Protocolli sicuri per la comunicazione fra sistemi embedded

La crescente pervasività dei dispositivi embedded dotati di connettività Internet impone l'adozione di protocolli efficienti per la sicurezza

Arun Subbarao
Director of Software Engineering presso LynuxWorks

Negli ultimi anni il numero di sistemi e di dispositivi embedded sul mercato è cresciuto in maniera esplosiva. Dal momento che questi dispositivi embedded diventano sempre più onnipresenti e dotati di connettività Internet per l'accesso in rete, la sicurezza del sistema embedded diventa una preoccupazione sempre più pressante.
La promessa della connettività universale crea maggiori possibilità per gli utenti malintenzionati per accedere ad informazioni riservate senza autorizzazione. È necessario disporre di livelli superiori di sicurezza negli stack del protocollo per assicurare che il flusso di informazioni fra i dispositivi embedded avvenga in tutta sicurezza.
Di seguito verranno analizzati alcuni aspetti chiave associati alla sicurezza dei sistemi embedded abilitati all'accesso ad Internet e le tecnologie che saranno alla base delle infrastrutture per le comunicazioni delle "reti embedded".

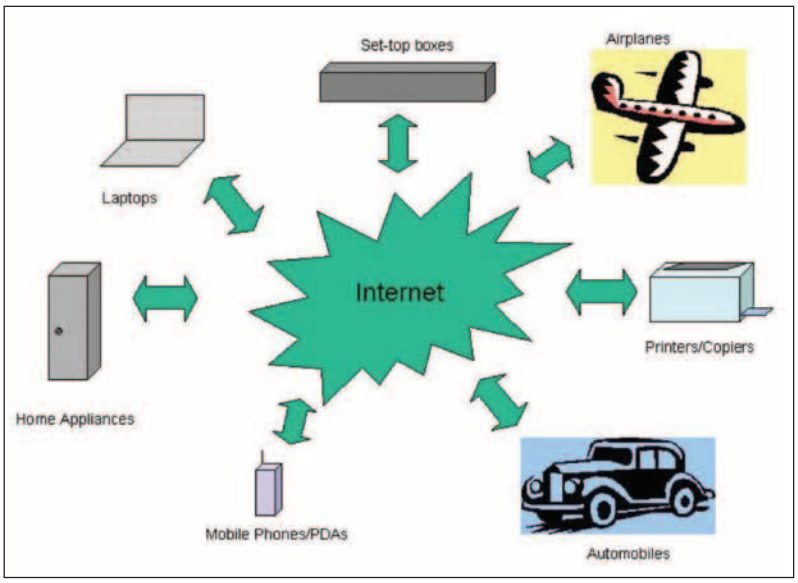

Fig. 1 - Alcuni esempi di sistemi embedded con accesso a Internet

Le sfide per la sicurezza

Secondo una stima di Nua Internet Surveys, la rete Internet conta attualmente oltre 600 milioni di utenti in tutto il mondo. Il numero dovrebbe crescere fino a oltre 2 miliardi entro la fine del decennio. Al diminuire del costo dei processori e della memoria, il numero di dispositivi embedded dotati di funzioni di comunicazione è aumentato nel corso degli ultimi anni e continua a crescere. D'altro canto, la proliferazione di dispositivi embedded sul mercato ha generato una sfida significativa per la sicurezza delle informazioni. Ai primordi dell'era Internet erano disponibili soluzioni che offrivano una connettività basata su PC su reti via cavo. Le criticità per la sicurezza erano comprese e gestite attraverso la caratterizzazione della topologia delle reti.
Dato che i dispositivi embedded stanno diventando sempre

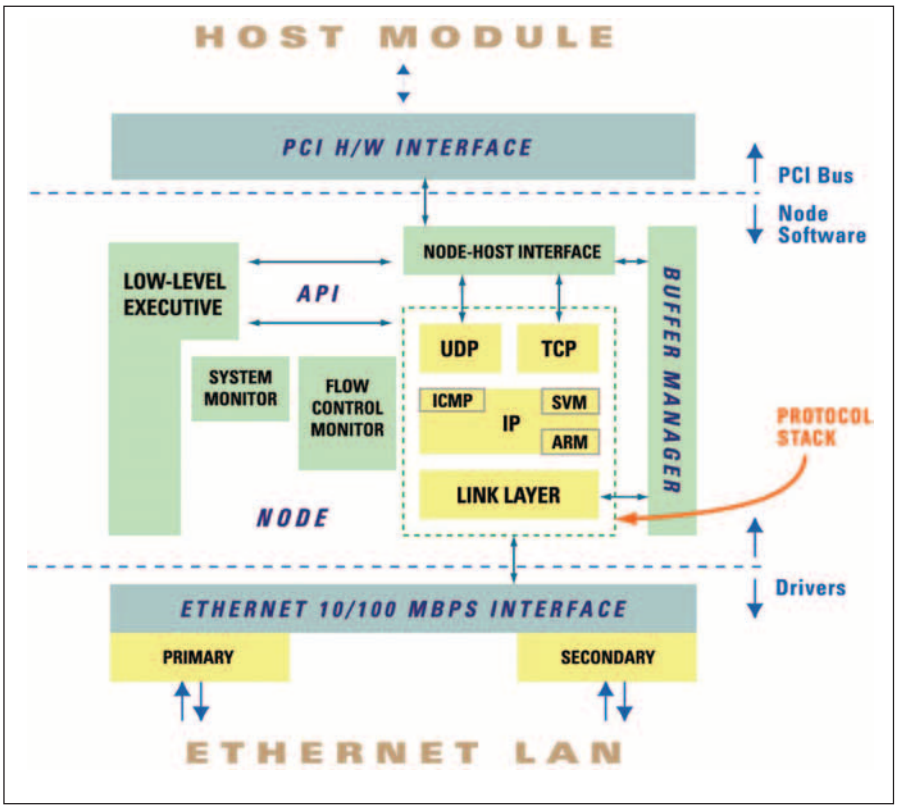

Fig. 2 - Lo stack Lynx Certifiable Stack funziona su un processore 8260 di Motorola e consente di scaricare l'elaborazione TCP/IP da un sistema host in tempo reale

più pervasivi e diffusi su larga scala, la complessità e la mobilità sono diventate concetti comuni. Le reti embedded sono caratterizzate da una varietà eterogenea di dispositivi come PDA, telefoni cellulari e altri dispositivi portatili. La loro topologia è estremamente dinamica dal momento che i dispositivi mobili possono apparire e scomparire in continuazione da una rete. Inoltre esistono molti più punti di guasto nelle reti embedded, il che crea maggiori opportunità per sfruttare le falle per la sicurezza e lanciare denial-of-service e altri attacchi. Di conseguenza esiste una necessità pressante di garantire la sicurezza all'interno degli strati dei protocolli di comunicazione.

Una comunicazione sicura

Sono stati definiti diversi protocolli per la sicurezza per vari livelli del modello di rete OSI. Questi possono essere classificati in tre macro categorie e seconda che agiscano sullo strato di trasporto, sullo strato di rete o sullo strato di collegamento. Tutti i protocolli usano le ben note tecniche di crittografia per cifrare i dati che vengono trasmessi lungo la rete di modo che non possano essere letti da chiunque ad eccezione del destinatario prestabilito.

I Secure Socket Layer (SSL) e Transport Layer Security (TLS) sono meccanismi per lo strato di trasporto e per la sicurezza a livello di applicazione, nei quali due applicazioni che comunicano lungo la rete possono condividere i dati cifrati usando una chiave segreta comune. Il protocollo di record e il protocollo di handshake sono definiti come parte degli schemi SSL/TLS e contribuiscono all'impostazione di una connessione sicura tra due applicazioni che hanno bisogno di comunicare fra loro. Questi protocolli sono usati più comunemente da applicazioni come i browser.

Il vantaggio di tale approccio è il fatto che garantisce la sicurezza end-to-end dall'applicazione client a quella server. Tuttavia ogni singola applicazione che richiede la gestione di comunicazioni sicure deve implementare il protocollo SSL/TLS.

Il protocollo IPsec (IP security) è un insieme di estensioni al protocollo Internet (IP, Internet Protocol), che può essere usato con i protocolli Ipv4 e Ipv6, ed è progettato per garantire la sicurezza pacchetto per pacchetto. Il protocollo IPsec assicura la cifratura dei pacchetti che sono instradati attraverso la rete Internet, allo scopo di evitare l'intercettazione da parte di utenti malintenzionati; il trasmettitore e il ricevitore condividono una chiave segreta. L'IPsec può essere usato per assicurare la cifratura per ciascuno dei protocolli per lo strato di trasporto come quelli TCP e UDP, e fornisce due protocolli separati per la cifratura dei pacchetti: l'Authentication Header (AH) e l'Encapsulated Security Payload (ESP).

Il protocollo AH protegge l'intero pacchetto dalla lettura e dalla manomissione, mentre ESP protegge i dati e i protocolli ai livelli superiori.

Il principale vantaggio dello schema IPsec è che non richiede che le applicazioni siano "consapevoli" delle funzionalità per la

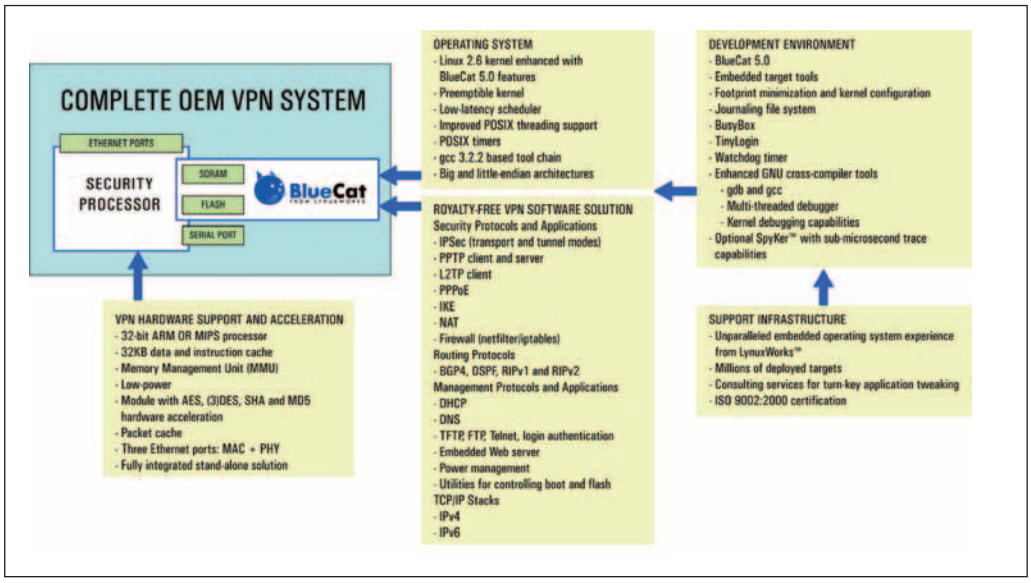

Fig. 3 - Caratteristiche di un sistema VPN (Virtual Private Network) sicuro basato su un processore sicuro e sul sistema operativo Linux BlueCat

sicurezza. Dal momento che agisce a livello di rete, è in grado di cifrare pacchetti IP e tutti i protocolli di livello superiore. Lo svantaggio risiede nell'onere sulle prestazioni che introduce e la complessità di implementazione.
I protocolli Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) e Robust Security Network (RSN) garantiscono la sicurezza a livello di connessione per le reti wireless, impedendo l'accesso in assenza di un'adeguata autenticazione. Lo schema WEP è stata la prima implementazione per la sicurezza per le reti wireless e presenta molte limitazioni significative. Il più recente protocollo WPA è un sottoinsieme delle specifiche IEEE 802.11i per la sicurezza per le reti wireless: è molto più robusto e offre un grado superiore di sicurezza per i punti di accesso e per i client delle reti wireless, pur mantenendo il supporto alle soluzioni legacy. Il protocollo RSN è anch'esso parte delle specifiche IEEE 802.11i e costituisce una soluzione più efficiente, che richiede tuttavia implementazioni hardware del tutto nuove. Le funzioni per la sicurezza wireless sono ancora in fase di evoluzione e le limitazioni e i vantaggi relativi di questi protocolli diventeranno più evidenti quando tali funzioni saranno ampiamente adottate.
La sicurezza totale può essere ottenuta solo se esistono funzionalità adeguate per la sicurezza a tutti i livelli del software di un sistema embedded, compreso il sistema operativo, lo strato middleware e le applicazioni. È indispensabile che durante il progetto di un sistema embedded i progettisti di sistemi embedded tengano in considerazione i compromessi necessari per mettere a punto questi meccanismi per la sicurezza.

Campi di applicazione e sviluppi futuri

Dato che la necessità di sicurezza per le informazioni sta crescendo, esistono numerose aree di applicazione in cui gli stack embedded per la sicurezza diventeranno indispensabili. Fra queste una delle più importanti è senza dubbio quella militare. L'uso di alta tecnologia sta diventando molto comune nei combattimenti, e mantenere le comunicazioni sicure è un fattore essenziale per la sopravvivenza. L'infrastruttura per le comunicazioni è un'altra applicazione nella quale l'uso dei protocolli per la sicurezza sarà critico. La convergenza delle tecnologie informatiche e per le comunicazioni nelle reti 3G richiedono l'adozione diffusa dei meccanismi per garantire la sicurezza dei questi sistemi di infrastruttura.
I dispositivi embedded stanno diventando sempre più pervasivi e la connettività universale sta diventando un concetto comune: di conseguenza una delle principali sfide nel prossimo futuro consisterà nel garantire lo scambio sicuro di informazioni fra i dispositivi embedded attraverso l'adozione diffusa dei protocolli per la sicurezza.

LynuxWorks (Elesia)
readerservice.it n. 39

Nua Internet Surveys
www.nua.com/surveys/how_many_online/index.html