Cyber Physical Systems

Panoramica sulla sicurezza

Bianca Crippa

Università degli Studi di Bergamo

`https://github.com/Biancolinaa/CPS-presentation.git`

31.05.2021

Argomenti

Cyber Physical Systems

I Cyber Physical Systems (**CPS**) sono una delle innovazioni tecnologiche della quarta rivoluzione industriale.

Sistemi il cui meccanismo è monitorato da algoritmi computer-based. Componenti fisiche e software fortemente interconnesse per operare su diverse scale temporali e spaziali e interagire tra loro in modi differenti in base ai cambiamenti del contesto.

L'insieme di queste tecnologie è in grado di dar vita ad un ulteriore sistema basato sull'**integrazione tra vari soggetti**, posti anche a distanza tra loro. Si fondono insieme conoscenze riguardanti la meccatronica, la cibernetica, il design e la scienza dei processi.

Livelli di funzionalità

Cinque livelli di funzionalità:

- **Smart Connection**: utilizzo di sensori per la gestione dei dati;
- **Data-to-information-connection**: aggregazione e conversione dei dati con aggiunta di eventuali informazioni;
- **Digital Twin**: sintetizzazione del dominio reale nella realtà digitale;
- **Cogniction**: considerazione di tutti gli scenari possibili. Indispensabile per un processo decisionale adeguato;
- **Configuration**: proiettare la realtà virtuale su quella fisica tramite l'invio di feedback.

Tecnologie

Tre tipologie di tecnologie abilitanti:

- **Sensori integrati**: ciascun sistema in pochi secondi riesce a capire la propria situazione operativa e inviare le informazioni relative al proprio stato e alla posizione;
- **Attuatori**: consentono lo svolgimento delle varie azioni senza rischi per rendere ogni processo più performante;
- **Intelligenza decentrata**: elabora gli scenari di scelta per fornire il più rapidamente possibile quello più consigliato.

L'insieme delle tecnologie costituisce il **dominio digitale** che permette alle informazioni di muoversi e garantisce una connessione veloce tra i componenti fisici.

Vantaggi

L'utilizzo dei Cyber Physical Systems può portare a:

- Nuove possibilità di business;
- Digitalizzazione del prodotto;
- Migliore gestione della produzione e delle performance;
- Gestione di impianti, macchinari e attrezzature più semplice;
- Trasferimento di informazioni e conoscenze più veloce.

Argomenti

Attacchi

Gli attacchi ai Cyber Physical Systems sono di tre tipi:

- **Attacchi all'availability del sistema**;
- **Attacchi all'integrità dei dati**: *deception attacks*, rappresentano la classe più ampia di attacchi;
- **Attacchi alla riservatezza**: *disclosure attacks*.

Principali attacchi

I principali attacchi che colpiscono i CPS sono:

- **False data injection**: appartengono ai *deception attacks* e riguardano la stima dello stato. É uno degli attacchi più studiati. L'avversario conosce le informazioni topologiche del sistema e manipola le misurazioni dei sensori per modificare la variabili di stato, baypassando gli schemi di rilevamento dei dati errati.
- **Generic deception**: è un attacco all'integrità dei dati. L'avversario invia false informazioni a uno o più sensori o controllori in modo tale da ingannare un componente compromesso e fargli credere che il falso dato ricevuto sia valido. É modellato come un segnale additivo arbitrario, mandato a sovrascrivere i dati originali.

Principali attacchi

- **Denial of Service (DOS)**: è il più noto tra gli attacchi alla disponibilità. Rende inaccessibili alcuni o tutti i componenti di un sistema di controllo e impedisce la trasmissione dei sensori e del controllo sulla rete.
- **Replay**: fa parte degli attacchi all'integrità dei dati e solitamente viene combinato con un attacco fisico. L'avversario prima raccoglie sequenze di dati di misurazioni o controllo, poi riproduce i dati registrati mentre inietta un segnale esogeno nel sistema. Può non conoscere il modello del sistema per generare un output dannoso ma, conoscendolo, può raggiungere più facilmente il suo obiettivo, come per esempio danneggiare anche fisicamente l'impianto.

Principali attacchi

- **Covert misappropriation**: l'avversario può ottenere il controllo dell'impianto senza essere rilevato dal controllore. Questo attacco richiede alti livelli di conoscenza del sistema e l'abilità dell'avversario di leggere e sostituire i segnali di comunicazione all'interno dell'anello di controllo.
- **Zero dynamic**: l'avversario costruisce una *open-loop policy* in modo tale che il segnale d'attacco non produca output. Gli attacchi sono quindi disaccoppiati dall'uscita dell'impianto e risultano furtivi rispetto ai rilevatori di anomalie arbitrarie.

Principali attacchi

- **Load altering**: possono far cadere la rete o causare danni significativi alla trasmissione della potenza e alle apparecchiature. Consiste nel tentativo di controllare e cambiare (generalmente aumentando) alcuni carichi per danneggiare l'impianto con overflow di circuito o disturbando l'equilibrio tra fornitura di energia e domanda.
- **Load redistribution**: è un tipo speciale di attacchi *false data injection*. Consiste nell'aumentare o nel ridurre il carico su alcuni bus, mantenendo inalterato il carico totale per nascondere l'attacco ai rilevatori. L'attaccante deve conoscere le informazioni topologiche della rete.

Principali attacchi

- **Topology poisoning**: l'avversario altera di nascosto i dati di contatori, interruttori di rete e linea per indurre l'errore nel centro di controllo con una topologia di rete sbagliata.
- **Physical layer**: riguardano gli attacchi all'infrastruttura fisica e alla rete di controllo e non richiedono la conoscenza del modello del sistema.
- **Data framing**: fa parte dei *deception attacks* e riguarda lo stato del sistema di alimentazione e sfrutta i meccanismi per il rilevamento e la rimozione dei dati errati. Intenzionalmente attiva il meccanismo di rilevamento errori e inquadra come fonte di errore dei misuratori che in realtà sono funzionanti, in modo tale che i dati da loro forniti vengano rimossi. In questo modo, lo stato risultante stimato può contenere un errore arbitrariamente grande.

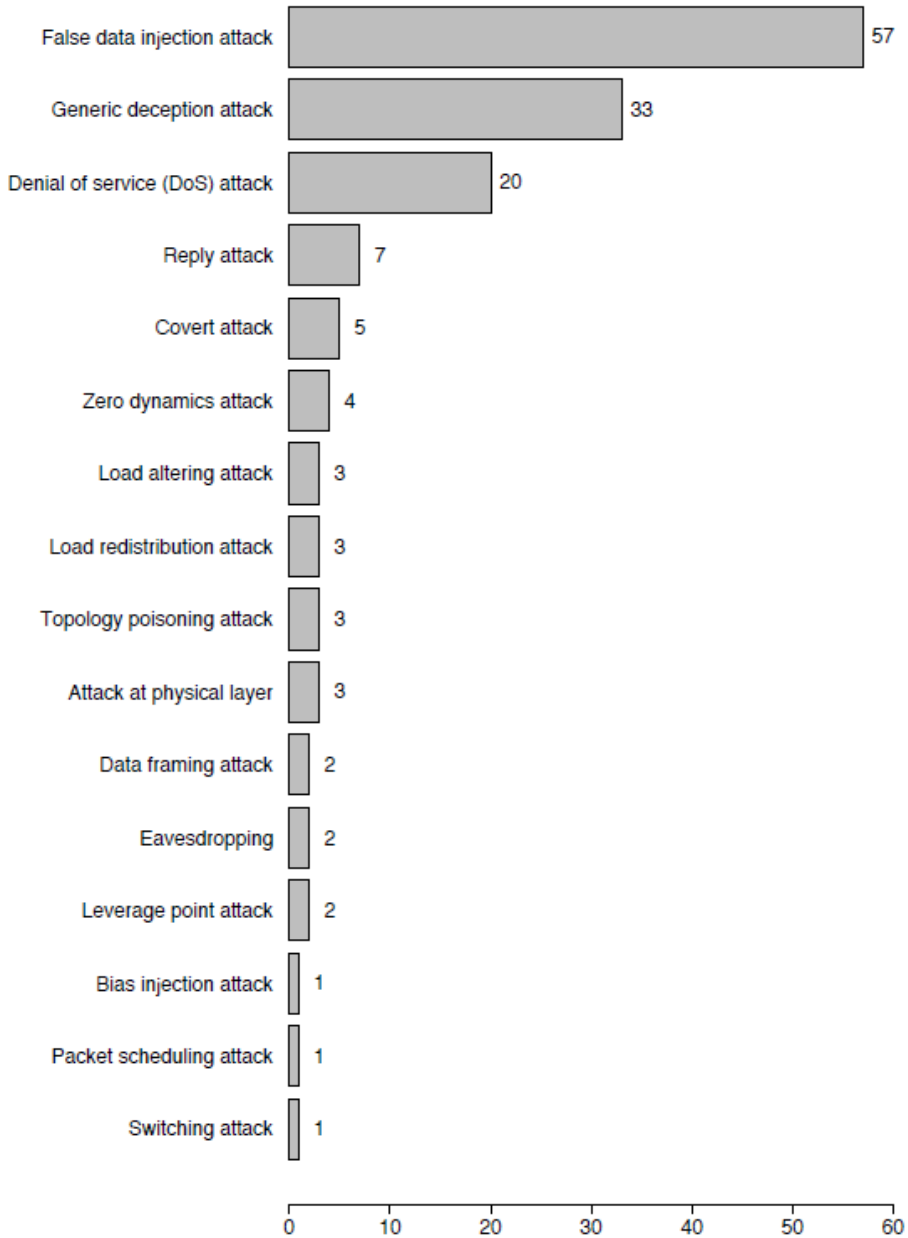
Principali attacchi

- **Leverage point**: fa parte dei *deception attacks* e crea punti di leva all'interno del sistema di alimentazione. Il residuo della misurazione corrispondente al punto di leva è molto piccolo, anche se è contaminato da un errore molto grande. In questo modo l'avversario può introdurre errori nelle misurazioni del contatore senza essere rilevato.
- **Bias injection**: l'avversario introduce un bias costante nel sistema senza essere rilevato. La corruzione dei dati può riguardare sia l'attuatore che il sensore e la quantità di risorse di interruzione deve essere superiore alla soglia di non rilevabilità.

Principali attacchi

- **Packet scheduling**: influenza le caratteristiche temporali della rete perchè si traduce in ritardi variabili nel tempo e pacchetti di dati ricevuti quando il sistema è fuori servizio. L'attaccante non è in grado di ritardare i pacchetti oltre un certo ritardo massimo consentito dal protocollo di rete in uso.
- **Switching**: l'avversario controlla più interruttori di circuito all'interno del sistema di alimentazione e utilizza un modello locale del sistema e le informazioni sullo stato per progettare una sequenza di commutazione dell'interruttore dipendente dallo stato per destabilizzare i generatori sincroni.

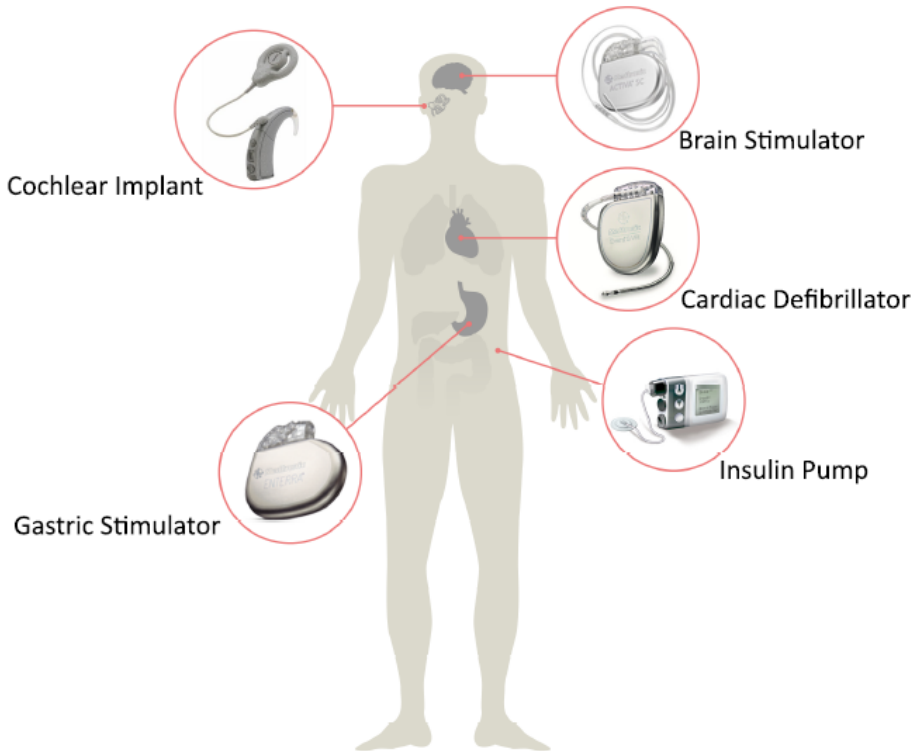
Principali attacchi



Caso di studio: dispositivi medici impiantabili

I moderni IMD comunicano in modalità wireless con un dispositivo esterno detto *programmer* e inviano dati per monitorare e ricevere la migliore terapia per il paziente.

Utili per monitorare i parametri vitali del paziente, soprattutto se in condizioni critiche.



Attacchi ai IMD

I principali attacchi ai dispositivi medici impiantabili sono:

- **Information Harvesting**: se nessun meccanismo di autenticazione è applicato nell'IMD, l'avversario può ottenere informazioni riservate sulla salute del paziente oppure ascoltare le comunicazioni tra dispositivo e programmer per utilizzarle in ulteriori attacchi.
- **Tracking the patient**: la comunicazione wireless può essere facilmente rilevata, soprattutto se si è all'aperto. L'attaccante può tracciare il movimento del paziente comportando una grave violazione della privacy.

Attacchi ai IMD

- **Impersonation**: se il canale wireless non è sufficientemente protetto, l'avversario può origliare comunicazioni e registrare la risposta dell'IMD. Utilizzati per raccogliere informazioni riguardo terapie e alimentazione del paziente e ritardare la risposta del medico curante ai bisogni del paziente.
- **Relaying**: l'IMD viene ingannato facendogli presumere che il programmer sia vicino ad esso. L'attaccante utilizza due device chiamati *ghost* e *leech* che impersonificano rispettivamente l'IMD e il programmer. In questo modo continuano a trasmettere i messaggi tra IMD e programmer ingannando l'IMD e facendogli credere di parlare con un programmer lecito.

Attacchi ai IMD

- **Denial of Service**: si vuole manomettere la capacità dell'IMD di svolgere il proprio lavoro:
  - Richiedere attività che consumano l'energia del dispositivo - *Power draining attack*;
  - Interferire nella comunicazione con il servizio di manutenzione;
  - Far spegnere il dispositivo applicando un campo magnetico in prossimità del paziente.

Argomenti

Difesa

La strategia di difesa si può classificare in:

- **Prevenzione**: riduzione della vulnerabilità del sistema. Riguarda tutte le operazioni eseguite *offline* prima che il sistema venga perturbato o attaccato;
- **Rilevazione**: operazioni eseguite *online*, quando un attacco si verifica. Il sistema viene costantemente monitorato per rilevare eventuali attacchi. L'attacco, se rilevato, viene isolato e vengono identificati i componenti compromessi;
- **Mitigazione**: interrompere e neutralizzare l'attacco e cercare di ridurne l'impatto.