(Versione documento: draft - 1.1)

Analisi delle problematiche di sicurezza all'interno della piattaforma SHELL

Dario Russo, Vittorio Miori

INDICE

1. Sommario

Nel modello architetturale di SHELL, le comunicazioni di rete tra nodi rivestono un ruolo principale. In particolare, le comunicazioni vengono effettuate tra *host*, tra un *host* ed uno o più *manager*, e tra l'*home manager* ed *Internet*.
La sicurezza nell'archiviazione e nella trasmissione dei dati, richiede di adottare adeguate misure per proteggere tali dati da intrusioni, sia da un loro utilizzo diverso da quello previsto dai legittimi possessori e/o operatori, sia da malfunzionamenti di sistema.
La problematica relativa alla sicurezza informatica all'interno della piattaforma SHELL, è considerata un punto chiave ed è affrontata tenendo conto di cinque aspetti: *riservatezza*, *integrità*, *non ripudio*, *disponibilità* e *aggiornamento*.

2. Abstract

In the SHELL architectural model, network communication between nodes plays a major role. In particular, communications occur between *hosts*, between a host and one or more *managers*, and between *home manager* and *Internet*.
Security in the storage and data transmission phases, requires to take adequate measures to protect such data from intruders, both to protect them from any use that is not as expected by the legitimate owners and/or operators, and by system malfunctions.
The information security within the SHELL platform issue is considered a key point and it is addressed taking into account five aspects: *confidentiality, integrity, non-repudiation, availability* and *upgrade*.

3. L'architettura SHELL in breve

L'architettura della piattaforma SHELL sulla quale occorre implementare meccanismi di sicurezza è basata su una rete di *HOST* che contengono al loro interno *device reali* e/o *virtuali* (Figura 1).

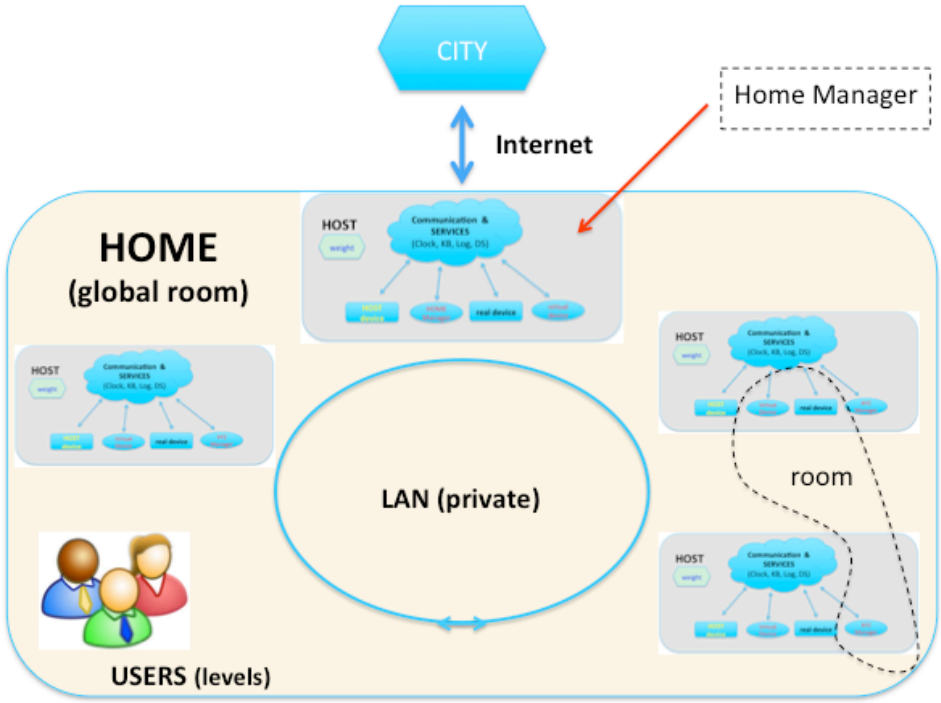

Figura 1: L'architettura SHELL

Un HOST è un sistema (embedded) reale connesso alla rete LAN che contiene l'implementazione di uno o più devices, esso quindi possiede sempre un indirizzo IP e una geolocalizzazione. I dispositivi implementati possono essere sia virtuali che reali, in quest'ultimo caso se sono nativi (SHELL compliant), l'host deve disporre dell'hardware necessario

alla loro implementazione. Se invece essi sono *wrapped* (appartenenti a una tecnologia domotica non compatibile con il sistema SHELL), l'host deve possedere le opportune interfacce per i bus fisici richiesti, al fine della loro integrazione nel framework.
I dispositivi possono essere raggruppati in gruppi (*room*). Ogni gruppo ha un *manager* che lo gestisce e ne determina le funzionalità e lo scopo.
Ogni dispositivo può appartenere ad uno o più gruppi. Esiste sempre un gruppo predefinito chiamato *home manager,* che supervisiona le attività di tutta la rete di dispositivi della casa.

4. La sicurezza all'interno della piattaforma SHELL

La sicurezza nell'archiviazione e nella trasmissione dei dati, richiede di adottare adeguate misure per proteggere tali dati da intrusioni, sia da un loro utilizzo diverso da quello previsto dai legittimi possessori e/o operatori, sia da malfunzionamenti di sistema. Questo problema, ha acquisito una connotazione particolare soprattutto nel campo informatico nell'uso dei computer e delle reti di trasmissione. La corsa odierna per fornire funzionalità sempre più specifiche ha portato a sistemi scarsamente sicuri, creando numerosissime vie di attacco per gli hackers. Fino ad ora le aziende produttrici si sono concentrate maggiormente sullo sviluppo dei vari dispositivi smart, in genere trascurando il fattore sicurezza, soprattutto a causa degli alti costi legati alla ricerca, sviluppo e supporto.

Negli ultimi anni, c'è stata un'esplosione di prodotti e di dispositivi che promettono di rendere le nostre case sempre più "intelligenti". Tuttavia i dispositivi per la domotica possono essere un facile obiettivo degli hackers se si trascura la sicurezza della smart home. Inoltre, il desiderio dei consumatori di controllare la loro casa dal proprio smartphone mediante applicazioni e portali web che consentono di operare da lontano, significa che se per esempio si perde il telefono, ciò potrebbe portare a spiacevoli conseguenze significative per la sicurezza domestica. E così, il sogno della casa intelligente, interconnessa, monitorabile e gestibile da remoto potrebbe trasformarsi in un incubo: estranei potrebbero averne il controllo, provocando danni, facendo razzia di dati personali, immagini, video, audio e informazioni sensibili con una conseguente maggiore esposizione ad intrusioni e furti, sia fisici che di identità personale.

Per questi motivi, la problematica relativa alla sicurezza informatica all'interno della piattaforma SHELL, è considerata un punto chiave ed è affrontata tenendo conto di cinque aspetti:

- *riservatezza*: evitare l'accesso ai dati a chi non è autorizzato (es. autenticazione e cifratura dei dati);
- *integrità*: evitare che i dati possano essere modificati, cancellati, resi illeggibili, attaccati da virus, garantendo quindi che questi siano sempre corretti (verifica del dato);
- *non ripudio*: permettere di garantire che una transazione non possa essere negata;
- *disponibilità*: garantire che i dati siano accessibili quando servono (es. gestione delle vulnerabilità, data loss prevention e backup);
- *aggiornamento*: permettere l'aggiornamento dei singoli componenti della piattaforma (infrastrutturali e dei singoli dispositivi) al fine di permettere la correzione di eventuali malfunzionamenti dovuti ad errori funzionali e falle di sicurezza.

4.1. Riservatezza

La protezione della riservatezza ha lo scopo di fornire l'accesso e la fruizione dei dati solamente alle persone e/o entità informatiche autorizzate. Per ottenere ciò è di fondamentale importanza un meccanismo che certifichi l'identità di chi richiede l'accesso ai dati e di chi li fornisce. Infatti, se un nodo A vuole parlare con un nodo B, chi può assicurare ad A che è realmente B il nodo con cui sta comunicando? Questo porta ad una esposizione ad attacchi così detti *Man-In-The-Middle*: un attaccante C può "mettersi in mezzo" tra A e B, spacciandosi presso A per B e viceversa. Per risolvere questo problema solitamente vengono introdotti meccanismi di *autenticazione* e di *cifratura*.

Con l'autenticazione vengono fornite le informazioni riguardo l'identità di un nodo e vengono validati i permessi di accesso. Con la cifratura vengono codificati i messaggi scambiati in modo che solo i due veri nodi siano in grado di interpretarli.

Nel modello architetturale di SHELL, le comunicazioni di rete tra nodi rivestono un ruolo principale. In particolare, le comunicazioni vengono effettuate tra *host*, tra un *host* ed uno o più *manager*, e tra l'*home manager* ed Internet. La comunicazione tra due o più dispositivi viene sempre mediata dagli *host*, i quali si fanno garanti della corretta comunicazione. Nel caso in cui un *host* debba interagire direttamente o con un dispositivo SHELL (fisico o virtuale), lo scambio dei messaggi avverrà tramite una comunicazione di rete che dovrà implementare i meccanismi di sicurezza più opportuni.

Diversamente, nella comunicazione tra *host* e un dispositivo fisico *wrapped*, la sicurezza e l'integrità del singolo dispositivo, sarà quella prevista dai meccanismi architetturali del sistema domotico a cui quest'ultimo appartiene. Contrariamente, occorrerebbe intervenire all'interno dello specifico protocollo domotico, alterandone così le sue caratteristiche ed il suo funzionamento, ma per una precisa scelta progettuale non si debbono modificare in alcun modo le singole architetture domotiche che vogliamo integrare.

In ogni transazione all'interno della piattaforma SHELL occorre quindi identificare con certezza assoluta il mittente ed il destinatario dei messaggi, verificare le loro caratteristiche e le loro autorizzazioni alla comunicazione, al fine di evitare che un nodo intruso possa inviare e ricevere comandi senza averne diritto.

Di non minore importanza è la problematica relativa al riconoscimento e certificazione dei dispositivi al momento del loro ingresso nel sistema. E' indispensabile fornire alla piattaforma dei meccanismi in grado di verificare che il dispositivo da integrare sia esattamente quello che vogliamo inserire, e non di uno che si possa fingere per tale e che venga introdotto da terzi all'interno della rete domestica, per fini non leciti.

Inoltre occorre gestire le connessioni provenienti dall'esterno evitando quelle malevoli. Essendo l'*home manager* connesso alla rete Internet per fornire alcune funzionalità della casa da e verso l'esterno, esso lo rende un punto sensibile agli attacchi da parte di hacker. Esso per gestire le comunicazioni utilizza il cosiddetto *home gateway* che consiste in un sisetma Hw/Sw dedicato allo scopo. Nel sistema SHELL, tale compito potrebbe essere svolto dal *set-top box,* che permette anche di aggiungere funzionalità multimediali all'interno dell'abitazione.

Per risolvere questo tipo di problemi, alcune delle tecnologie e delle soluzioni che è possibile introdurre sono:

- *firewall*: è un componente di difesa perimetrale di una rete informatica, che può anche svolgere funzioni di collegamento tra due o più tronconi di rete, garantendo dunque una protezione in termini di sicurezza informatica della rete stessa;
- *virtual private network (VPN)*: connessioni *point-to-point* su una rete pubblica o privata, ad esempio Internet, che utilizzano protocolli di tunneling per eseguire una chiamata virtuale a una porta virtuale su un server VPN. Il server di accesso remoto risponde alla chiamata virtuale, autentica il chiamante e trasferisce i dati tra il client VPN e la rete privata della casa.
- *intrusion detection system*: per identificare accessi non autorizzati ai computer o alle reti locali;
- *intrusion prevention system*: per impedire ad un programma non autorizzato di entrare in esecuzione;
- *certificati e / o chiavi asimmetriche*: permettono di criptare i messaggi e di garantire che solo il mittente ed il destinatario siano in grado di interpretare correttamente tali messaggi.

4.2 Integrità

L'integrità consente di verificare con assoluta certezza se un dato o una informazione siano rimasti integri, ossia inalterati nel loro contenuto, durante la loro trasmissione e/o la loro memorizzazione. In un sistema che garantisce l'integrità, l'azione di una terza parte di modifica del contenuto delle informazioni scambiate tra mittente e destinatario viene rilevata.

C’è una sostanziale differenza tra il controllo della corretta trasmissione delle informazioni e la loro protezione sicura. Poiché nelle trasmissioni, il codice di controllo di integrità del messaggio può viaggiare non protetto, al fine della sicurezza è necessario garantire sia che solo il mittente possa generare tale codice, sia la sua opportuna protezione durante la trasmissione. Se così non fosse, chiunque potrebbe modificare tale messaggio e sostituire il codice originale.

Il controllo dell’integrità dei dati permette al sistema di difendersi da due tipi distinti di minacce: quelle intenzionali e quelle non intenzionali. Le minacce intenzionali sono quelle effettuate da terze parti esterne alla piattaforma che, con finalità criminali, si potrebbero introdurre nel sistema alterandone le comunicazioni ed il funzionamento. Le minacce non intenzionali comprendono la vulnerabilità del sistema o dei dati critici, a causa di errori, scarso giudizio o atti non voluti.

Tali problematiche le ritroviamo anche nel modello architetturale SHELL, l’integrità dei messaggi scambiati all’interno della piattaforma, dei programmi memorizzati all’interno dei dispositivi e delle informazioni memorizzate nelle banche di dati, sono infatti di importanza strategica in quanto garantiscono la bontà e l’efficacia del funzionamento dell'intero sistema.

Anche le comunicazioni SHELL infatti possono essere alterate, per fini malevoli, da soggetti terzi durante il loro transito all’interno del framework. Un attacco al sistema molto pericoloso e quello del *Man-In-The-Middle.* In questo caso, invece della sostituzione del nodo destinatario del messaggio (come visto sopra nel caso della riservatezza), l’attacco potrebbe consistere nell’alterazione dei contenuti dei pacchetti dati e nel loro rinvio con il loro contenuto modificato, ai veri nodi destinatari. Un altro esempio di un possibile attacco all’integrità è quello di cambiare in modo fraudolento la programmazione di un dispositivo (solitamente memorizzato su una EPROM - Erasable Programmable Read Only Memory), alterandone così il suo comportamento. Anche le informazioni presenti all’interno di banche di dati potrebbero essere alterate a fini malevoli modificando, ad esempio, lo storico di determinati eventi e la cancellazione delle tracce degli attacchi.

Le comunicazioni o il comportamento di un dispositivo potrebbero vernire alterati anche a causa di malfuzionamenti dei nodi del sistema, dei dispositivi o dell’infrastruttura di rete. Con un sistema di controllo dell’integrità è possibile intercettare il problema e gestirlo di conseguenza.

Per risolvere questo tipo di problematiche, alcune delle tecnologie e delle soluzioni che è possibile introdurre all'interno delle trasmissioni, sono:

- *crittorgrafia simmetica o asimmetrica*: oltre che ad identificare il mittente ed il destinatario, spesso permette di controllare anche l’integrità dei dati scambiati;
- *MD5*: funzione hash crittografica standardizzata con la RFC 1321. E' una funzione unidirezionale diversa dalla codifica e dalla cifratura perché essa è irreversibile. Questa funzione prende in input una stringa di lunghezza arbitraria e ne produce in output un'altra a 128 bit. Il processo avviene molto velocemente e l'output (noto anche come *MD5 Checksum* o *MD5 Hash*) restituito, è tale per cui è altamente improbabile ottenere da due diverse stringhe in input, uno stesso valore hash in output.

4.3 Non ripudio

Il non ripudio ha lo scopo di fornire la prova incontestabile di un'avvenuta spedizione o di un'avvenuta ricezione di dati in rete. Il non ripudio assume due modalità:

- *non ripudio della sorgente*: prova chi è il mittente dei dati in una transazione;
- *non ripudio della destinazione*: prova che i dati sono arrivati ad uno specifico destinatario.

Generalmente il servizio di non ripudio è richiesto in quelle transazioni in cui bisogna avere garanzie di avvenuta spedizione/ricezione di flussi telematici.

Nel modello architetturale SHELL, la prova di chi è il mittente dei dati e che i dati siano arrivati correttamente allo specifico destinatario, è un’informazione cruciale. La certezza, la tracciabilità ed il controllo dell’avvenuta ricezione delle informazioni che viaggiano all’interno della rete, è un requisito importante per il corretto funzionamento del

sistema. Il meccanismo del non ripudio, ad esempio, potrebbe comprendere il mantenimento di uno storico dei messaggi, al fine di una loro verifica nel tempo.

4.4 Disponibilità

La disponibilità di un sistema misura la sua attitudine a svolgere una funzione richiesta in determinate condizioni e in un dato istante (es. fornire un servizio ad un utente), o durante un dato intervallo di tempo. La disponibilità dei dati è invece intesa come l'utilizzabilità del patrimonio informativo e riguarda l'accesso e la fruibilità delle informazioni. Da un punto di vista di gestione della sicurezza, le protezioni per la disponibilità saranno rivolte a ridurre a livelli accettabili i rischi connessi all'accesso alle informazioni.

Nel modello architetturale SHELL, i nodi di rete sono numerosi e ognuno di essi svolge un compito ben determinato. E' cruciale che tutti i nodi siano funzionanti e disponibili. Dovendo gestire molti dati in real-time, è importante anche avere la disponibilità delle informazioni, solo quando necessario e solo a chi ne compete. Occorrono quindi strumenti in grado di garantire il corretto funzionamento degli *host,* dei *manager,* e delle banche dati, proteggendoli da eventuali *crash* di sistema e da errori *fatali* (*fault* e *failure*) durante la loro esecuzione. Occorre inoltre sviluppare soluzioni di recupero delle informazioni e dei dati di sistema in caso vengano persi accidentalmente o malevolmente, con meccanismi di auto-ripristino in modo da rimettere in piena operatività il sistema nel più breve tempo possibile.

Per risolvere questo tipo di problematiche, alcune delle tecnologie e delle soluzioni che è possibile introdurre sono:

- *verifica della sicurezza di un programma*: verifica del suo comportamento, in modo tale da effettuare una ricerca estesa dei difetti presenti, per passare poi alla loro eventuale eliminazione. Esistono diversi modelli di sicurezza per il controllo dei programmi, basati perlomeno su due metodi differenti:

  (a) *Semantic-based security model* (modelli di sicurezza basati sulla semantica): la sicurezza del programma controllato viene esaminata in termini di comportamento del programma;

  (b) *Security-typed language* (modelli di sicurezza basati sul linguaggio): comportamento errato o indesiderabile del programma causato da una discrepanza tra i tipi di dati utilizzati per le costanti, le variabili e i metodi del programma (funzioni);

- *backup*: metodo per recuperare dati eventualmente persi o danneggiati. Il backup consiste nell'esecuzione di copie di sicurezza dei dati del sistema, onde evitare che essi vadano perduti o diventino illeggibili;

- *cloud*: molti aspetti di sicurezza dei dati vengono devoluti al cloud provider che eroga il servizio sulla "nuvola", con l'aiuto un opportuno staff tecnico.

4.5 Aggiornamento

Gli analisti informatici affermano che un facile obiettivo per gli hackers sono i dispositivi per le smart home in quanto sono tra i sistemi informatici sono quelli periodicamente meno aggiornati in assoluto, dopo l'installazione e collaudo.

Il rischio è davvero concreto perché mentre tutti ben conoscono e verificano gli aggiornamenti automatici del proprio computer e la presenza dell'antivirus attivo ed aggiornato, pochissimi sono quelli che invece si preoccupano di verificare da quanto tempo la centrale domotica non aggiorna il proprio sistema applicativo.

Secondo uno studio condotto dalla società di sicurezza *Synack*, se un utente malintenzionato è in grado di ottenere l'accesso ad un dispositivo domotico, quasi tutti i dispositivi della casa intelligente possono essere facilmente compromessi e trasformati. Ciò può essere ottenuto con il metodo di attacco informatico denominato *cavallo di Troia*.

Il modello architetturale SHELL è un sistema complesso dove sono previste numerose tecnologie che tra loro devono essere in grado di cooperare ed interagire nella maniera più corretta e sicura possibile. A questo fine, manenere tutti i sistemi aggiornati è un requisito che non deve essere trascurato. Per affrontare queste problematiche devono essere implementate soluzioni che automatizzino il processo di auto-aggiornamento delle singole componenti. Al termine di ogni aggiornamento, il sistema deve essere in grado di effettuare autonomamente dei test per verificare il corretto

funzionamento di tutti i suoi componenti e, in caso di problemi, ripristinare il sistema all'ultima configurazione funzionante.