Reti da proteggere

Le trasmissioni via radio sono di per sè soggette a intercettazioni, proteggersi è dunque essenziale

Fonte: www.jkcustomnetwoks.com

Stefano Cazzani

È un dato di fatto: quando si trasmette il dato via radio l'informazione è a disposizione di chiunque sappia e/o voglia ascoltare. Come proteggersi allora da 'orecchie' e 'occhi' indesiderati senza per questo rinunciare a tutti i benefici offerti dall'utilizzo delle reti wireless in ambito industriale? La risposta non può essere univoca, ma il primo passo indispensabile è rendersi conto che il problema esiste e che non va sottovalutato. Se non si è disposti ad affrontarlo, tanto vale lasciare perdere per evitare brutte sorprese. Per fortuna, però, oggi le soluzioni tecnologiche atte a mitigare i rischi e realizzare sistemi di comunicazione affidabili esistono, per cui le reti di comunicazione radio meritano di essere considerate a pieno titolo tra le alternative a disposizione dei progettisti di reti per ambiente industriale.

Le minacce

Le tipologie di minaccia appartengono principalmente a due grandi gruppi: intercettazione dei dati da parte di utenti non autorizzati oppure intralcio intenzionale ai dati in arrivo, per impedire la comunicazione o, peggio, alterarne il contenuto. Le possibilità di ascolto non autorizzato sono fortemente influenzate dalla 'copertura' della rete. È infatti praticamente impossibile 'confinare' un segnale radio all'interno della zona alla quale è destinato, per esempio un capannone, per cui è inevitabile che possa essere ricevuto anche all'esterno. Per mitigare il rischio di ascolti indesiderati, la prima regola è limitare la potenza dei trasmettitori allo stretto necessario per garantire comunicazioni affidabili. Ogni eccesso è inutile e allarga potenzialmente l'area utile per chi volesse captare i segnali. La tecnica fondamentale per garantire la riservatezza e l'integrità delle comunicazioni consiste però nella crittografia o cifratura dei dati, ossia nel codificare mediante codici 'segreti' tutte le informazioni, che diventano così non-intellegibili da parte di chi non possiede le relative chiavi di cifratura.

Come in guerra, le tecniche di crittografia sono tantissime e costituiscono una sfida intellettuale sempre attuale tra chi le progetta e chi cerca di neutralizzarle. Per utilizzare una rete wireless in ambito industriale, quindi, non solo è indispensabile impiegare apparati dotati delle tecniche di cifratura e protezione al momento più sicure, ma anche assicurarsi che nel corso della vita operativa della rete, tipicamente molti anni, vengano effettuati tutti gli aggiornamenti d'obbligo per mantenere un grado di sicurezza confacente.

La rete diventa 'sorda'

Una minaccia troppo spesso sottovalutata, alla quale vanno incontro le reti radio, è il cosiddetto 'jamming', ossia la presenza di un segnale interferente di forte potenza sulla stessa banda impiegata per la comunicazione, che viene intenzionalmente emesso da un trasmettitore 'maligno' oppure dovuta a un guasto inaspettato a un'apparecchiatura elettronica. Di fatto questo rende 'sorda' l'intera rete. Le tecniche

INSIEME PER SAPERNE DI PIÙ

*La consapevolezza, la formazione, il continuo aggiornamento professionale e lo scambio di informazioni sono gli strumenti più efficaci per affrontare razionalmente il problema della sicurezza delle reti informatiche. In Italia esiste dal 2000 l'associazione Clusit (**www.clusit.it**), nata per affrontare queste tematiche in modo professionale. Tra gli obiettivi primari dell'associazione vi è la diffusione a tutti i livelli della sicurezza informatica, la partecipazione all'elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello comunitario che italiano, la formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza ICT e la promozione dell'utilizzo di metodologie e tecnologie che consentano di migliorare il livello di sicurezza in varie realtà applicative, tra cui il mondo industriale.*


Punto di accesso Wifi per ambiente industriale

Fonte: Siemens

tata di mano un analizzatore di spettro, qualora sorga anche solo il dubbio che il degrado delle prestazioni della rete possa essere dovuto alla presenza di potenti trasmettitori indesiderati.

di jamming costituiscono le munizioni tipiche della 'guerra elettronica' e sono oggi utilizzate non solo nelle operazioni militari, ma anche durante manifestazioni ed eventi particolari, dove si vuole impedire il corretto funzionamento delle comunicazioni radio, per esempio dei cellulari, per esigenze di ordine pubblico.

Senza necessariamente pensare a scenari alla James Bond, un'attività di jamming può verificarsi anche all'interno di un ambiente industriale. Il più delle volte è semplicemente il risultato di un guasto o di un'errata taratura di altre apparecchiature che niente hanno a che fare con la rete di comunicazione. In sostanza, il più delle volte si tratta di una degenerazione dei fenomeni d'interferenza elettromagnetica, che fanno parte della quotidianità di ogni sistema elettrico. Anche un semplice dispositivo elettronico malfunzionante può diventare un assordante emettitore di onde elettromagnetiche a radiofrequenza, che, se sufficientemente potenti a causa della loro vicinanza e se ricadono nella stessa banda di utilizzo di una rete wireless, possono addirittura paralizzare la comunicazione. Per mitigare il rischio, le moderne tecnologie wireless sfruttano modulazioni digitali a banda larga a spettro disperso o a salto di frequenza, proprio per evitare che un forte disturbo su una singola frequenza paralizzi la rete, ma il fenomeno dei disturbi indesiderati è comunque sempre in agguato. Pertanto, vale la pena tenere a portata di mano un analizzatore di spettro, qualora sorga anche solo il dubbio che il degrado delle prestazioni della rete possa essere dovuto alla presenza di potenti trasmettitori indesiderati.

La cattiva fama del Wifi

Un caso emblematico di falle nella sicurezza è rappresentato dalle reti Wifi, diffuse ormai ovunque, anche in svariate applicazioni industriali. La prima generazione (e non solo) di prodotti per le comunicazioni wireless a standard Wifi supportavano solamente un algoritmo di cifratura, detto WEP, rivelatosi inefficace, tanto che oggi in pochi minuti con strumenti alla portata di tutti (basta un notebook) è possibile decodificare e accedere a reti Wifi apparentemente protette dall'algoritmo WEP.

L'industria è corsa ai ripari e nel corso degli anni sono stati sviluppati algoritmi di cifratura e protezione più potenti e difficili da violare, oggi a disposizione nella maggior parte degli apparati di ultima generazione.

In particolare, lo standard di crittografia più recente per il Wifi è definito nelle norme Ieee 802.11i ed è noto come WPA2. È basato sull'algoritmo di cifratura a blocchi AES (Advanced Encryption Standard) e su vari nuovi meccanismi di scambio delle chiavi segrete. Dovendo però mantenere la compatibilità con gli apparati delle generazioni precedenti, i prodotti Wifi moderni supportano comunque tanti metodi di protezione, tra cui il vecchio WEP. Attenzione quindi a configurare correttamente tutti gli apparati che si utilizzano, optando sempre per il tipo di crittografia più sicura e sostituendo i prodotti obsoleti, che non sono aggiornabili alle ultime versioni degli standard di sicurezza.

MVK PROFINET

Il modulo I/O resistente

MVK Metallico è la risposta ottimale per l'installazione su macchine utensili in condizioni estreme.

Con Profinet potete contare sui vantaggi dell'innovazione per un'installazione di macchina all'avanguardia!

PROFINET INDUSTRIAL ETHERNET

Murrelektronik S.r.l.
Tel. +39 39 673167
info@murrelektronik.it
www.murrelektronik.it
readerservice.it n.25377

MURR ELEKTRONIK
stay connected

STRUMENTI DEL MESTIERE

- L'analizzatore di spettro

Come si vedono le onde radio? Lo strumento principe è l'analizzatore di spettro, ossia un radioricevitore di misura specializzato, in grado di mostrare in tempo reale lo spettro di frequenze radioelettriche, indicando per ciascuna di esse la potenza emessa. In altre parole, con l'analizzatore di spettro si ottiene una 'mappa' in frequenza di ciò che viene trasmesso nell'etere.

Il primo passo per identificare eventuali sorgenti di interferenze o di emissioni disturbanti è proprio quello di capirne la banda o frequenza di emissione. Inoltre, ogni tipo di sorgente emittente è caratterizzata da una 'forma' tipica dello spettro in frequenza, determinata dal tipo di modulazione utilizzata nella trasmissione. Osservando frequenza e forma dello spettro, dunque, è possibile ipotizzare la presenza di segnali non desiderati e identificarne il tipo. Pertanto, chi decide di utilizzare una rete wireless farebbe bene ad attrezzarsi con un analizzatore di spettro adatto a captare i segnali sulla banda di frequenze occupata dalla propria rete, per esempio 900 MHz e 2,4 GHz per Zigbee, 2,4 GHz e 5 GHz per Wifi. Il primo passo è farsi un'idea dell'occupazione dello spettro in condizioni normali, per avere un punto di riferimento qualora si notassero successivamente malfunzionamenti o degradi delle prestazioni, che facciano pensare alla presenza di radiotrasmittenti non desiderate.

Un analizzatore di spettro portatile è uno strumento che non dovrebbe mai mancare tra gli attrezzi a disposizione di chi gestisce una rete di comunicazione wireless

- Software di attacco

Uno dei metodi base per capire se una 'porta' resiste alle intrusioni è metterla alla prova utilizzando gli strumenti tipici di chi vuol fare l'intruso. E proprio come per verificare la solidità di una serratura è normale provare a forzarla con un comune grimaldello, per verificare che la rete wireless sia opportunamente protetta è possibile utilizzare vari strumenti software di pubblico dominio, che provano ad attaccarla. La maggior parte dei programmi di utilità che provano a forzare una rete sono disponibili in ambiente Linux, il più delle volte anche nella forma open source. Una della più note 'cassette degli attrezzi' per questo tipo di attività è costituita da una particolare distribuzione Linux pronta all'uso, utilizzabile anche sui comuni PC eseguendo la procedura di avvio direttamente da CD. Si trova anche sul sito ***www.backtrack.it****, una destinazione molto frequentata dai professionisti italiani della sicurezza.*

Uno dei tanti software disponibili per l'analisi in tempo reale delle reti wireless per identificare nodi sospetti

Quanto è sicuro Zigbee?

Nato per favorire lo scambio di dati su brevi distanze, quindi particolarmente adatto alle applicazioni industriali, lo standard Zigbee e i relativi protocolli di comunicazione di base definiti in Ieee 802.15.4 hanno sin dal principio cercato di contemplare l'utilizzo di scambi di informazioni protetti. La sfida in questo caso è data dalla tipologia dei prodotti, generalmente pensati per essere minuscoli e a basso consumo, pertanto equipaggiati con microcontrollori piuttosto semplici, che non possono farsi carico di operazioni crittografiche computazionalmente complesse. Forse anche alla luce degli errori scontati dalle prime versioni di Wifi, gli sviluppatori dei protocolli Zigbee hanno optato fin da subito per l'utilizzo di sistemi di crittografia più affidabili, come AES, che possono essere opzionalmente attivati nelle rete Zigbee. Rimane però il problema di garantire all'interno di una struttura così flessibile e per certi versi autoconfigurante, come quella di Zigbee, lo scambio sicuro delle chiavi crittografiche tra i nodi che devono scambiarsi dati. Inoltre, è stato necessario definire regole di accesso alla rete, il cui rispetto e imposizione è demandato a un dispositivo particolare, denominato 'trust center' o coordinator, che ha il compito di ammettere alla rete Zigbee i dispositivi autorizzati, consegnando loro di volta in volta le chiavi crittografiche necessarie. Anche in questo caso, la tecnologia si è evoluta, e si evolve tuttora, in quanto i requisiti di sicurezza e il conseguente livello di complessità infrastrutturale necessario varia molto in funzione delle applicazioni. Vale dunque sempre il suggerimento di valutare attentamente a priori le funzionalità di sicurezza di un qualunque nodo Zigbee, evitando di dimenticarsi di utilizzare sempre il livello di sicurezza massimo consentito e, soprattutto, di non dimenticarsi di tenere aggiornato nel tempo il firmware dei nodi, in base all'evoluzione dei criteri di sicurezza. ■