Luigi Coppolino
Salvatore D'Antonio
Luigi Romano
Luigi Sgaglione

Università degli Studi di Napoli "Parthenope"

IoT: una tecnologia "disruptive"

IoT: a disruptive technology.

Sommario: L'internet delle cose o "Internet of Things" (IoT) è il nome dato alla crescente tendenza di aggiungere sensing e communication capabilities agli oggetti per la casa/industria per rendere possibile monitoraggio e gestione in remoto. Frigoriferi connessi ad Internet, semafori intelligenti, bracciali ed orologi "smart" sono dispositivi IoT del nostro quotidiano. Studi recenti prevedono la presenza entro il 2020 di circa 17 miliardi di dispositivi IoT connessi alla rete internet. Appare evidente come l'aspetto sicurezza di tale dispositivi assuma un aspetto sempre più rilevante. Infatti, i dispositivi IoT sono affetti dagli stessi problemi di sicurezza degli attuali sistemi connessi in rete (in quanto le tecnologie di base sono fondamentalmente le stesse), ma i rischi connessi sono di gran lunga superiori a quelli dell'attuale rete Internet, perché controllano – e sempre più lo faranno – il mondo fisico (mentre i sistemi informatici tradizionalmente controllavano solo il mondo logico) con importanti ripercussioni anche sulla safety dei sistemi. Il presente articolo fornisce una panoramica sull'IoT, partendo dagli elementi chiave fino ad arrivare ai relativi problemi di sicurezza, fornendo inoltre anche un'evidenza sperimentale di semplici attacchi che possono essere lanciati a distanza contro una vasta classe di cyber-physical systems (CPS), come ad esempio quelli di una Smart Home ZigBee che includa dispositivi di uso generale.

Abstract: The Internet of Things (IoT) is the name given to the growing trend of adding sensing and communication capabilities to objects of emerging home/industry setups, to enable monitoring and remote management. Refrigerators connected to the Internet, intelligent traffic lights, "smart" bracelets and watches are IoT devices of our everyday life. Recent studies forecast the presence in 2020 of about 17 billions of IoT devices connected to the Internet. It is evident that the security implications of such a massive deployment of IoT devices will be a major security concern in the future. Widely speaking, IoT devices are affected by the same security problems of existing networked systems (as the underlying technologies are basically the same), but the risks involved are by far more threatening than those of

the Internet, since they control - and will increasingly do so - the physical world (as opposed to traditional computer systems, that typically control only the logical world). This has a dramatic impact in terms of safety of IoT systems and applications. In this article, we provide an overview of IoT enabling technologies, and analyse the main security issues. The main findings of the study are also supported by experimental evidence, demonstrating how simple yet effective attacks that can be launched remotely against a wide class of Cyber Physical Systems (CPS), and in particular Smart Home ZigBee-based setups that include general purpose devices.

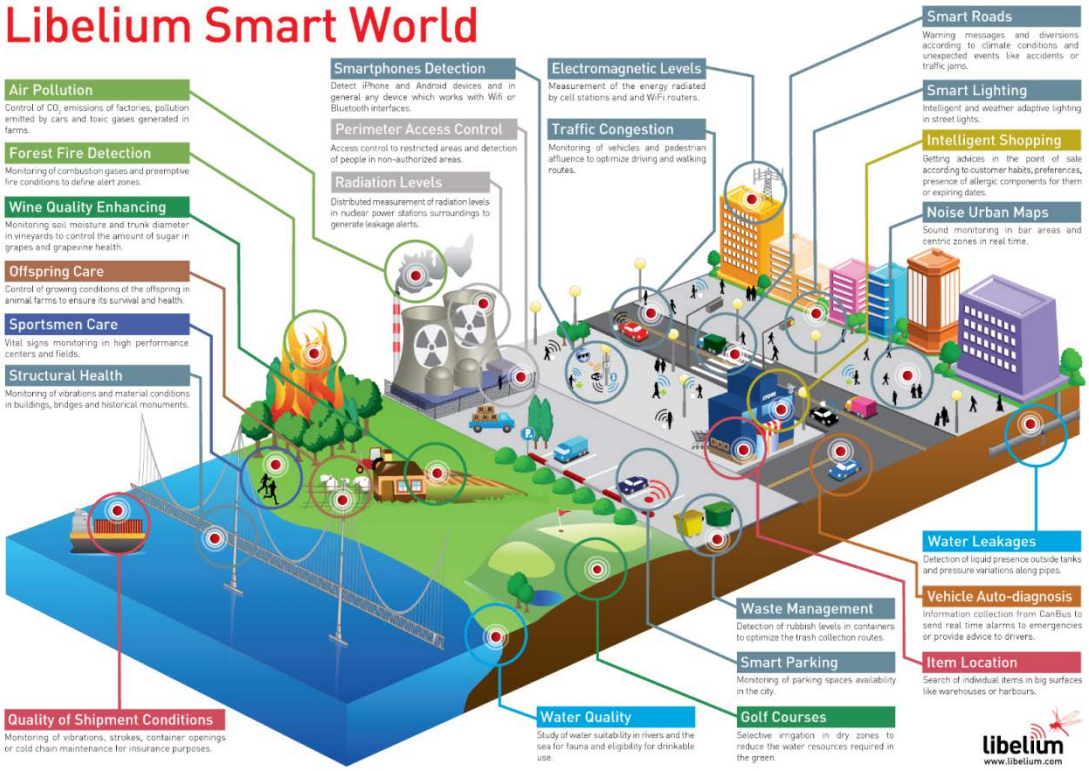
1. IoT - definizione

L'internet delle cose o "Internet of Things" è il nome dato alla crescente tendenza di aggiungere di aggiungere sensing e communication capabilities agli oggetti per la casa/industria per rendere possibile monitoraggio e gestione in remoto.

Quando si parla di "Internet of Things", si fa riferimento quindi a tutti quegli strumenti e applicazioni che permettono non solo alle persone di "dialogare" con le macchine, ma anche agli oggetti di dialogare direttamente tra loro. L'IoT è vista come una possibile evoluzione dell'uso della Rete. Gli oggetti si rendono riconoscibili e acquisiscono intelligenza grazie al fatto di poter comunicare dati su sé stessi, di poter accedere ad informazioni aggregate da parte di altri, e di poter utilizzare software e tecnologie per l'analisi avanzata dei dati.

Frigoriferi connessi ad internet controllabili direttamente dal cellulare, o frigoriferi che ordinano la spesa quando il frigorifero è vuoto (ambiti ancora sperimentali), o semafori intelligenti che diventano verdi quando non passano automobili dal senso di marcia opposto, o bracciali ed orologi "smart" che controllano il battito del cuore, la temperatura e altro, questi sono solo alcuni degli esempi dei dispositivi IoT che sono già entrati a far parte del nostro quotidiano.

Questa tendenza non ha risvolti solo in ambito consumer ma anche in ambito business, infatti l'IoT risulta essere uno dei pillar dell'Industry 4.0 ("Quarta Rivoluzione Industriale"), o in altre parola dell'unione delle competenze e dell'esperienza in ambito industriale con la totale automazione ed interconnessione delle produzioni.



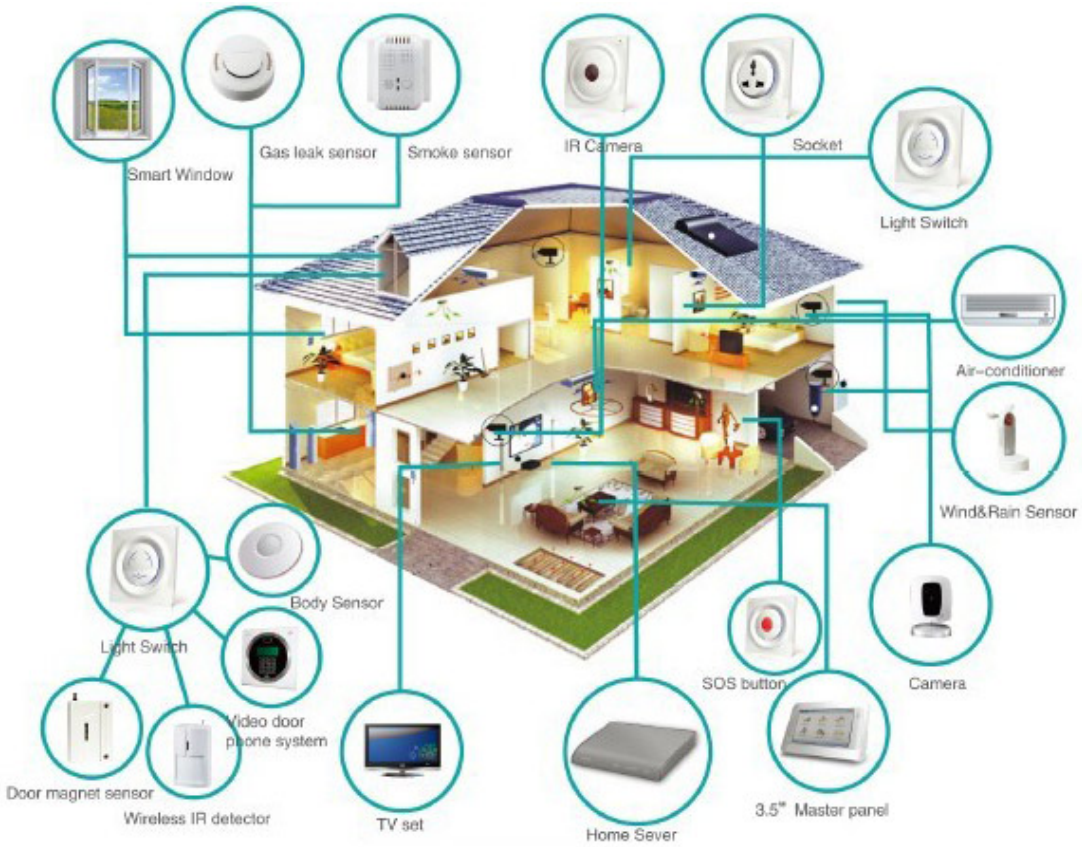
2. IoT domini applicativi

I campi di applicabilità dell'IoT sono molteplici e vanno dalle applicazioni industriali (processi produttivi), alla logistica e all'info-mobilità, fino all'efficienza energetica, all'assistenza remota e alla tutela ambientale.

Tra i principali domini applicativi ed ambiti operativi interessati dalla IoT vengono ad essere annoverati: la domotica (Smart Home) e l'Industrial IoT.

Smart Home - La smart home è, per definizione una casa intelligente, che sfrutta un impianto integrato di tipo domotico per migliorare il comfort, la sicurezza e i consumi di chi vi abita. Il sistema centralizzato della smart home consente agli utenti di gestire diverse funzionalità interne alle mura domestiche, di attivare o disattivare i dispositivi presenti, di ottimizzare i carichi energetici e di creare "scenari" su misura, sulla base delle proprie preferenze e abitudini.

Figura 1. Smart World (http://www.libelium.com/)



IoT industriale porta a vedere l'applicazione dell'IoT in un contesto non-consumer ma business, all'interno del quale macchine intelligenti, dispositivi e persone sono tra di loro collegate. Questa interconnessione dà la possibilità di prendere decisioni in maniera efficiente ed ottimizzata in base all'elaborazione – in maniera sia puntuale che cumulativa - di grandi volumi di dati (Big Data), in modalità sia batch che real-time. Ciò si tradurrà in una rapida evoluzione delle singole fabbriche e delle linee di produzione in generale, costituite da componenti interconnessi tra di loro, che saranno sempre più intelligenti (Industry 4.0). Esempi di dispositivi IoT attualmente utilizzati in tale ambito sono:

- gli Smart Meter. Uno smart meter è uno strumento di monitoraggio e misurazione dei consumi elettrici/gas/acqua. Il suo scopo è quello di valutare ad esempio l'assorbimento di elettricità da parte dell'utente finale. La sua particolarità è quella di poter comunicare in due direzioni: può inviare al gestore le letture dei dati degli apparecchi domestici ma anche essere contattato a distanza dagli operatori delle aziende.
- I Sincrofasori. Essi sono strumenti di monitoraggio in tempo reale della rete elettrica che consentono una stima pressoché diretta dei flussi di potenza nella rete.

Figura 2. Smart Home (http://smarthomeenergy.co.uk/)

Altri esempi di domini applicativi sono: l'industria automobilistica, la biomedica, il monitoraggio in ambito industriale, le reti wireless di sensori, la sorveglianza, le Smart grid e le Smart City, i Sistemi Embedded, e la telematica/telemedicina.

3. IoT - Word things

La crescente diffusione dell'IoT ha portato alla ribalta tutta una serie di termini che stanno entrando a far parte del nostro quotidiano di seguito una breve lista dei termini più importanti:

- Things as a Service (TaaS) - Sistema che gestisce la fornitura dei servizi in ambiente cloud
- Internet dei veicoli
  - V2V – Vehicle to Vehicle
  - V2P – Vehicle to Person
  - V2I – Vehicle to Infrastructure
- Body-area Network (BAN) - reti che interconnettono dispositivi indossabili
- Bring Your Own Device (BYOD) si è evoluto in BYOWearable (BYOW)
- Social Web of Thing (SWoT)
  - Permette agli utenti di gestire, accedere, condividere ed integrare gli smart objects con i Social Network Site (SNS)
- Crowdsensing
  - È la raccolta di informazioni su un dato ambiente usando sensori di cui sono dotati gli smartphone e gli altri dispositivi usati dalle persone che sono presenti in tale ambiente
- Internet of Everything (IoE)
  - Caratterizzato dal passaggio Machine To Machine (M2M) ☐ Machine To Person (M2P)

4. Il mercato IoT

Il mercato dell'IoT è in vertiginosa crescita come dimostrato da una recente ricerca degli analisti di Gartner, la quale ha stimato che saranno 4,9 miliardi gli oggetti connessi ad internet nel 2015, in crescita del 30% sul 2014, con una tendenza in continua crescita destinata a raggiungere i venticinque miliardi entro il 2020 {4}.

In Tabella 1 sono riportati ad esempio il numero di dispositivi IoT installati dal 2013 ad oggi e le previsioni per il 2020.

Category	2013	2014	2015	2020
Automotive	96.0	189.6	372.3	3,511.1
Consumer	1,842.1	2,244.5	2.874.9	13,172.5
Generic Business	395.2	479.4	623.9	5,158.6
Vertical Business	698.7	836.5	1,009.4	3,164.4
Grand Total	**3,032.0**	**3,750.0**	**4,880.6**	**25,006.6**

Nella Tabella 2 è riportato un elenco di paesi con il relativo numero di dispositivi IoT on-line per 100 abitanti cosi come pubblicata dall'OCSE nel 2015.

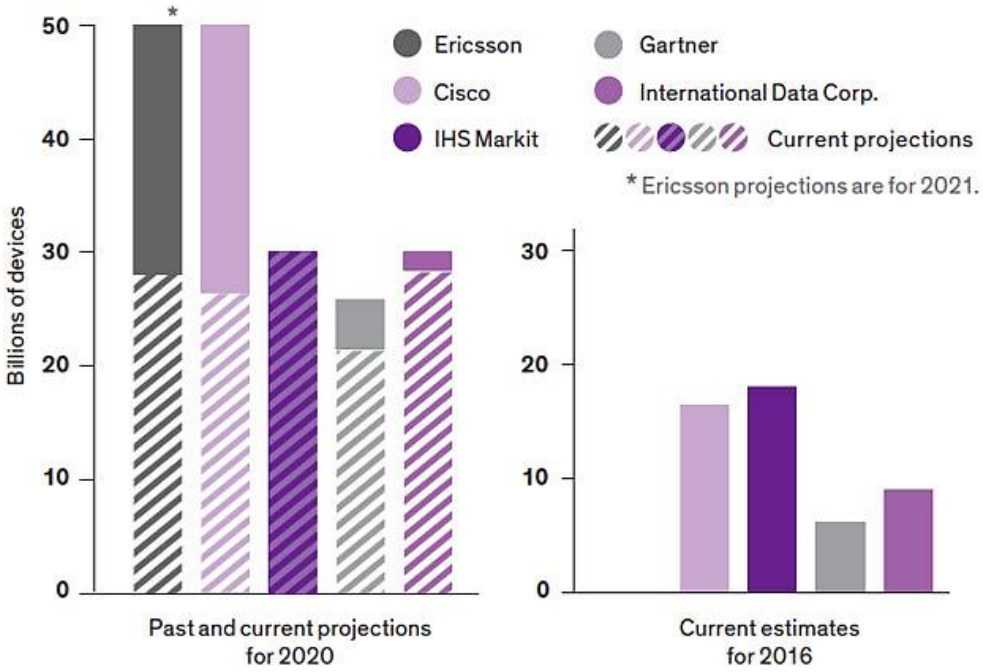
Un recente studio commissionato dalla European Commission prevede che il mercato dell'IoT all'interno dell'EU acquisterà un valore superiore al trilione di euro nel 2020.

Tutte queste stime sono state largamente diffuse e pubblicizzate in questi anni, ma quello che si è capito è che esse sono troppo ottimistiche in termini di numeri, infatti di recente tali numeri sono stati ridimensionati Figura 3 e il vero totale di dispositivi connessi è tra i 6,4 miliardi stimati da Gartner (escludendo smartphone, tablet e computer) e i 17,6 miliardi stimati da IHS Markit (includendo i dispositivi elencati prima)

Rank	Country	Devices online	Relative size
1	Korea	37.9	
2	Denmark	32.7	
3	Switzerland	29.0	
4	United States	24.9	
5	Netherlands	24.7	
6	Germany	22.4	
7	Sweden	21.9	
8	Spain	19.9	
9	France	17.6	
10	Portugal	16.2	
11	Belgium	15.6	
12	United Kingdom	13.0	
13	Canada	11.6	
14	Italy	10.2	
15	Brazil	9.2	
16	Japan	8.2	
17	Australia	7.9	
18	Mexico	6.8	
19	Poland	6.3	
20	China	6.2	
21	Colombia	6.1	
22	Russia	4.9	
23	Turkey	2.3	
24	India	0.6	

Tabella 1. Dispositivi IoT installati (milioni) Source: Gartner (November 2014)

Tabella 2. Dispositivi IoT online ogni 100 abitanti



In ogni caso, pur rivalutando al ribasso le stime fatte, appare evidente come la diffusione dei dispositivi IoT e il relativo interesse economico in tale campo sono destinati ad una crescita esponenziale, che presto sarà parte integrante del nostro quotidiano.
La situazione italiana è stata studiata a fondo dall'Osservatorio Internet of Things della School of Management del Politecnico di Milano. L'Italia occupa una posizione intermedia rispetto agli altri paesi, raggiungendo un valore di mercato di circa 2 miliardi di euro, con una crescita del 30% rispetto al 2014, spinta sia dalle applicazioni che sfruttano la connettività cellulare che da quelle che utilizzano altre tecnologie come Wireless M-Bus o Bluetooth Low Energy.

Figura 3. IoT, stime recenti e passate (http://spectrum.ieee.org/telecom/internet/the-internet-of-fewer-things)

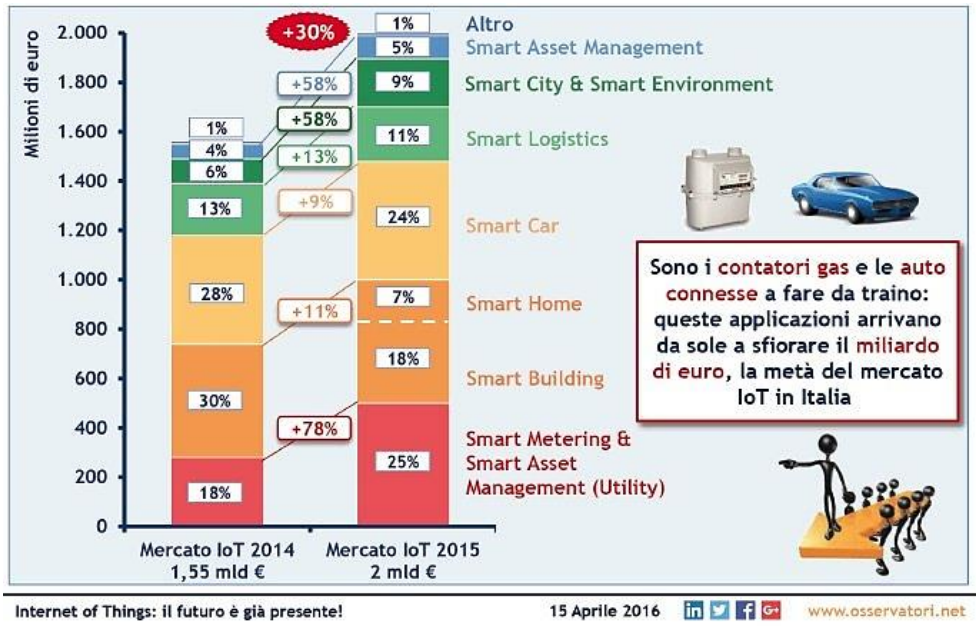
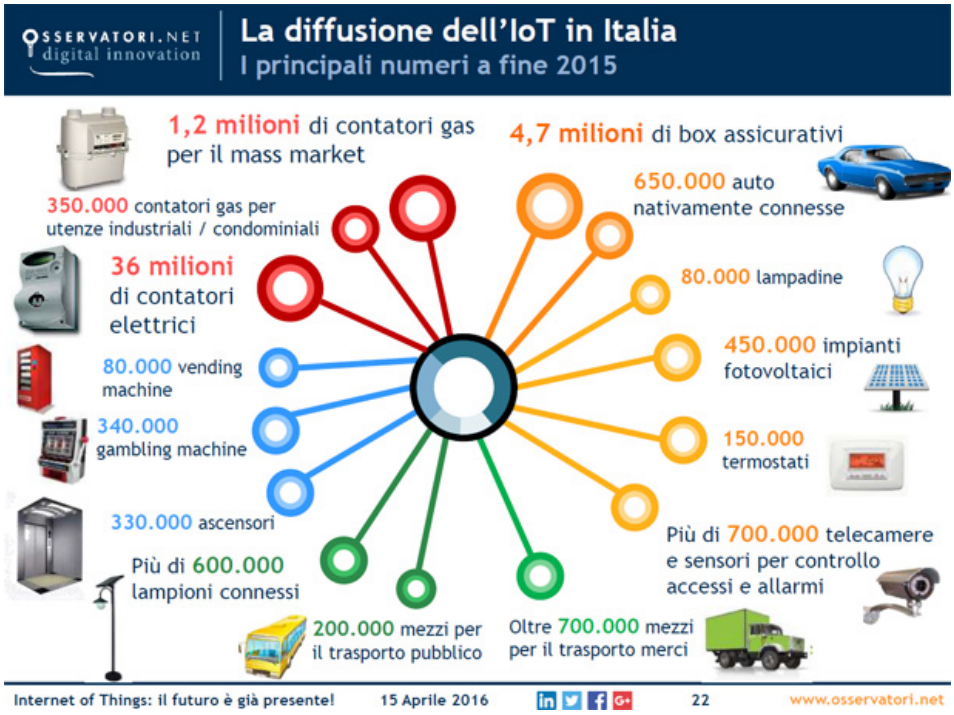


Figura 4. IoT mercato in Italia

In Figura 5 è riportata la diffusione dell'IoT in Italia suddivisa per segmenti, il principale è costituto dai contatori intelligenti per la misura dei consumi (Smart Metering) e di Smart Asset Management nelle utility. Segue la Smart Car, con 5,3 milioni di auto connesse in Italia, un settimo del totale parco circolante. A seguire troviamo le soluzioni di Smart Building (videosorveglianza e la gestione degli impianti fotovoltaici), quelle di Smart Logistics (gestione di flotte aziendali e antifurti satellitari), Smart City & Smart Environment e poi la Smart Home (7%), soprattutto con applicazioni di antintrusione e termostati controllati a distanza.



5. IoT and COTS

Una cosa da tenere in considerazione quando si parla di IoT è il fatto che qualsiasi dispositivo elettronico corredato da opportune tecnologie abilitanti può entrare a far parte del mondo IoT.

Un'importante definizione dell'IoT è la seguente: "The Internet of Things (IoT) is the interconnection of **uniquely identifiable embedded computing devices** within the existing **Internet infrastructure**." [1]

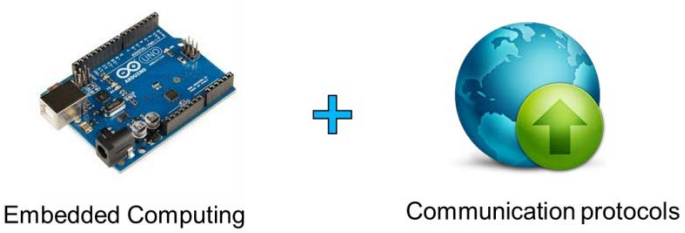


Figura 5. Diffusione dell'IoT in Italia

Figura 6. Tecnologie abilitanti di un dispositivo IoT

Si può ben comprendere come tale peculiarità apra al mondo IoT l'utilizzo dei dispositivi COTS (Commercial Off The Shelf) con i conseguenti problemi di sicurezza che affliggono tale dominio.

La valutazione dei "Commercial-Off-Shelf" software è un "Hot Topic" per le applicazioni mission and safety critical. I componenti COTS sono sempre più utilizzati nel controllo/monitoraggio (e quindi IoT) delle applicazioni critiche, sia per motivi economici (acquistare un prodotto disponibile sul mercato è più economico di svilupparne uno ex novo) sia per ridurre il time-to-market. Tuttavia, nella maggior parte dei casi, questi componenti non sono specificamente progettati e sviluppati per operazioni "robuste", ciò comporta non pochi problemi quando si vuole ottenere un profilo di funzionamento affidabile.

La mancanza di garanzie in termini di affidabilità non è più accettabile per le applicazioni safety-critical. Pertanto, laddove questi componenti sono stati utilizzati per la realizzazione di applicazioni safety-critical, si rende necessaria una valutazione formale e ben strutturata.

Considerata la definizione data in [1] si ha che gli elementi costituenti un dispositivo IoT sono:

1. Dispositivo Embedded (COTS CPU)
2. COTS Software
3. Protocollo di comunicazione

a. COTS CPU

In termini di unità vendute, i processori per PC raggiungono solo il 6% del mercato mondiale, il restante 94% - 5 miliardi di chip – è costituito da embedded microprocessors (Fonte: Computerworld).

Ogni produttore di circuiti integrati e/o dispositivi OEM ora produce componenti e soluzioni per IoT, indossabili e alimentati a batteria, ciò si traduce in una sfida tra prestazioni e potenza che sta portando alla necessità di nuovi tipi di processori a basso consumo.

b. COTS Software

Sono software nati con il principale requisito di essere poco esosi in termini di risorse hardware, energetiche ed economiche. Esempi sono:

- Embedded Operating System: Tiny OS, Contiki, Mantis, LiteOS, FreeRTOS, ARM mbed …
- Tools: Busybox, IoT Toolkit …
- Middleware: IoTSyS, OpenIoT …

c. Protocollo di comunicazione

In via generale tutte le tecnologie che permettono una comunicazione a basso consumo possono essere annoverate tra le tecnologie abilitanti dell'IoT. Di seguito una breve carrellata dei protocolli di comunicazione più utilizzati.

I. Bluetooth

Bluetooth [2] è una tecnologia di comunicazione a corto raggio che è diventata molto importante nel campo dell'informatica e in molti mercati di prodotti di consumo. Essa è la tecnologia chiave per prodotti indossabili (wearable). In particolare una nuova versione di tale protocollo Bluetooth Low-Energy (BLE) [3]- o Bluetooth Smart - è diventata uno dei punti di riferimento per le applicazioni IoT. Tale versione offre un range di trasmissione simile a quello della precedente ma con un consumo di energia notevolmente ridotto (peculiarità chiave in ambiente IoT).

II. ZigBee

ZigBee [4] è una specifica per un insieme di protocolli che utilizzano piccole antenne a bassa potenza per creare una PAN (Personal Area Network) basata sullo standard IEEE 802.15.4. La prima versione è stata ratificata a fine 2004, quando molte reti wireless venivano progettate solo per specifiche applicazioni. Ciò ha portato all'implementazione di profili per ogni tipo di settore (home automation, building automation, controlli industriali, sicurezza, medicina, ecc.), consentendo ai produttori di includere solo determinate funzionalità nei loro dispositivi. La ZigBee Alliance ha annunciato l'unificazione dei suoi standard wireless in ZigBee 3.0. Questa nuova versione elimina tutti i problemi che ne hanno rallentato la diffusione, offrendo la completa interoperabilità tra un'ampia varietà di dispositivi che ora possono funzionare insieme e interagire tra loro all'interno dell'abitazione. ZigBee 3.0 semplifica inoltre la realizzazione di applicazioni e servizi per la smart home e la Internet of Things da parte degli sviluppatori.

III. Z-Wave

Z-Wave [5] venne inizialmente sviluppato nel 2001 dalla startup danese Zen-Sys , con il tempo è diventato uno standard internazionale per la realizzazione di reti mesh interoperabili e a bassa potenza. Il protocollo supporta la comunicazione bidirezionale tra i dispositivi abilitati, permettendo a prodotti di costruttori diversi di funzionare assieme in modo trasparente. Z-Wave utilizza un flusso di dati ridotto per scelta progettuale. Questa scelta permette di ottenere una comunicazione a bassa latenza con una velocità di trasmissione dei dati fino a 100 kbps. Z-Wave fa dell'interoperabilità dei prodotti di diversi costruttori uno dei propri punti di forza e persegue tale obiettivo anche tramite un processo di certificazione dei dispositivi.

IV. 6LoWPAN

6LoWPAN [6] è l'acronimo di IPv6 over Low power Wireless Personal Area Networks. Il concetto alla base di 6LoWPAN nasce dall'idea che il protocollo Internet potrebbe e dovrebbe essere applicato anche a dispositivi più piccoli, e che i dispositivi a bassa potenza con capacità di elaborazione limitate dovrebbero essere in grado di partecipare alla Internet of Things. Il gruppo 6LoWPAN ha definito meccanismi di incapsulamento e compressione che

permettono ai pacchetti IPv6 di essere inviati e ricevuti su reti IEEE 802.15.4.

V. Thread

Thread [7] è un nuovo protocollo basato su reti IPv6 mirato alla home automation. Esso nasce come evoluzione di 6LoWPAN ed è quindi basato sul protocollo IEEE 802.15.4.

VI. WiFi

WiFi è spesso una scelta ovvia per molti sviluppatori, soprattutto data la pervasività del WiFi all'interno dell'ambiente domestico. Lo standard WiFi più comunemente usato è lo standard 802.11n, che offre un throughput di centinaia di megabit al secondo, ma che potrebbe essere troppo esoso in termini di energia consumata in un contesto IoT.

VII. Cellular

Qualsiasi applicazione IoT che richiede il funzionamento su lunghe distanze può usufruire della capacità di comunicazione delle reti cellulari GSM/3G/4G. Tali reti però richiedono un consumo energetico molto elevato e pertanto sono valide alternative solo per sensori che inviano basse quantità di dati su Internet.

VIII. NFC

Near Field Communication (NFC) [8] è una tecnologia che fornisce connettività wireless (RF) bidirezionale a corto raggio (fino a un massimo di 10 cm). Contrariamente ai più semplici dispositivi RFID, NFC permette una comunicazione bidirezionale: quando due apparecchi NFC (lo initiator e il target) vengono accostati entro un raggio di 4 cm, viene creata una rete peer-to-peer tra i due ed entrambi possono inviare e ricevere informazioni. La tecnologia NFC opera alla frequenza di 13,56 MHz e può raggiungere una velocità di trasmissione massima di 424 kbit/s.

IX. Beacon/iBeacons

I termini iBeacon e Beacon [9] sono spesso usati come sinonimi. iBeacon è il nome della tecnologia standard di Apple, che permette alle App Mobile (in esecuzione sia su dispositivi iOS che Android), di mettersi in ascolto di segnali provenienti da Beacon fisici e di reagire in conseguenza. In sostanza, la tecnologia iBeacon permette alle App di capire la loro posizione su scala micro-locale e fornire contenuti iper-contestuale per gli utenti in base alla posizione. La tecnologia di comunicazione sottostante è Bluetooth Low Energy.

Altre tecnologie degne di nota sono: Wireless M-Bus, MQTT, WeMo, Sigfox, Neul, e LoRaWAN

6. IoT – aspetti di privacy, safety e sicurezza

Lo studio "Disruptive Civil Technologies Six Technologies with Potential Impacts on US Interests out to 2025" effettuato dal National Intelligence Council [10], classifica tra le prime sei tecnologie "disruptive" l'Internet Of Things. Dove per tecnologia "disruptive" si intende una tecnologia con il potenziale di causare una notevole - anche se temporanea - degradazione o miglioramento di uno degli elementi del potere nazionale degli Stati Uniti (politico, militare, economico, o di coesione sociale).

La Commissione Europea (EC) definisce una infrastruttura come critica quando: "it is so vital that, if it is disrupted or destroyed, this would have a serious impact on the health, safety, security or economic well-being of Citizens or the effective functioning of governments."

Le similitudini tra le due definizioni sono evidenti il che porta classificare l'IoT stessa come una infrastruttura critica.

Gli individui, le imprese e i governi non sono preparati per un possibile futuro in cui i nodi di Internet risiedono in ogni cosa del quotidiano come ad esempio nei contenitori del cibo, nei mobili, nei documenti cartacei, e altro ancora. Gli sviluppi odierni indicano quali saranno le future opportunità e i rischi che si presenteranno quando le persone potranno controllare a distanza, individuare e monitorare gli oggetti del quotidiano.

Pertanto la sicurezza dell'IoT assume sempre più importanza e gli oggetti dell'IoT saranno soggetti agli stessi problemi di sicurezza dagli attuali sistemi connessi in rete (in quanto le tecnologie di base sono fondamentalmente le stesse), ma i rischi connessi saranno di gran lunga superiori a quelli dell'attuale rete Internet, per due motivi fondamentali:

- Hanno una diffusione capillare (che è destinata ad aumentare)
- Controllano – e sempre più lo faranno – il mondo fisico (mentre i sistemi informatici tradizionalmente controllavano solo il mondo logico)

Inoltre, le minacce alla privacy sono enormi, così come la possibilità di controllo sociale e di manipolazione politica. In un articolo pubblicato su Forbes nel gennaio 2014 [11] sono stati elencanti molti apparecchi collegati a Internet che possono già "spiare le persone nelle loro case", tra cui televisori, elettrodomestici da cucina, macchine fotografiche, e termostati. I Sistemi x-by-wire del settore automotive (dispositivi controllati dal computer in automobili come i freni, motore, serrature, clacson, e il cruscotto) hanno dimostrato di essere vulnerabile agli attacchi che hanno accesso alla rete di bordo.

Infine, un aspetto importante (forse il principale) della sicurezza dell'IoT è che in questo dominio i problemi di security possono avere effetti diretti sulla safety del sistema. In tutti gli oggetti dell'IoT, la sicurezza è quasi sempre inscindibile dalla safety, un'interferenza (accidentale o dolosa) con i comandi di un pacemaker, di una

macchina, o di un reattore nucleare rappresenta una minaccia per la vita umana.

Molte pertanto sono state le preoccupazioni sollevate sul fatto che l'IoT si stia sviluppando molto (se non troppo) rapidamente, senza adeguata considerazione per le questioni di sicurezza coinvolte e i cambi regolamentari che potrebbero essere necessari. Questa percezione di (in)sicurezza è pervasiva: secondo il Business Insider Intelligence Survey condotto nell'ultimo quadrimestre del 2014, il 39% degli intervistati ha sostenuto che la sicurezza è il problema più pressante nell'adozione dell'IoT [12].

In risposta alle crescenti preoccupazioni in termini di sicurezza, il 23 settembre 2015 è stato lanciato l'Internet of Things Security Foundation (IoTSF). IoTSF ha la missione di garantire la sicurezza dell'IoT attraverso la promozione di conoscenze e "best practice". I membri fondatori di tale fondazione sono fornitori di tecnologia ICT varie e società di telecomunicazioni, tra cui si annoverano BT, Vodafone, e Imagination Technologies [13].

7. IoT – esempi di problemi di sicurezza riscontrati in contesti reali

Molti sono gli esempi di problemi di sicurezza cui sono soggetti gli odierni dispositivi per l'IoT, uno dei più recenti è il DDoS Mirai del 21/10/2016, ovvero un Distributed Denial-of-Service verso i server DNS di provider americano (Dyn) che ha causato l'interruzione di internet per diverse ore.

Mirai è un malware progettato con lo scopo di prendere possesso dei dispositivi connessi alla rete con lo scopo di creare botnet di attacco. I suoi obiettivi principali sono i dispositivi elettronici di consumo, come telecamere casalinghe e router. Esso scansiona continuamente la rete cercando dispositivi IoT e cerca di infettarli utilizzando una lista di nomi utente e password impostati di default dalle aziende produttrici nei loro dispositivi o nei tool da esse installati sulla telecamera come ad esempio il software BusyBox, utilizzato per permette di eseguire diversi strumenti Unix in una varietà di ambienti POSIX che dispongono di risorse limitate. A fine settembre 2016, l'hacker responsabile della creazione del malware Mirai, ne ha rilasciato il codice sorgente, consentendo a «chiunque» di costruire in modo efficace il proprio esercito di attacco (botnet) usando Mirai.

La botnet utilizzata nell'attacco del 21/10/2106 era costituita da dispositivi IoT compromessi - principalmente Digital Video Recording (DVR) e telecamere IP – realizzati con hardware di una società hi-tech cinese chiamata XiongMai Technologies. La vulnerabilità sfruttata è il fatto che tali dispositivi erano (e lo sono ancora) dotati di una combinazione username, password di default e il software a corredo non obbliga l'utente a cambiare almeno la password. Questo tipo di vulnerabilità purtroppo è largamente diffusa come testimoniato da una ricerca effettuata da Flashpoint in cui Internet è stata scansionata alla ricerca di dispositivi che presentassero tale vulnerabilità,

identificandone 515000. Lo strumento utilizzato per identificare tali dispositivi è stato un noto motore di ricerca per gli oggetti dell'IoT "Shodan" [14]. Da notare come tale motore di ricerca possa anche essere utilizzato da un attaccante per individuare nodi che potenzialmente possono essere candidati alla creazione di una botnet.

Altri esempi di problemi di sicurezza reali sono:

- Alcuni ricercatori hanno dimostrato per il magazine WIRED come sia possibile hackerare da remoto una Jeep Cherockee del 2014 e disabilitare trasmissione e freni
- Il frigo Samsung RF28HMELBSR (3599 US$) progettato per sincronizzarsi via Wi-Fi con il Google Calendar dell'utente, presenta vulnerabilità che consentono ad un attaccante di rubare le credenziali dell'account Google
- Mattel ha aggiunto la connettività Wi-Fi alla sua «Hello Barbie» per consentire conversazioni con un'intelligenza artificiale in real time. La connessione all'app smartphone della bambola è vulnerabile allo spoofing e all'intercettazione di tutto l'audio registrato sulla stessa
- Baby monitor, nonostante il rischio raccapricciante di qualcuno che spia i bambini, rimangono insicuri: uno studio condotto dalla società di sicurezza Rapid7, in cui si testavano 9 baby monitor commerciali, ha scoperto che tutti e nove risultavano relativamente facili da hackerare
- Alcuni studenti della University of Alabama hanno violato il pacemaker impiantato nel paziente robot «iStana» utilizzato per addestrare gli studenti di medicina e teoricamente lo hanno ucciso.

8. IoT – esempi di problemi di sicurezza riscontrati in contesti reali

Visti i tre componenti chiave dei dispositivi IoT e le minacce reali cui essi sono sottoposti viene naturale chiedersi quale sia l'anello debole dal punto di vista della sicurezza.

Per quanto riguarda Il livello di sicurezza dei processori embedded, esso è già molto elevato ed è in aumento: un gruppo di aziende (tra cui ARM, Intercede, Solacia e Symantec) ha sviluppato Open Trust Protocol (OTrP). Esso fornisce un'architettura e una gestione del codice sicura per proteggere i dispositivi collegati ed utilizza tecnologie impiegate nel settore bancario e per la gestione di dati sensibili su smartphone e tablet. ARM si è mossa in tal senso creando nei suoi processori la Trust Zone che fornisce sia un dominio sicuro che uno insicuro per l'esecuzione delle istruzioni.

Lo stesso non si può dire né del software, né delle tecnologie di comunicazione. Sono la parte più vulnerabile, in quanto progettate avendo come requisiti principali il basso costo e il basso consumo (vedi DDOS Mirai).

9. I nostri esperimenti

Abbiamo progettato degli attacchi (incredibilmente semplici) che possono essere lanciati a distanza contro una vasta classe di cyber-physical systems (CPS), come ad esempio quelli di una Smart Home ZigBee che includa dispositivi di uso generale (quali COTS di tipo ricreativo di larghissima diffusione). Abbiamo lanciato gli attacchi, dimostrandone la fattibilità e la pericolosità.
Due diversi allestimenti:

- Ambiente emulato → banco di prova di tipo commerciale che viene regolarmente utilizzato da un importante gestore di rete per la convalida delle configurazioni che devono andare in esercizio
- Hardware prototipale → rappresentativo di una vasta gamma di prodotti.

a. Rete ZigBee

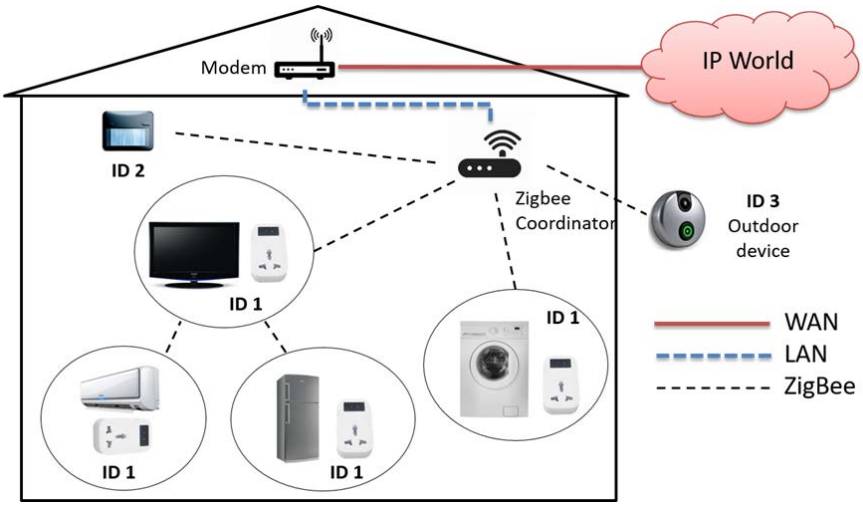


Figura 7. Smart Home ZigBee tradizionale [ZigBee Plug (ID1), ZigBee Sensore di comfort (ID2), ZigBee sensore esterno (ID3)]

In Figura 7 è riportata la tipica configurazione di una rete ZigBee:

- I dispositivi Smart Home usano il protocollo ZigBee per raggiungere il coordinatore della rete
- Il coordinatore ZigBee funge da gateway verso il mondo IP, ed è l'unico nodo dotato di una connessione Internet.

In Figura 8 invece è riportato lo scenario emergente delle Smart Home ZigBee, dove nuovi dispositivi multipurpose vengono ad essere connessi alla rete ZigBee. Tali dispositivi sono dispositivi che possono avere scopi molteplici oltre quello di permettere la comunicazione sulla rete ZigBee, anzi nella maggior parte dei casi la comunicazione ZigBee è solo una delle tante disponibili come ad esempio nel caso del tablet "Geek Land tablet GK-ZIG-001" o del "Zigbee Android 4.0 Wall

Mounted Tablet for Home Automation GK-EKG-001" dotati di diverse connessioni tra cui ZigBee, WiFi e 3G. Con l'uso di tali dispositivi il router ZigBee cessa di essere l'unico punto di accesso alla rete Internet esponendo cosi la Smart Home a problemi di sicurezza che non erano stati considerati.

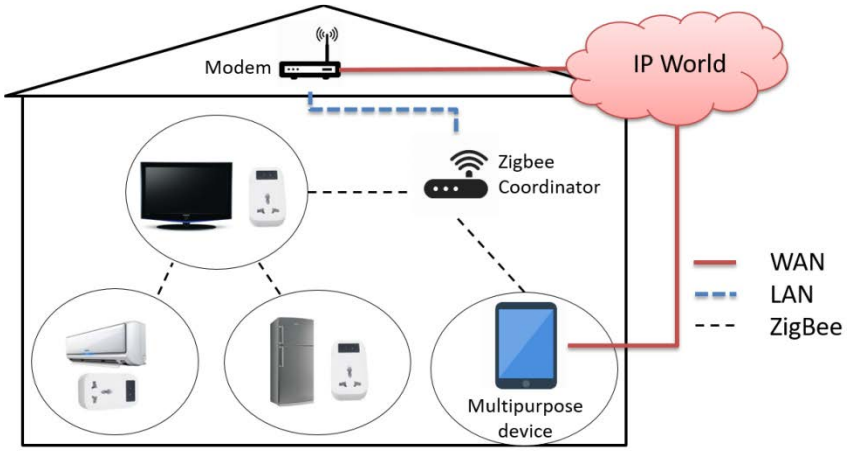


Figura 8. Scenario emergente di una Smart Home ZigBee

b. Protocollo ZigBee

Molte brevemente descriveremo alcune caratteriste del protocollo ZigBee.
ZigBee nasce per applicazioni che richiedono: basso consumo di potenza, alta densità di nodi nella rete, bassi costi, transfer rate non elevato e semplicità nella creazione di una rete.
All'interno di una rete ZigBee possono essere identificati i seguenti nodi:

- ZigBee Coordinator, costituisce la radice di una rete ZigBee, esso è in grado di memorizzare informazioni riguardo alla sua rete e può gestire le chiavi di sicurezza. Ci può essere un solo "Coordinator" in ogni rete
- ZigBee Router, sono dispositivi intermedi che trasmettono i dati da e verso altri dispositivi
- ZigBee End Device, posso dialogare solo con il nodo padre (Coordinator o Router), non possono trasmettere dati provenienti da altri dispositivi e sono i nodi che richiedono il minor quantitativo di risorse.

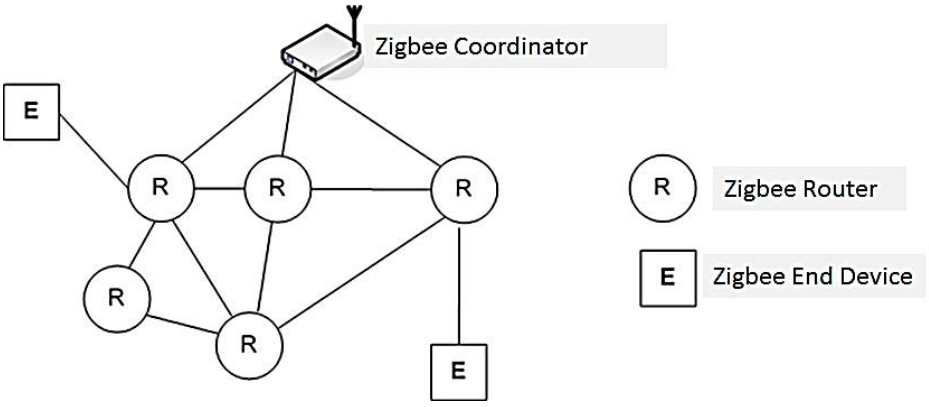


Figura 9. Rappresentazione di una rete ZigBee

Il protocollo ZigBee è caratterizzato da un algoritmo di routing adattativo AODV (Ad-hoc On-Demand Distance Vector) dove la scelta del percorso può dipendere sia dalla potenza trasmissiva del nodo da usare per raggiungere il coordinatore sia dal rapporto segnale/rumore nel percorso.

c. Attacco Sinkhole

Uno degli attacchi da noi implementato è l'attacco Sinkhole.
Esso si basa sul presupposto che ci sia un nodo maligno che diffonde informazioni false - direttamente o indirettamente – sulle sue capacità di routing, che inducono gli altri nodi a pensare che il nodo maligno abbia il miglior percorso verso la stazione base. Il traffico dei nodi "vicini" viene deviato al nodo maligno che può operare diverse azioni dannose sui pacchetti che lo attraversano:

- Leggere i dati (violazione della confidentiality)
- Modificare il contenuto dei dati (violazione dell'integrity)
- Gettare via i dati (violazione di availability)

Si tratta di un attacco molto pericoloso, esso colpisce un'intera sezione di una rete, non solo un singolo nodo, ed è molto difficile da rilevare in quanto il nodo maligno può mascherare la sua presenza continuando a funzionare in un modo apparentemente normale.

Esso inoltre può essere utilizzato come punto di partenza per una serie di altri attacchi ed è abbastanza comune nelle reti di sensori wireless.

d. Setup sperimentale emulato

In Figura 10 è mostrato l'ambiente emulato che è stato realizzato per i nostri test.

Abbiamo utilizzato un ambiente di tipo commerciale emulato, ovvero "Hybrid Environment for Development and Validation" (HEDVa). Questo ambiente è utilizzato da IEC (Israel Electric Corporation, https://www.iec.co.il/en/ir/pages/default.aspx) per la convalida dei loro sistemi di controllo industriale (ICS).

Il testbed è costituito da 15 dispositivi, ogni dispositivo si accende e si spegne in modo casuale (simulando in tal modo la connessione e disconnessione dalla rete domestica) e una volta collegato, invia un pacchetto di dati ogni 30 secondi al Coordinatore (120 pacchetti / ora).

Solo l'attaccante è sempre collegato alla rete, abbiamo eseguito l'esperimento per 24 ore, con l'attacco lanciato dopo 7 ore.

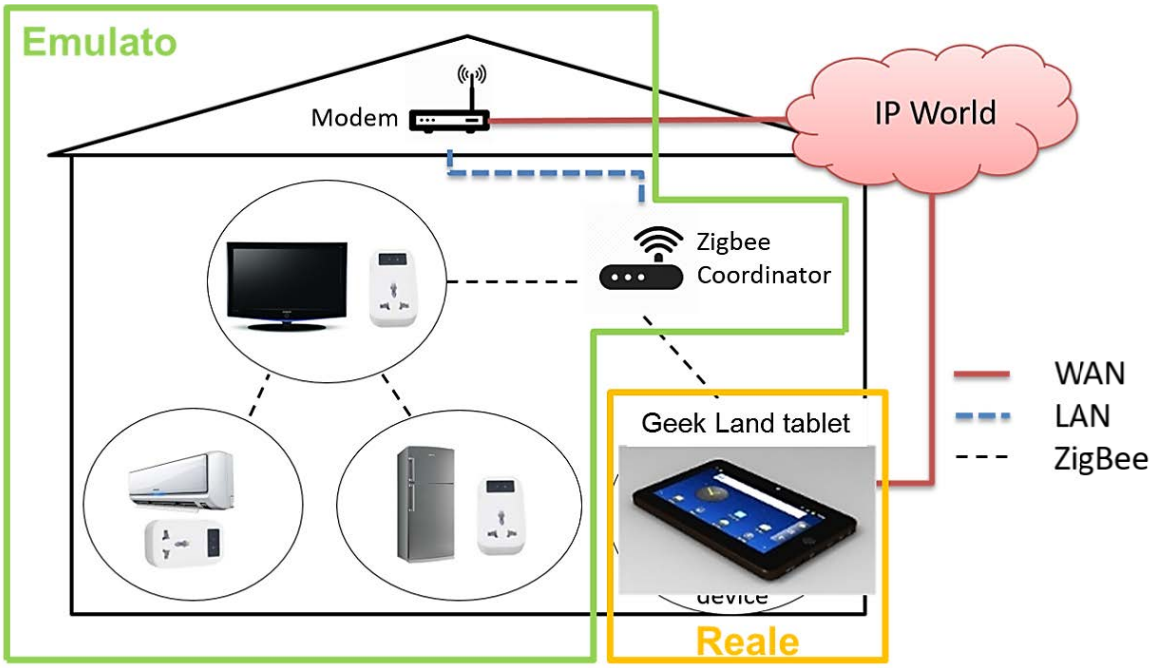


Figura 10. Ambiente emulato

I. Hacking ambiente emulato

Di seguito vengono descritti i passi necessari per implementare un attacco di tipo Sinkhole sul nostro ambiente emulato.

1. Si parte da uno scenario tipico: una rete ZigBee, tra cui alcuni dispositivi ZigBee + 1 coordinatore
2. Un dispositivo multiuso (in particolare: un tablet Android) si unisce legalmente alla rete (il tablet Android ha una connessione diretta a Internet)
3. Il dispositivo Android è violato per mezzo di uno specifico malware
4. Il malware prende il controllo del dispositivo Android, e lo utilizza per lanciare un attacco Sinkhole alla rete domestica ZigBee
5. Il dispositivo Android è in grado di leggere / cancellare / modificare i pacchetti intercettati

Attività chiave di tale attacco sono:

1. Prendere il controllo (totale) del dispositivo Android
   a. Ottenuto mediante l'utilizzo di una variante del malware Backdoor.AndroidOS.Obad.a («the most sophisticated mobile trojan to date», Kaspersky Lab)
2. Modificare la Potenza trasmissiva del Chip ZigBee
   a. Questo può essere fatto andando a cambiare uno dei parametri di configurazione del chip ZigBee (Texas Instrument's CC2530) equipaggiato sul tablet
      1. Code excerpt:
      2. uint8 value = 0xF5;
      3. MAC MlmeSetReq(MAC PHY TRANSMIT POWER, &value);

La modifica della potenza di trasmissione fa sì che gli altri nodi vedano il nodo malevolo come il miglior percorso verso il coordinator e pertanto esso sarà utilizzato come percorso preferenziale.

II. Risultati sperimentali

Abbiamo monitorato la percentuale di nodi attivi (cioè collegati alla rete domestica) che utilizzano il dispositivo dannoso come gateway Figura 11. L'attacco ha successo: il 70 +% dei dispositivi è ingannato dall'attaccante (numero esatto è dipendente dall'installazione). Maggiori dettagli possono essere trovati qui [15].

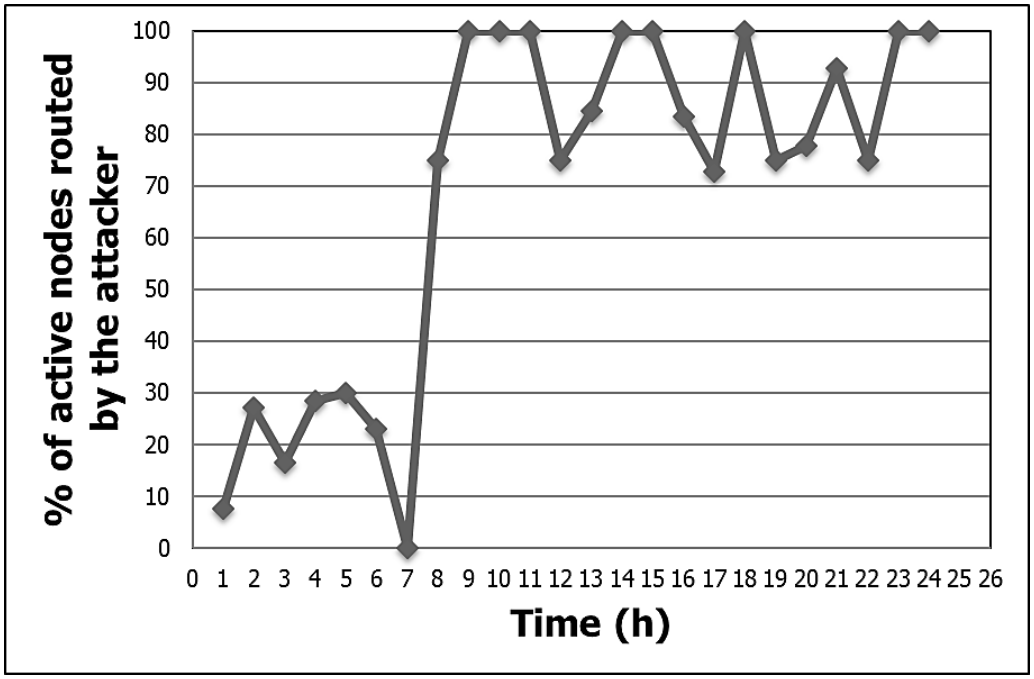


Figura 11. Hacking ambiente emulato

a. Setup sperimentale prototipale

In Figura 12 è mostrato l'ambiente prototipale che è stato realizzato per i nostri test, in cui i singoli dispositivi ZigBee sono stati sostituiti da una opportuna configurazione hardware di tipo prototipale dando vita alla configurazione mostrata in Figura 13.

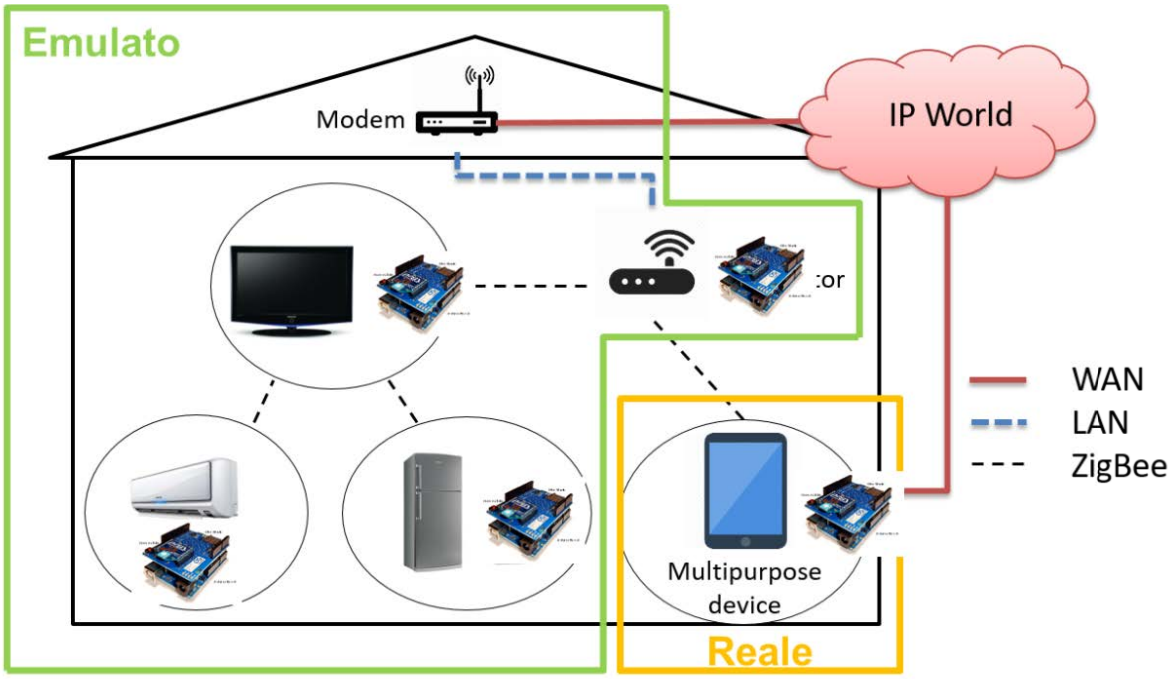


Figura 12. Ambiente prototipale

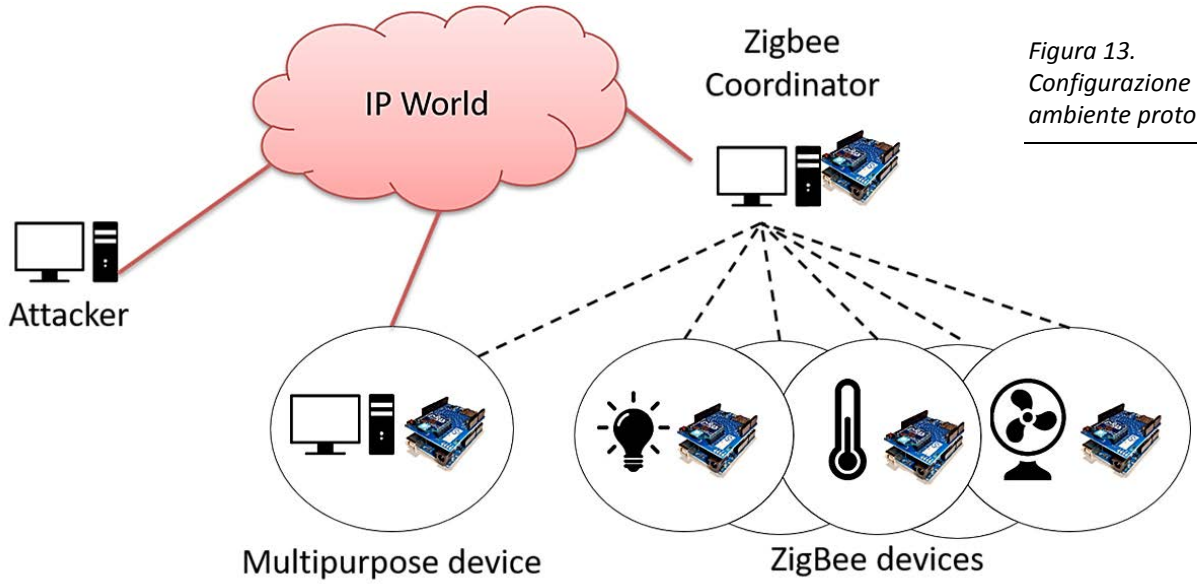


Figura 13. Configurazione ambiente prototipale

La configurazione hardware che abilità alla connessione ZigBee (mostrata in) è stata realizzata usando i seguenti componenti:

- Arduino - board prototipale
- Xbee Zigbee module – permette la comunicazione mediante il protocollo ZibBee
- ZigBee Shield – adattatore Arduino ☐ Xbee

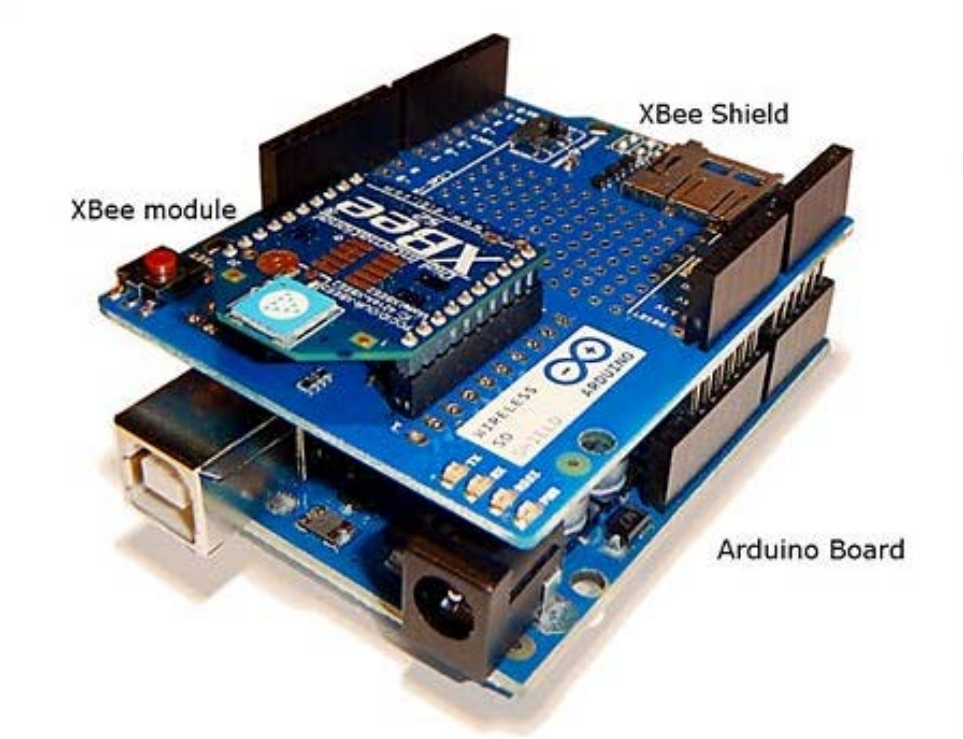


Figura 14. Hardware abilitante la connessione ZigBee

Tale configurazione è equiparabile dal punto di vista della connessione a molti dispositivi commerciali tra cui:

- AES1220 - ZigBee Smart Energy
- SafePlug 1203 - ZigBee Home Automation
- IHD2-TS - ZigBee Smart Energy In-Premise Display

I. Hacking ambiente prototipale

Di seguito vengono descritti i passi necessari per implementare un attacco di tipo Sinkhole sul nostro ambiente prototipale.

1. Si parte da uno scenario tipico: una rete ZigBee, tra cui alcuni dispositivi ZigBee + un coordinatore
2. Un dispositivo multiuso (emulato tramite un pc windows) si unisce legalmente alla rete (il dispositivo multiuso ha una connessione diretta a Internet)

3. Il dispositivo multiuso è violato per mezzo di uno specifico attacco
4. Tramite l'attacco, l'hacker prende il controllo del dispositivo multiuso, e lo utilizza per lanciare un attacco sinkhole alla rete domestica ZigBee
5. Il dispositivo multiuso è in grado di leggere / cancellare / modificare i pacchetti intercettati.

Attività chiave di tale attacco sono:

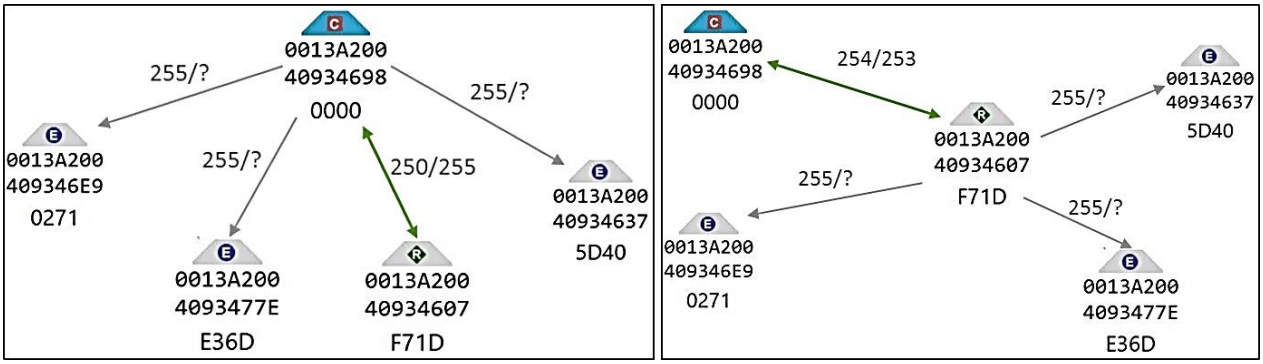
1. Prendere il controllo (totale) del dispositivo multifunzione
   a. Ottenuto sfruttando una vulnerabilità di uno dei software installati su tale dispositivo come ad esempio un popolare tool di automatizzazione di task HP Client Automation
   b. HP Client Automation a causa di alcuni problemi di autenticazione è vulnerabile al "Remote code Execution"
   c. In Metasploit (un noto tool di penetration testing) è disponibile un exploit per poter sfruttare tale vulnerabilità, che installa sulla macchina target una connessione desktop remoto e abilita un utente malevolo con privilegi di amministrazione

2. Modificare la Potenza trasmissiva del modulo XBee ZigBee
   a. Tramite riga di commando
   b. Tramite le API XBee ZigBee
   c. Tramite un opportuno software di configurazione XCTU

Anche in questo caso, la modifica della potenza di trasmissione fa sì che gli altri nodi vedano il nodo malevolo come il miglior percorso verso il coordinator e pertanto esso sarà utilizzato come percorso preferenziale.

II. Risultati sperimentali

Abbiamo monitorato la percentuale di nodi attivi (cioè collegati alla rete domestica) che utilizzano il dispositivo dannoso come gateway. L'attacco anche in questo caso ha successo.



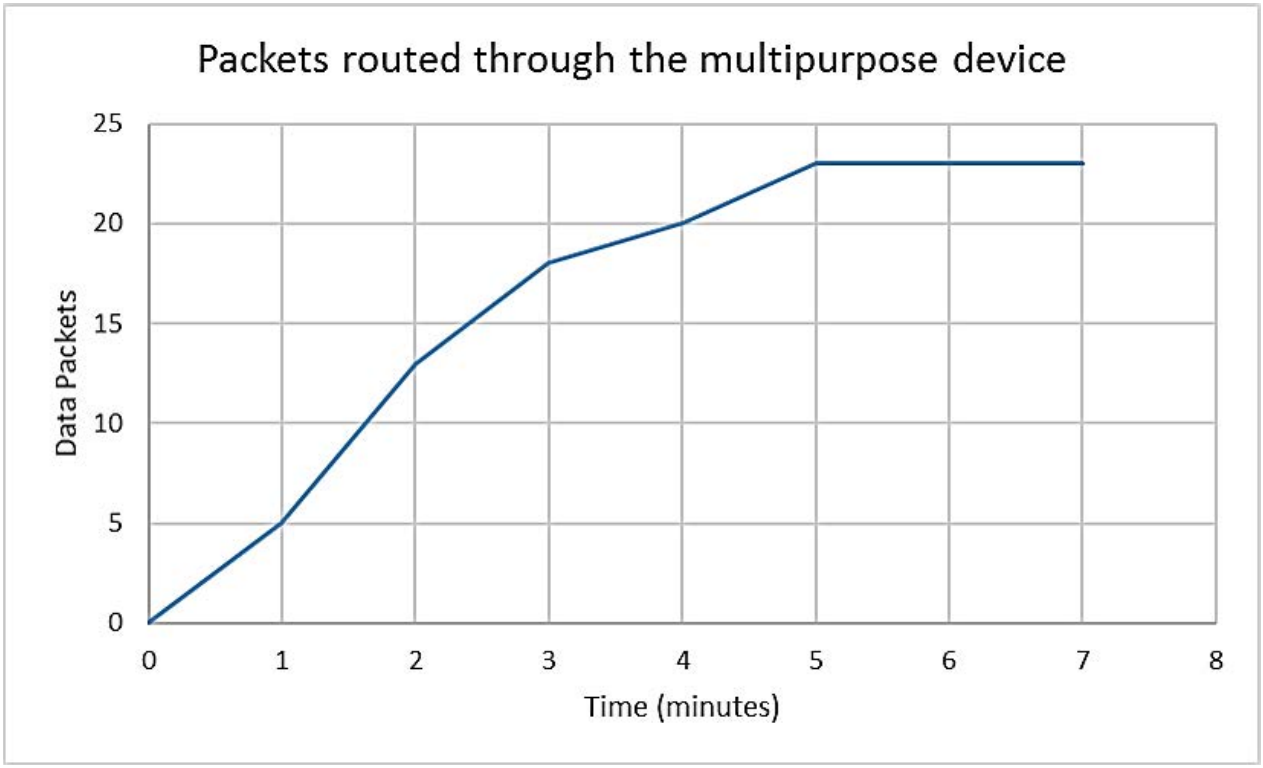


Figura 15. Stato delle connessioni tra i nodi prima e dopo l'attacco (l'attaccante è evidenziato dalla lettera R)

Figura 16. Hacking ambiente prototipale (Ogni nodo invia un pacchetto al coordinatore al minuto)

Conclusioni

Molte delle tecnologie emergenti che vengono sempre più utilizzate nelle Smart Home, le espongono ad una moltitudine di attacchi informatici. Sorprendentemente, tuttavia, questo è un problema in larga misura trascurato o comunque sottostimato. In particolare, la minaccia alla sicurezza rappresentata da dispositivi che possono potenzialmente fungere da ponte tra la rete ZigBee e la rete IP non è analizzata nella letteratura scientifico/tecnica. Tutto ciò rende possibile portare a termine attacchi (relativamente) semplici ma efficaci, che possono avere effetti devastanti.

Bibliografia

[1] S. Perumal, N. M. Norwawi and V. Raman, "Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology," Digital Information Processing and Communications (ICDIPC), 2015 Fifth International Conference on, Sierre, 2015, pp. 19-23.

[2] https:// www.bluetooth.com/what-is-bluetooth technology/bluetooth

[3] https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics/low-energy

[4] http://www.ZigBee.org/

[5] http://www.z-wave.com/

[6] http://6lowpan.net/

[7] http://threadgroup.org/About.aspx

[8] http://www.nearfieldcommunication.org/

[9] http://www.ibeacon.com/

[10] https://fas.org/irp/nic/disruptive.pdf

[11] http://www.forbes.com/sites/josephsteinberg/2014/01/27/these-devices-may-be-spying-on-you-even-in-your-own-home/#3baf9bd76376

[12] http://www.businessinsider.in/We-Asked-Executives-About-The-Internet-Of-Things-And-Their-Answers-Reveal-That-Security-Remains-A-Huge-Concern/articleshow/45959921.cms

[13] https://iotsecurityfoundation.org/

[14] https://www.shodan.io/

[15] Luigi Coppolino, Valerio D'Alessandro, Salvatore D'Antonio, Leonid Levy, and Luigi Romano "My smart home is under attack", in Christian Plessl, Didier El Baz, Guojing Cong, Joo M. P. Cardoso, Lus Veiga, and Thomas Rauber, editors, CSE, pages 145-151. IEEE Computer Society, 2015