart-home

https://www.bluetooth.com/learn-about-bluetooth/topology-options/

Bibliografia

https://www.wired.com/insights/2015/03/internet-things-data-go/

https://www.mdpi.com/2078-2489/7/3/44/htm

https://www.theverge.com/2019/10/21/20924886/alexa-google-home-security-vulnerability-srlabs-phishing-eavesdropping

https://www.agendadigitale.eu/sicurezza/domotica-smart-quello-che-i-consumatori-non-sanno-cosi-ci-giochiamo-privacy-e-sicurezza/

Collegamenti Utili

https://yourthings.info/scorecards/

https://bjoernkarmann.dk/project_alias