Nuovi sensori di rilevamento per aiutare le ferrovie a far fronte agli attacchi EM

Virginie Deniau, coordinatrice del progetto SECRET, parla dei dispositivi sviluppati dalla sua equipe per identificare gli attacchi elettromagnetici (EM) nel momento in cui avvengono, in modo che gli operatori possano passare a una modalità ferroviaria sicura.

Undici anni fa, l'attentato ai treni di Madrid ha dimostrato quanto la sicurezza delle ferrovie europee avesse bisogno di essere rafforzata. Ma adesso che le attrezzature ferroviarie – come nella maggior parte degli altri settori – sono sempre più standardizzate e connesse, emergono nuovi tipi di attacchi più insidiosi: gli attacchi elettromagnetici (EM). Un progetto finanziato dall'UE ha sviluppato tecnologie di rilevamento che possono aiutare il settore a fronteggiare questa nuova minaccia.

Lo sapevate che presto ci saranno tanti dispositivi connessi quanti sono gli esseri umani sulla Terra? Cinque miliardi di questi dispositivi sono adesso in uso e questo numero è destinato a raggiungere i 25 miliardi nel 2020. Sicuramente ogni tipo di dispositivo connesso ci porta un passo più vicino all'avvento delle città intelligenti e di tutti i benefici previsti. Dall'altra parte però, come hanno mostrato le prime pagine di recente, rende gli hacker e altri esperti di tecnologia con cattive intenzioni una minaccia sempre più grande per la sicurezza.

Nel settore europeo delle ferrovie per esempio, l'omogeneizzazione delle tecnologie di rete e l'aumento dell'uso di comunicazioni wireless hanno reso la possibilità di un attacco EM molto probabile. I jammer delle comunicazioni sono facili da usare ed è possibile acquistarli senza restrizioni su internet, il che significa che le comunicazioni potrebbero essere disturbate, i treni ritardati, bloccati o persino dirottati.

Per preparare il settore a questa nuova minaccia, il progetto SECRET ("SECurity of Railways against Electromagnetic aTtacks") ha sviluppato un set di sensori di rilevamento in grado di identificare attacchi EM nel momento in cui si verificano, in modo che gli operatori ferroviari possono smistare la rete in una "modalità sicura" immune allo specifico tipo di attacco EM perpetrato.

Virginie Deniau, coordinatrice di SECRET, ci parla delle probabilità di un attacco EM, dei dispositivi sviluppati dalla sua equipe e di come il settore presto dovrà adattarsi a questa nuova realtà.

Quanto crede siano possibili gli attacchi EM?

La definizione di un attacco EM si evolve con la moltitudine delle applicazioni basate sulle tecnologie di comunicazione wireless. In passato, gli attacchi EM si basavano sulla generazione di interferenze intenzionali ad alta potenza (impulsi elettromagnetici o microonde ad alta potenza) in grado di disturbare o danneggiare le attrezzature elettroniche. Oggi, le funzioni di queste attrezzature possono essere attivate da un commando o un'informazione trasmessi da collegamenti wireless, il che significa che adesso è più facile disturbare le informazioni trasmesse e danneggiare le attrezzature. Tali attacchi richiedono un segnale meno potente che si può generare con telefoni cellulari e altri dispositivi di piccole dimensioni.
Dal punto di vista tecnologico quindi, le probabilità di un attacco aumentano con la vulnerabilità delle infrastrutture. È difficile però stabilire una probabilità chiara perché oggi è impossibile distinguere un guasto tecnico da un attacco EM. Gli attacchi EM basati su un segnale di potenza relativamente "bassa" causano interruzioni ma non danni permanenti.

Ha menzionato i dispositivi mobili. Significa forse che chiunque potrebbe in teoria perpetrare questo tipo di attacchi?

La conoscenza dell'obiettivo è essenziale per definire i mezzi necessari per fare un attacco EM. Oggi i jammer della comunicazione pubblica possono essere acquistati facilmente sul mercato pubblico ma il loro potere e la loro azione sono limitati. Adesso se consideriamo i servizi professionali o di sicurezza, sono necessari generalmente dispositivi specifici per questi attacchi. Questi dispositivi sono normalmente limitati al mercato professionale o devono essere sviluppati partendo da zero. Anche se è possibile, per farlo è necessario un certo livello di abilità e conoscenza.
Quando queste applicazioni professionali però si basano su servizi wireless pubblici, possono essere disturbati da jammer comuni. Sta emergendo quindi un problema reale e la sicurezza e la criticità dei servizi wireless devono essere prese seriamente in considerazione.

SECRET si occupa in particolare di sicurezza delle ferrovie. Quali potrebbero essere

le conseguenze degli attacchi EM in questo settore?

Il principale rischio diretto è una perturbazione del traffico della rete ferroviaria. Potrebbe essere possibile impedire la partenza di treni, obbligare i treni a fermarsi e causare significative perdite finanziarie e situazioni difficili da gestire. È difficile però stimare con precisione i rischi conseguenti perché dipendono dalle caratteristiche delle singole reti ferroviarie (sfruttamento, infrastruttura, applicazioni, ecc.).

Può parlarci degli strumenti che avete sviluppato?

La visione di SECRET è che se siamo in grado di rilevare un attacco EM con certezza, possiamo pensare di passare a una modalità ferroviaria sicura perfettamente adattata alla situazione e che permette agli operatori di riacquistare il controllo. La sfida quindi è sviluppare soluzioni di rilevamento veloci e affidabili. Tenendo a mente questo sono state studiate diverse soluzioni nell'ambito di SECRET. Alcune potrebbero essere implementate direttamente nei terminal di comunicazione e altre avranno bisogno di dispositivi dedicati ma offrono il vantaggio di essere in grado di monitorare più di un collegamento di comunicazione.
Per ottenere la resilienza, i nostri sensori di rilevamento sono stati associati a un terminal di acquisizione e decisione che è stato incaricato di analizzare i risultati di questi sensori di rilevamento e di comandare una piattaforma di telecomunicazioni riconfigurabile. Secondo i risultati dei sensori, il terminale responsabile delle decisioni indirizza i messaggi da trasmettere verso il collegamento di comunicazione che è più resistente agli attacchi EM. Ovviamente, un tale approccio richiede lo sviluppo di diverse reti di comunicazione.

Quando vedremo la tecnologia di SECRET sul mercato?

A causa della mobilità e dell'ampio spettro degli ambienti ferroviari elettromagnetici, la robustezza e l'assenza totale di errore delle soluzioni di rilevamento è difficile da dimostrare a bordo di un treno. Quando il treno non si muove però, le tecnologie di SECRET possono essere molto efficienti. Possiamo quindi prevedere di arrivare sul mercato relativamente presto con queste tecnologie per proteggere le stazioni ferroviarie o altre infrastrutture critiche.
Parallelamente, le tecnologie di SECRET possono contribuire all'evoluzione degli standard di telecomunicazioni usati nelle infrastrutture critiche. Invece di migliorare le prestazioni in termini di velocità dei dati, gli standard possono evolversi fino a fornire informazioni in tempo reale sulla qualità dei servizi o la presenza di segnali di disturbo (intenzionali o non intenzionali). Potrebbero quindi offrire la diagnostica necessaria e attivare un processo di intervento adeguato.

Le ferrovie europee sono già sotto pressione dal punto di vista economico e di sicurezza. Pensate che il settore possa sopportare gli ulteriori costi che comporterebbe l'implementazione delle soluzioni di SECRET?

Penso che con questa minaccia sempre più importante, sarà necessario garantire la resilienza della rete ferroviaria contro questi attacchi. Generalmente i sistemi di comunicazione wireless rappresentano solo una piccola percentuale del budget di un progetto ferroviario. Questi sistemi però sono essenziali nei piani operativi e di sicurezza. Gli attacchi EM possono avere conseguenze drammatiche in termini di costi e se sono facili da mettere in atto possono diventare frequenti. Una soluzione contro gli attacchi EM dovrebbe essere presa in considerazione equilibrando allo stesso tempo i rischi, gli impatti e gli investimenti.

Quali sono i vostri piani adesso che il progetto sta per concludersi?

Ci piacerebbe testare la nostra analisi degli attacchi EM con altri tipi di attacchi come quelli fisici o altri tipi di attacchi cibernetici. In effetti gli attacchi di jamming si possono usare facilmente a sostegno di altre azioni criminali per evitare la trasmissione di video o allarmi. Di conseguenza, le analisi del rischio devono prendere in considerazione eventuali attacchi fisici e di jamming associati. Pensiamo anche che l'architettura di rilevamento per gli attacchi EM proposta da SECRET dovrebbe essere associata ad altri strumenti di monitoraggio per l'infrastruttura in modo da avere un'idea migliore di quello che succede sulla rete in tempo reale.

Per ulteriori informazioni, visitare:

SECRET
http://www.secret-project.eu/

Paesi

Francia

Progetti correlati

ARCHIVED

SECurity of Railways against Electromagnetic aTtacks

SECRET

12 Settembre 2016

PROGETTO

Questo articolo è contenuto in...

RIVISTA RESEARCH*EU

L’incontro tra scienza e sicurezza

Articoli correlati

NUOVI PRODOTTI E TECNOLOGIE

Nuovi strumenti e metodi per proteggere le infrastrutture critiche d’Europa

19 Maggio 2016

Ultimo aggiornamento: 14 Luglio 2015

Permalink: https://cordis.europa.eu/article/id/117444-new-detection-sensors-can-help-railways-cope-with-em-attacks/it