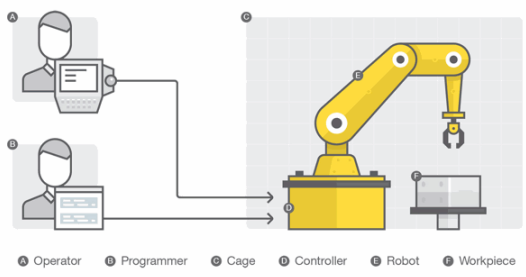
Polimerica
Attualità e notizie dal mondo della plastica

Robot industriali vulnerabili?

Una ricerca del Politecnico di Milano e Trend Micro FTR mette in luce i rischi di attacchi informatici e gli strumenti per combatterli.

21 giugno 2017 07:18

Dopo PC e server, il prossimo obiettivo dei criminali informatici potrebbero essere i robot industriali, sabotati a distanza o presi in ostaggio, in attesa del pagamento di un riscatto, come oggi avviene per i sistemi informatici aziendali. Secondo uno studio realizzato in collaborazione tra Politecnico di Milano e Trend Micro FTR, "*Rogue Robots: Testing the Limits of an Industrial Robot's Security*", i robot industriali possono essere compromessi, alterando in maniera decisiva la normale funzionalità dei sistemi industriali e minando la sicurezza del personale e dei consumatori finali.



RISCHI PER INDUSTRIA 4.0. Secondo alcune stime, l'anno prossimo saranno 1,3 milioni i robot in funzione nelle fabbriche di tutto il mondo, con un trend in costante crescita per supportare l'Industry 4.0, una nuova era di innovazione che automatizza e rende più intelligenti le fabbriche.
Il report rivela che nel momento in cui questi sistemi diventano sempre più intelligenti e interconnessi, cresce la loro superficie di attacco. Ad esempio - segnalano i ricercatori - opportuni servizi web permettono a software o dispositivi esterni di comunicare con i robot attraverso richieste HTTP, mentre nuove APIs permettono agli esseri umani di controllare i robot attraverso app per gli smartphone. Anche app store dedicati ai robot hanno cominciato a diffondersi.
Questo nuovo ecosistema è composto però da software obsoleti, basato su sistemi operativi vulnerabili e librerie non sempre aggiornate, scarso o scorretto utilizzo di crittografia, sistemi di autenticazione deboli, con credenziali predefinite che non possono essere cambiate facilmente. Alcuni robot possono addirittura essere raggiunti direttamente da Internet, per il monitoraggio e la manutenzione a distanza. Come se non bastasse - aggiungono gli estensori dello studio -, i robot sono progettati per interagire sempre più a stretto contatto con gli esseri umani e questo aumenta la possibilità di causare danni fisici agli operatori che lavorano con i robot.

CASO DI STUDIO. È stato anche esaminato approfonditamente un caso reale, per mostrare come sia possibile attaccare un robot industriale. I ricercatori del Politecnico in collaborazione con Trend Micro hanno trovato diverse vulnerabilità, tra cui: servizi di rete senza protezione, bug di "command injection" che permettono a un aggressore di eseguire comandi arbitrari sul computer che controlla un robot, scarso o scorretto utilizzo di crittografia, bug di "memory

corruption” che permettono a un aggressore di controllare il codice macchina in esecuzione, mancanza di controllo d’integrità e autenticazione del codice e scarso o assente isolamento dei processi.
Combinando queste vulnerabilità, i ricercatori hanno dimostrato l’esistenza di cinque attacchi specifici dei sistemi robotici industriali, che vanno ad esempio dalla violazione dei minimi requisiti di sicurezza fisica, fino all’introduzione di micro difetti negli oggetti manipolati dal robot.

A CHE SCOPO? I robot rappresentano un elemento sempre più critico del nostro tessuto industriale. Ciò li rende un bersaglio potenziale sia per gruppi cybercriminali in cerca di guadagno, sia per stati che vogliono colpire l’operatività di un avversario. Gli scenari sono svariati: creazione di danni fisici, sabotaggio di prodotti, esfiltrazione di segreti industriali, fino alle richieste di riscatto avanzate dall’aggressore in cambio di rivelare in quali unità di prodotto sono stati introdotti micro-difetti (per esempio automobili, aerei, medicinali).
Per tutelarsi è necessario un approccio e uno sforzo olistico che richiede il sostegno e la partecipazione di tutti gli stakeholder, inclusi i vendor di security e gli sviluppatori di software e questo va oltre il migliorare semplicemente la qualità dei software embedded.

Scarica la ricerca “Rogue Robots: Testing the Limits of an Industrial Robot’s Security”