www.elettronica-plus.it

FIERA MILANO MEDIA

EMBEDDED

FEBBRAIO 2018 67

SPECIALE
Le reti industriali scelgono IIoT

LA COPERTINA di EMBEDDED
EDGE COMPUTING: l'intelligenza di IoT si delocalizza

Supplemento a Elettronica oggi n° 466 - Novembre-Dicembre - In caso di mancato recapito inviare al CMP/CPO di Roserio-Milano per la restituzione al mittente previo pagamento resi

Un concetto innovativo per la sicurezza delle applicazioni IoT e Industry 4.0

Kontron ha sviluppato un approccio olistico alla protezione dei sistemi embedded basato sulla sicurezza a livelli di BIOS, sistema operativo e applicazioni

Norbert Hauser
Vice president Marketing
Kontron

La società di ricerca Gartner ha stimato che entro il 2020 oltre il 50% di tutti i principali processi aziendali saranno in qualche modo connessi a Internet of Things (IoT). La pervasività delle applicazioni IoT, sia nella vita privata sia nelle attività aziendali, comporterà sicuramente requisiti più severi in termini di implementazione in molti settori e campi di applicazione. Tra gli aspetti da tenere in considerazione, vi è senz'altro quello della sicurezza: gli analisti della società di ricerca si aspettano un considerevole incremento della spesa in questo comparto e prevedono che la quota del budget per la sicurezza finalizzata alla protezione della tecnologia operativa (OT – Operational Technology) e della tecnologia informatica (IT – Information Technology) crescerà dall'1% attuale a non meno del 20% entro il 2020.
Aziende, Enti e Organizzazioni devono tenere in considerazione non solo i vantaggi di tecnologie quali Internet of Things, Industry 4.0, Smart Home e così via, ma anche i rischi connessi. I produttori di componenti dovranno quindi adeguarsi realizzando sistemi e soluzioni economiche e di semplice implementazione per la minimizzazione dei rischi.

Il concetto di sistemi sicuri secondo Kontron

In base a queste considerazioni Kontron, verso la fine del 2016, aveva già introdotto la sua prima soluzione, espressamente ideata per proteggere i dispositivi terminali utilizzati in applicazioni industriali. Da allora APPROTECT, la soluzione per la sicurezza della società, è una funzionalità standard di tutti i prodotti di Kontron, mentre una parte dei componenti già implementati può essere aggiornata in modo semplice. APPROTECT è ora diventata una delle basi del concetto di "Kontron Secure Systems" basato su tre livelli introdotto all'inizio del 2017. Esso garantisce la sicurezza completa del dispositivo terminale – dall'acquisizione dei dati alla trasmissione verso il gateway, dall'avvio del dispositivo all'esecuzione dell'applicazione fino al completamento del backup. Kontron è perfettamente consapevole delle problematiche connesse alla protezione dei dispositivi terminali nelle applicazioni IoT e IIoT (IoT industriale). Il concetto di sistema sicuro di Kontron si basa su tre concetti base: protezione del BIOS, del sistema operativo e delle applicazioni con i loro dati. Questo concetto è stato sviluppato per implementare la visione di Kontron di sistemi embedded sicuri. Esso viene utilizzato per proteggere tre livelli essenziali dei sistemi degli utilizzatori in modo che questi ultimi non debbano più preoccuparsi della sicurezza dei loro dati, permettendo loro di concentrare l'attenzione sul loro "core business" e competere con successo su scala internazionale.

Proteggere i dispositivi terminali dal codice dannoso

Kontron fa ricorso a standard consolidati per la protezione del BIOS. Aggiornamenti sicuri del firmware e il modulo TPM (Trusted Platform Module) 2.0 assicurano che durante l'avvio siano fatti girare solamente i programmi precedentemente verificati e firmati. Codici non autorizzati e quindi potenzialmente dannosi che potrebbero essere usati per manipolare un dispositivo terminale sono semplicemente ignorati. Non è quindi più possibile apportare modifiche indesiderate al BIOS o al boot loader (ovvero al programma che nella fase di avvio carica

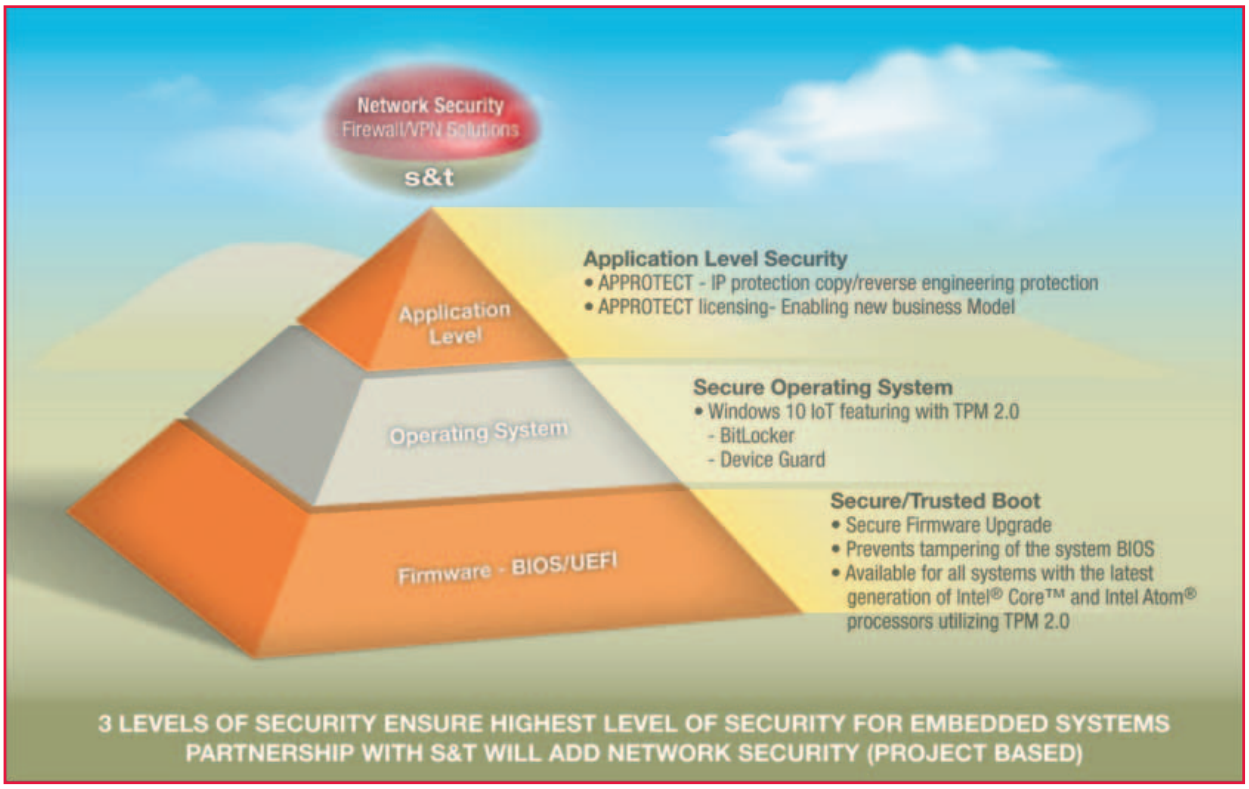

Fig. 1 – La piramide per la sicurezza a tre livelli di Kontron basata per sistemi embedded e IoT garantisce una protezione completa, dalla procedura di avvio ai dati dell'applicazione

il kernel del sistema operativo dalla memoria secondaria a quella primaria). Oltre a ciò il boot sicuro/fidato di Kontron non solo assicura la protezione a livello di BIOS ma consente anche di far girare un sistema operativo sicuro.

Protezione del sistema operativo durante le fasi di start-up e shutdown

Come sistema operativo sicuro Kontron ha deciso di utilizzare Windows 10 IoT, una versione di Windows 10 espressamente ottimizzata per applicazioni IoT. Esso garantisce una protezione completa del sistema e dei dati aziendali che elabora. La combinazione tra funzioni di sicurezza quali Secure Boot, BitLocker, Device Guard e Credential Guard e il chip TPM 2.0 è in grado di respingere in maniera efficace eventuali attacchi durante le fasi di avvio e di arresto.

Protezione dei dati e delle applicazioni con APPROTECT

La soluzione di sicurezza "Kontron APPROTECT – powered by Wibu" protegge il livello applicativo: si tratta di un chip smartcard che, attraverso la cifratura effettuata sui sistemi hardware di Kontron, garantisce la sicurezza dei dati dell'applicazione e del codice del programma. Kontron prevede l'integrazione del chip fornito dal suo partner Wibu-Systems in tutti i nuovi moduli e schede madri. Gli utenti possono scegliere se attivare la funzione di sicurezza, mentre è disponibile un aggiornamento che permette di equipaggiare con questo chip i sistemi meno recenti. Il codice binario dell'applicazione è cifrato in modo da rendere impossibile l'operazione di reverse engineering, la semplice riproduzione del programma (protezione dell'IP). Oltre a ciò, il monitoraggio continuo della cifratura garantisce che l'applicazione venga eseguita solo sui dispositivi cui è destinata (protezione contro la copia).

Per Kontron la sicurezza informatica nell'ambito delle applicazioni IoT è un elemento centrale delle strategie per la digitalizzazione dei clienti ed è fornita di serie in tutti i prodotti della società. Una base hardware che integri per default meccanismi di sicurezza semplifica notevolmente i processi di realizzazione delle applicazioni IoT rendendo da un lato un più efficiente lo sviluppo dei prodotti e consentendo dall'altro di implementare prodotti in grado di supportare future evoluzioni. Questa soluzione può

Fig. 2 – Il modulo COMe-cSL6 di Kontron garantisce per default la sicurezza delle applicazioni IoT in quanto supporta la "Embedded Security Solution" della società grazie all'integrazione del chip per la sicurezza di Wibu

essere aggiunta anche ai sistemi esistenti sfruttando kit di aggiornamento basati su moduli mPCIe o chiavette USB.

APPROTECT: uno sguardo in profondità

Nello sviluppo di APPROTECT, l'idea di base è stata quella di suddividere il complesso processo di protezione di un dispositivo terminale in diverse parti che possono abbinate in funzione delle singole esigenze. Ciò consente di soddisfare requisiti di sicurezza specifici senza per questo sottrarre risorse. Gli utenti non sono quindi costretti a effettuare investimenti di notevole entità per proteggersi contro un numero pressoché infinito di possibili minacce, molte delle quali destinate a rimanere nel campo delle ipotesi.

Il chip per la sicurezza proposto da Wibu incluso nella soluzione per la sicurezza APPROTECT di Kontron prevede un meccanismo di controllo che esegue la verifica della cifratura dell'applicazione in modo da assicurare che il programma sia eseguito solamente sui dispositivi ai quali è effettivamente destinato. La comunicazione su base continuativa con il chip che decifra le diverse parti dell'applicazione durante il funzionamento impedisce che i dati dell'applicazione vengano letti (ovvero prelevati) dalla memoria. In questo modo Kontron è in grado di garantire la protezione dell'applicazione senza oneri di compilazione aggiuntivi o complicati processi di gestione di chiavi. Le modalità di commercializzazione della licenza di APPROTECT messe a punto da Kontron permettono di implementare nuovi modelli di business. L'accesso alle singole funzioni dell'applicazione può, ad esempio, essere limitato a un certo periodo di tempo o a un determinato numero di sequenze di avvio (boot). Una modalità di questo tipo può essere utile ad esempio nelle applicazioni di test e può dar spazio a nuove idee di utilizzo, limitate solo dalla creatività.

Kontron e S&T: una collaborazione finalizzata alla sicurezza

La fusione con il gruppo S&T, completata nel mese di agosto del 2017, ha contribuito a rafforzare le competenze di Kontron nel settore della sicurezza. Gli utenti possono ora disporre un ampio portafoglio di soluzioni nei settori dei moduli embedded, schede e sistemi, IoT e Industry 4.0 tutte raggruppate sotto il marchio Kontron. Un folto gruppo composto da circa 2.300 specialisti nell'ambito IT e OT stanno lavorando sullo sviluppo di soluzioni che permetteranno di connettere in modo semplice e sicuro sistemi embedded con un cloud pubblico o embedded.

Dopo la fusione con S&T, la sicurezza embedded è diventata uno dei capisaldi della strategia aziendale. In questo nuovo contesto Kontron è stata in grado di migliorare le proprie capacità di assicurare la sicurezza di dati e applicazioni. Ciò è dovuto sia al gran numero di specialisti che lavorano allo sviluppo di soluzioni per la sicurezza sia alla capacità dell'azienda di proporsi come fornitore unico per una gamma sempre più ampia di componenti. Kontron ha creato un'infrastruttura coerente per i propri clienti che è compatibile con tutte le interfacce. In questo modo è possibile innalzare il livello di sicurezza a fronte di oneri di implementazione veramente minimi.

"La sicurezza è la carta vincente per conquistare la fiducia degli utilizzatori in tutte le applicazioni che riguardano la tecnologia operativa" – ha detto Norbert Hauser, vice president Marketing di Kontron. "Ciò è vero per la tecnologia già disponibile ma ancor più sia per le nuove applicazioni che riguardano IoT, Smart Factory o Industry 4.0, sia per altri settori come quello medicale. Le aziende sfrutteranno le nuove possibilità che si prospettano solamente se avranno fiducia in esse".