Elementi di sicurezza negli impianti domotici - parte seconda

Author : Matteo De Simone

Date : 11 settembre 2018

Continuiamo questo excursus sul tema della sicurezza negli impianti domotici iniziato con il precedente articolo. Siamo partiti analizzando le fragilità introdotte dal fattore umano e ora, in questo articolo, affronteremo il tema dal punto di vista dell'infrastruttura tecnica impiantistica. Concluderemo il nostro percorso nel prossimo articolo affrontando le problematiche che nascono con l'apertura della casa domotica a servizi Internet esterni.

Un impianto domotico può essere visto come un sistema di reti specializzate ed interconnesse. Ad esempio, in una casa potremmo avere una rete dedicata all'automazione e controllo luci che sarà implementata con protocolli e modalità specifiche, un impianto di raffrescamento e uno di diffusione audio/video. Queste reti verranno, quindi, interconnesse e messe in grado di comunicare tra loro per raggiungere il livello di intelligenza oggi atteso in un'abitazione domotica.

La fase di integrazione dei diversi sistemi non è sempre presente nei progetti. Ci sono casi in cui i vari sistemi vivono indipendentemente l'uno dall'altro e resta all'utente l'onere di eseguire singolarmente le operazioni su ogni comando. Tuttavia, per la nostra trattazione, definiremo questo scenario – ovvero la realizzazione di uno o più sistemi specializzati giustapposti all'interno di una costruzione – con il termine *home automation*; mentre, una rete interconnessa di sistemi specializzati – e la conseguente forma di comportamento intelligente che ne scaturisce – definisce per noi un impianto di tipo domotico (si faccia riferimento al concetto di Ambient Intelligence introdotto nell'articolo precedente).

Tipologie di reti di automazione e propensione alla sicurezza

Se dovessimo individuare un elemento che possa descrivere l'evoluzione degli impianti domotici residenziali, potremmo focalizzarci sull'idea di contenuto informativo, ossia il passaggio da impianti a basso contenuto informativo a quelli ad alto contenuto informativo. Per gli specialisti dell'IT questa evoluzione può sembrare lapalissiana ma per il settore edile che la sta vivendo dall'interno proprio in questo momento, risulta un cambio radicale non solo

tecnologico ma soprattutto culturale.

Esplicitiamo il concetto con un semplice esempio: un impianto elettrico tradizionale attraverso la propria rete distribuiva un'unica informazione ovvero la presenza o meno della corrente elettrica (acceso/spento). Un impianto domotico, invece, può abbinare all'informazione di stato della lampadina anche informazioni di consumo, frequenze di utilizzo, descrizioni dei corpi luminosi e così via. Tipicamente questo avviene affiancando ai cavi di distribuzione elettrica, dei *bus* di comunicazione seriali tra dispositivi. Stesso discorso può essere applicato a sistemi di natura non elettrica, dove il passaggio alla codifica digitale delle informazioni non è propriamente affine. Gli impianti idrici o di termoregolazione oggi affiancano alle reti di tubature, reti di sensori che raccolgono e arricchiscono le informazioni che circolano nella infrastruttura da loro governata.

In questo scenario il tema della sicurezza dell'informazione trasmessa viene risolta principalmente considerando i sistemi come chiusi e difficilmente manomissibili: cavi interrati o murati, necessità di accedere ai locali per poter manomettere l'impianto, etc. Tuttavia, con la crescente diffusione della domotica, la crescente integrazione degli impianti con reti IP e la progressiva introduzione nel mercato di dispositivi wireless, i sistemi non sono più realmente chiusi, non è più necessario introdursi in casa per poter accedere ad un impianto e la manomissione diventa più semplice e probabile.

Sicurezza dei principali protocolli della domotica

Di protocolli nell'ambito domotico ve ne sono molti e spesso legati principalmente alla tipologia di impianto. A puro titolo esemplificativo (e non esaustivo), abbiamo analizzato alcuni dei protocolli più diffusi al momento e con i quali abbiamo avuto l'opportunità di lavorare in prima persona: **Dali, DMX, Modbus, LonTalk, BACnet, Konnex, ZigBee e Z-Wave**.

Dali (Digitally Addressable Lighting Interface) [11] e **DMX (Digital MultipleX)** sono due protocolli seriali dedicati al controllo luci, uno più diffuso in ambito industriale e grandi edifici e il secondo più legato all'illuminotecnica per lo spettacolo. Nessuno dei due protocolli presenta meccanismi di sicurezza (autenticazione, identificazione dei nodi, cifratura delle comunicazioni). Forse devono parte della loro fortunata diffusione anche alla semplicità di installazione e configurazione che deriva dalla mancanza di funzionalità di sicurezza che, obiettivamente, necessitano di competenze e attenzioni aggiuntive. Lavorando con reti basate su questi protocolli, non c'è altra soluzione di sicurezza che non scegliere attentamente eventuali gateway di conversione verso TCP/IP o, ancora meglio, sarà opportuno cercare di evitare di esporre questi impianti all'esterno. Non è difficile pensare ad attacchi di tipo *network sniffing* o *man-in-the-middle* da implementare con un po' di *reverse engineering* sui pacchetti TCP.

Modbus è un protocollo di comunicazione nato in ambito industriale. Il Modbus non offre meccanismi di sicurezza ma lascia questa incombenza ad un successivo *layer* di trasporto. Ad esempio Modbus offre due opzioni: seriale e TCP/IP. Un dispositivo che implementa un Modbus-TCP potrà utilizzare tutte le opzioni di autenticazione e cifrature definite dal livello di trasporto dello stack TCP. Di fatto, Modbus-TCP resta molto fragile a livello di sicurezza tanto che diverse tecniche di attacco sono state documentate (DoS, pacchetti malformati, invio comandi da device

non autorizzati) [7] e parimenti è possibile trovare proposte di varianti che introducono un livello di sicurezza maggiore [3] ma che al momento non hanno riscontrato sufficiente successo e diffusione.

LonTalk [5], invece, è un protocollo ampiamente diffuso tra i produttori di sistemi di raffrescamento e condizionamento. Il protocollo offre un meccanismo di autenticazione dei device ma nessun livello di cifratura [8]. Purtroppo, lo standard utilizzato per l'implementazione dell'autenticazione (ISO/IEC 14908) risulta essere poco sicuro come evidenziato già dal 2015 [9]. Fortunatamente, in modo analogo a quello che fa Modbus con il TCP/IP, LonTalk può essere veicolato attraverso reti basate su BACnet rafforzandone la sicurezza.

BACnet, appena citato, è un protocollo per reti di sensori e attuatori che offre uno stack di comunicazione completo: *layer* applicativo, network, data-link e fisico. Il protocollo può supportare differenti metodologie di autenticazione anche se al momento l'unico implementato è la *proxy user authentication* [10], mentre l'identità dei nodi della rete è garantita attraverso 6 tipologie differenti di chiavi; la comunicazione è cifrata utilizzando il protocollo AES. Le reti BACnet sono particolarmente esposte ad attacchi di *spoofing*, DoS, attacchi che alterino i valori degli oggetti dati scambiati e attacchi che puntano a corrompere le tabelle di *rounting* [6].

Un altro colosso dei protocolli per la domotica è il **Konnex (KNX)**, standard frutto della collaborazione dei maggiori produttori di materiale elettrico in Europa. Fino al 2016 non ha offerto alcun livello di sicurezza. La comunicazione KNX, che può essere effettuata utilizzando sia comunicazione seriale che TCP/IP ed è esposta ad attacchi di vario genere: *denial of service*, *network sniffing, man-in-the-middle, code injection, message replay* [1]. Fortunatamente nel 2016 il consorzio KNX ha introdotto una cifratura AES e un meccanismo di identificazione dei nodi basato su chiavi Diffie-Hellman [2] per arginare il problema. Nella pratica, però, queste novità hanno una diffusione limitata sia perché molto recenti rispetto ai ritmi dell'industria edile, sia a causa della gran quantità di hardware preesistente.

ZigBee è un protocollo pensato per la comunicazione senza fili. In particolare le reti ZigBee puntano a minimizzare i consumi e a compensare le problematiche di robustezza tipiche del WiFi. Anche questo protocollo offre uno stack completo in quattro layer, dal livello applicativo fino a quello fisico. Una rete ZigBee offre cifratura tramite AES a 128bit sul canale di trasmissione e assicura l'integrità dei pacchetti usando il *cipher block chaining message authentication code* (CBC-MAC). Inoltre, a livello applicativo, sono definiti dei profili di capacità che garantiscono specifici permessi a seconda del tipo di scopo del device. Il protocollo è considerato, dal punto di vista della sicurezza, uno tra i più sicuri e robusti del settore. I rischi principali, in questo caso, restano eventuali problemi o carenze implementative dei produttori.

Chiudiamo citando un altro protocollo leader nella comunicazione wireless in particolare orientato specificatamente verso i *device consumer*: **Z-Wave** [13]. Probabilmente, la differenza principale con lo ZigBee, è il contesto applicativo. Il protocollo offre, infatti, caratteristiche specificatamente pensate per rendere facile e sicura la comunicazione dei nodi di una rete con servizi cloud TCP/IP di monitoraggio, aggregazione dati e gestione. Dato il tipo di mercato a cui si rivolge (molto ampio e con poche competenze tecniche specifiche) l'attenzione alla sicurezza è molto alta e sono presenti meccanismi di cifrature AES e di autenticazione tramite chiave. Nel

2017 a seguito di una falla riscontrata in una rete Z-Wave dovuta ad un problema implementativo di uno specifico device [14], la Z-Wave Alliance – il consorzio che cura il protocollo – ha deciso, invece che minimizzare l'accaduto, di rilasciare un aggiornamento pensato per rafforzare ulteriormente il grado di sicurezza contro attacchi *man-in-the-middle* e *brute force* con un nuovo algoritmo di *key exchange* (ECDH) e ha potenziato la sicurezza di comunicazione verso servizi cloud abilitando il *tunneling* su TLS [14].

In generale, è bene sottolineare un aspetto intrinseco che, al di là dello specifico protocollo, impatta in modo determinante sulla sicurezza di una casa domotica. Da un lato ci sono i produttori che devono combattere – soprattutto in questo momento dove il mercato si è fatto aggressivo – con vincoli di consumi, costi e ingombri: a volte quindi la tentazione di prendere una scorciatoia o di proporre una variante proprietaria dei protocolli che supportino in modo meno stringente alcune *feature* può essere molto forte. Dall'altro lato, bisogna tenere conto che la capacità del parco installato esistente di essere aggiornato è molto limitato: un *device* con un problema o che implementa un protocollo non aggiornato, probabilmente resterà al suo posto per tutta la vita dell'immobile o fino ad un suo guasto.

Altri rischi nelle reti domotiche

Oltre agli aspetti legati ai singoli device e ai protocolli, ci sono altri aspetti che meritano attenzione per cercare di completare il quadro:

- mancanza di separazione tra reti LAN dedicate alla domotica e quelli di uso quotidiano;
- sicurezza insufficiente delle LAN;
- obsolescenza e aggiornamento;
- variabilità: ovvero introduzione di sistemi end-user non verificati o messi in sicurezza.

Tema delicato è la **mancanza di separazione** tra la rete LAN domestica e quella dedicata ai sistemi domotici. Una prassi che si può constatare spesso è l'abitudine di connettere gli apparati direttamente alla LAN esistente in casa. Questo, ovviamente, espone gli impianti nevralgici di casa ad ogni tipo di attacco proveniente da Internet. L'installatore e il progettista dovrebbero considerare sempre la creazione di una rete LAN dedicata e protetta esplicitamente a supporto degli impianti.

Fa il paio con il punto precedente la **necessità di proteggere in modo adeguato l'accesso della rete** Internet domestica. A riguardo viene parzialmente in aiuto la crescente attenzione da parte delle società fornitrici di servizi di connettività al tema della sicurezza: i dispositivi messi a disposizione sono cresciuti in termini di qualità e in termini di preconfigurazione e capacità di autoaggiornamento. Ovviamente l'intervento di uno specialista in fase di installazione e buone norme di comportamento restano fondamentali (cfr. nostro precedente articolo).

Altro tema importante – ma che non ha una risposta adeguata al momento – è quello della **manutenzione e la necessità di mantenere aggiornati i *device*** che formano l'impianto. Soprattutto i *gateway* di connessione dei protocolli seriali verso IP e i dispositivi che governano e formano la LAN di supporto. Nel residenziale l'idea di manutenzione programmata è del tutto aliena: anche gli stessi installatori non offrono spesso servizi di manutenzione per l'utente

residenziale. Questa situazione favorisce la diffusione di impianti con apparati non aggiornati soprattutto a livello software/firmware. Sarà necessario che gli operatori del settore si adoperino per trovare una risposta a questa esigenza; magari gli stessi produttori di hardware potrebbero favorire l'introduzione di meccanismi di autoaggiornamento o servizi specifici come già accade per telefoni e laptop.

Ultimo punto della nostra lista è la **variabilità**. Con il progressivo ingresso nel settore di dispositivi IP acquistabili direttamente degli utenti anche una rete messa inizialmente in sicurezza può, con l'aggiunta di ulteriori *device*, esporre progressivamente l'infrastruttura a problemi di sicurezza derivanti da cattive configurazioni, bug o servizi non affidabili. La cronaca riporta regolarmente notizie di problematiche di sicurezza e privacy dovute a *device end user* [4]. Questo fattore di rischio, più che altro, è un moltiplicatore delle criticità precedenti: un accesso fraudolento alla rete tramite un *device* non protetto può favorire il controllo degli impianti di casa se, ad esempio, la rete domestica non è adeguatamente separata da quella tecnica e se magari è governata da un router non aggiornato.

Nel prossimo articolo ci dedicheremo al mondo sempre più importante che riguarda i servizi online dedicati alla casa e degli aspetti di sicurezza che, l'interfacciamento verso tali servizi, interessano sia dal punto di vista dell'utilizzatore e che dell'installatore.

Note

1. A Practical Attack Against a KNX-based Building Automation System – A. Antonini, F. Maggi, S. Zanero – http://dx.doi.org/10.14236/ewic/ics-csr2014.7
2. Using KNX Secure in ETS5 - KNX Association – http://www.knx.it/download/DOCUMENTAZIONE_KNX/07_M.Vettorato_-_KNX_Secure_-_Use_in_ETS5.pdf
3. DESIGN AND IMPLEMENTATION OF A SECURE MODBUS PROTOCOL – I.N. Fovino, A. Carcano, M. Masera, Trombetta – https://pdfs.semanticscholar.org/6f6e/477a9e2bcafcc94f5b13cf8cbf6ab694ecc7.pdf
4. https://www.corrierecomunicazioni.it/media/smart-tv-allarme-security-rischio-intrusioni-hacker/
5. LonWork protocol overview – https://www.rtaautomation.com/technologies/lonworks/
6. https://www.certsi.es/en/blog/security-protocols-building-automation
7. https://www.cyberbit.com/blog/ot-security/scada-modbus-protocol-vulnerabilities/
8. LonTalk® Protocol Specification – http://www.enerlon.com/JobAids/Lontalk%20Protocol%20Spec.pdf
9. Dumb Crypto in Smart Grids: Practical Cryptanalysis of the Open Smart Grid Protocol – P. Jovanovic, S. Neves – https://eprint.iacr.org/2015/428.pdf
10. https://en.wikipedia.org/wiki/Proxy_server
11. Digitally Addressable Lighting Interface (DALI) Communication – http://ww1.microchip.com/downloads/en/AppNotes/01465A.pdf
12. https://it.wikipedia.org/wiki/Digital_MultipleX
13. https://z-wavealliance.org
14. https://www.cnet.com/news/your-z-wave-smart-home-gadgets-just-got-more-secure/

A cura di: **Matteo De Simone, Michelangelo De Bonis**