Scenari di Attacchi Cyber ai Sistemi IoT

Ing. Luisa Franchina

Francesco Ressa

Angelo Socal

Scenari di attacco Cyber ai sistemi IoT

INDICE

Introduzione agli scenari di attacco Cyber 1/3

Al fine di aver una chiara comprensione di quali tipologie di attacchi possano venir inflitti ad un sistema IoT, proponiamo una tassonomia basata su quattro categorie di superfici di attacco (come proposto dal lavoro di Hezam Akram Abdul-Ghani ed altri*):

Superficie d'attacco	Descrizione
Oggetti fisici	Attacchi fisici ai componenti hardware. Tags RFID, lettori RFID, microcontrollori, attuatori e sensori sono possibili esempi.
Protocolli	Attacchi ai protocolli IoT connettività, rete e routing, protocolli a livello di applicazione e trasporto, protocolli di servizi web.
Dati	Attacchi ai dati statici situati negli IoT devices o nel cloud. (Gli attacchi ai dati dinamici fanno parte della categoria Protocolli).
Software	Attacchi a software IoT, comprese le applicazioni IoT che si trovano negli IoT devices o nel cloud, firmware, sistemi operativi, gateway applicazione e servizi.

*Fonte: Hezam Akram Abdul-Ghani, Dimitri Konstantas e Mohammed Mahyoub "A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model")

Introduzione agli scenari di attacco Cyber 2/3

Sono stati presi in considerazione diversi scenari di attacco che coinvolgono i **settori per i quali le tecnologie IoT sono sempre più critiche** in quanto parte dei relativi sistemi critici di back-end*: **industria, energia, traffico urbano, trasporti e sanità**.

Per ciascuno dei settori considerati, sono stati analizzati i relativi scenari di attacco fornendo le seguenti informazioni:

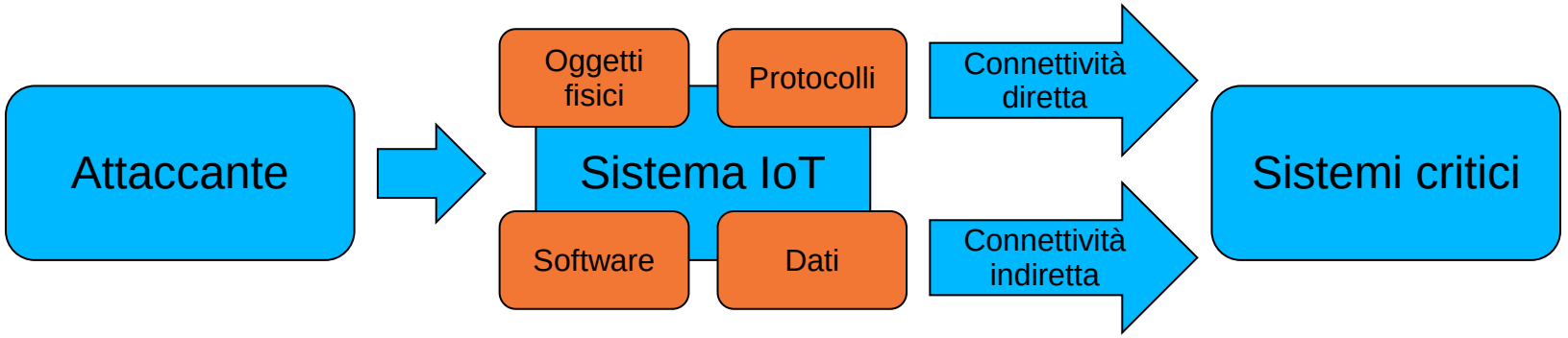
1. Una breve descrizione dell'attacco
2. Anno di occorrenza / anno di pubblicazione
3. Vettore di attacco
4. Debolezze rilevate
5. Descrizione dello scenario di attacco
6. Natura dell'attacco (proof of concept / caso reale)
7. Superficie di attacco (oggetti fisici, protocolli, dati, software)
8. Connettività con il sistema critico (diretta, indiretta)

*Fonte: Hezam Akram Abdul-Ghani, Dimitri Konstantas e Mohammed Mahyoub “A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model”)

Introduzione agli scenari di attacco Cyber 3/3

In particolare, per **connettività con il sistema critico**, si intende il tipo di connettività che si verifica tra il dispositivo IoT attaccato e il sistema critico.

Questa connettività può essere **diretta**, quando il dispositivo IoT è fisicamente o logicamente connesso a un sistema critico, o **indiretta**, quando il dispositivo IoT non è connesso a un sistema critico ma può essere sfruttato per creare nuovi vettori di attacco (Stellios ed altri, 2018*).

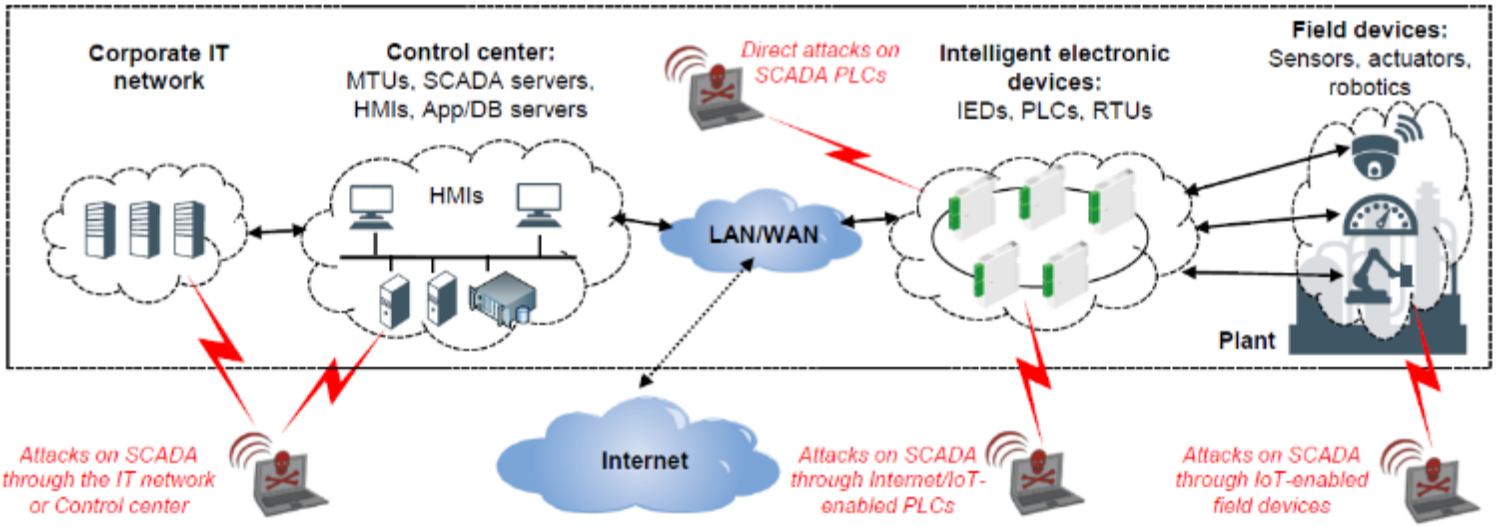


*Fonte: Ioannis Stellios, Panayiotis Kotzanikolaou, Mihalis Psarakis, Cristina Alcarazy, Javier Lopezy, A Survey of IoT-enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services accepted for publication in the online magazine IEEE Communications Surveys & Tutorials – 2018

Scenari di attacco Cyber ai sistemi SCADA industriali

I sistemi SCADA utilizzati in vari contesti industriali settoriali possono essere spesso un facile bersaglio di attacchi abilitati all'IoT.

Le vulnerabilità di questi sistemi sono spesso legate alla loro elevata esposizione, essendo **facilmente identificabili tramite strumenti come Shodan**, nonché a metodi di autenticazione deboli o inesistenti. Pertanto, le **superfici di attacco** più frequenti sono rappresentate da **Software** e **Protocolli** utilizzati.

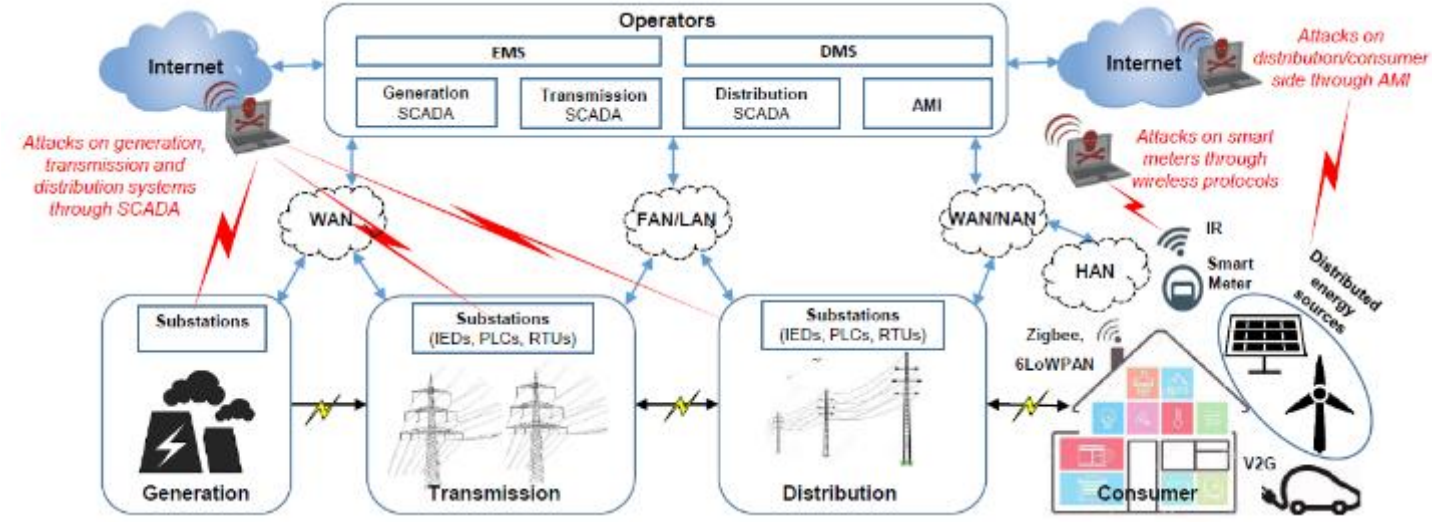


*Fonte: Ioannis Stellios, Panayiotis Kotzanikolaou, Mihalis Psarakis, Cristina Alcarazy, Javier Lopezy, A Survey of IoT-enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services accepted for publication in the online magazine IEEE Communications Surveys & Tutorials – 2018

Scenari di attacco Cyber alle infrastrutture energetiche

Negli ultimi anni, le infrastrutture energetiche elettriche e le smart grid sono state bersaglio di attacchi mediante vulnerabilità di sistemi IoT. Inoltre, diverse proof of concept hanno dimostrato le vulnerabilità di sensori, contatori e altri dispositivi che fanno parte della rete, mentre sono connessi a Internet.

Debolezze significative in questo campo sono date da interfacce di comunicazione esposte, **autenticazioni deboli e password e protocolli di rete non crittografati**. Pertanto, la **superficie di attacco** più frequente è rappresentata dai **Protocolli** utilizzati.



*Fonte: Ioannis Stellios, Panayiotis Kotzanikolaou, Mihalis Psarakis, Cristina Alcarazy, Javier Lopezy, A Survey of IoT-enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services accepted for publication in the online magazine IEEE Communications Surveys & Tutorials – 2018

Scenari di attacco Cyber alle smart-car, al traffico stradale e ai sistemi di trasporto intelligenti 1/2

Le tecnologie IoT stanno diventando ampiamente utilizzate nelle automobili, nelle infrastrutture stradali e nei sistemi di controllo del traffico e negli altri sistemi di trasporto (aerei, navi e treni).

Per quanto riguarda le **auto intelligenti**, sono stati simulati attacchi che sfruttano i **protocolli di comunicazione radio (come LAN, DAB e WiFi)**, attacchi che sfruttano le **vulnerabilità dei sistemi di infotainment** e attacchi basati sulla **manipolazione dei sensori IoT**.

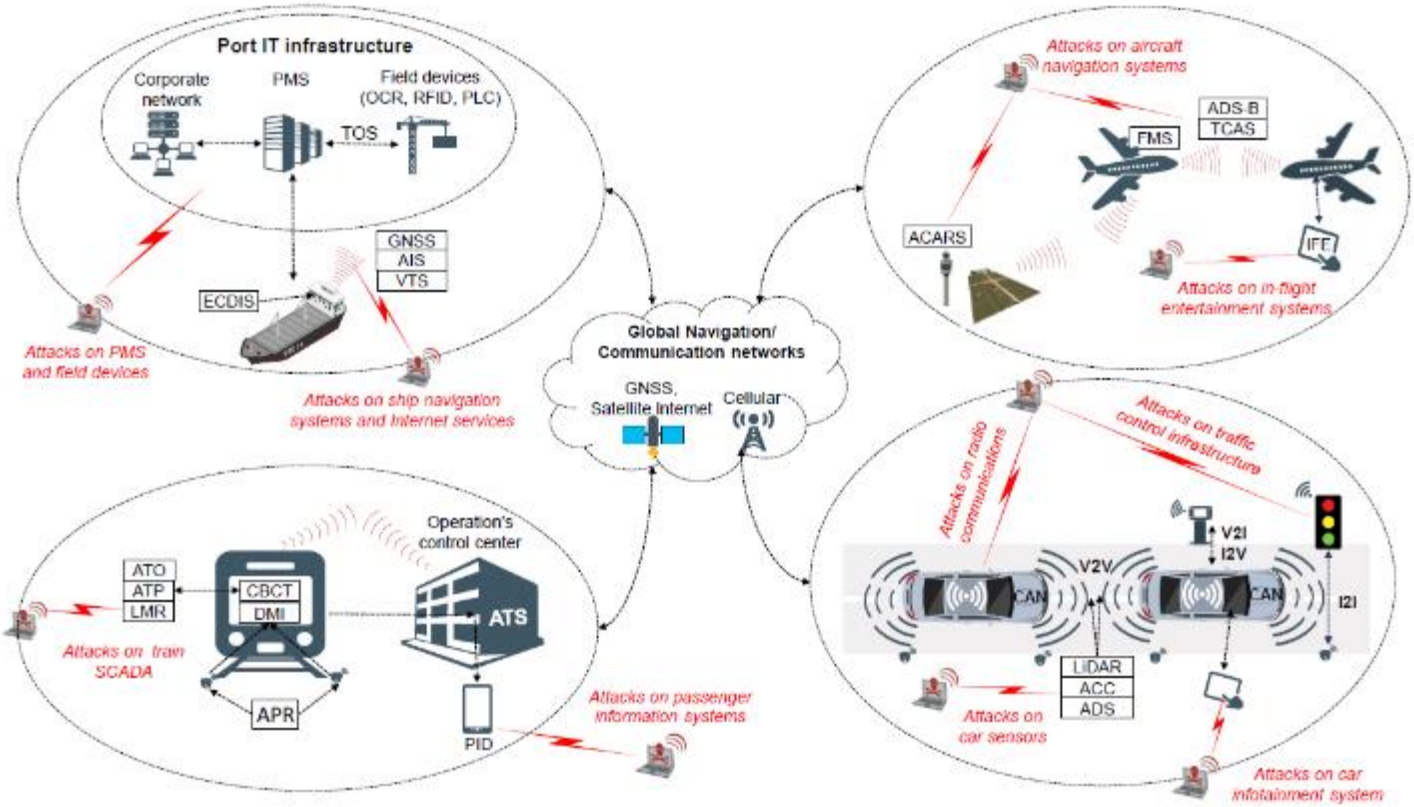
Per quanto riguarda gli **altri sistemi di trasporto**, gli scenari più significativi sono quelli caratterizzati da **attacchi a sistemi di missione critici**, ad esempio sfruttando il sistema transponder ADS-B (Automatic Dependent Surveillance - Broadcast) su un aereo o il sistema di tracciamento delle navi AIS (Automatic Identification System) su una nave.

Questi tipi di attacchi sono generalmente condotti costruendo un **emulatore del sistema da attaccare**, sostituendolo al sistema attaccato al fine di prendere il controllo dell'FMS (Flight Management System) o del sistema di navigazione della nave.

Alcuni di questi attacchi richiedono una certa **vicinanza fisica al bersaglio** e spesso sfruttano i punti deboli del **software** e dei **protocolli**.

*Fonte: Ioannis Stellios, Panayiotis Kotzanikolaou, Mihalis Psarakis, Cristina Alcarazy, Javier Lopezy, A Survey of IoT-enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services accepted for publication in the online magazine IEEE Communications Surveys & Tutorials – 2018

Scenari di attacco Cyber alle smart-car, al traffico stradale e ai sistemi di trasporto intelligenti 2/2

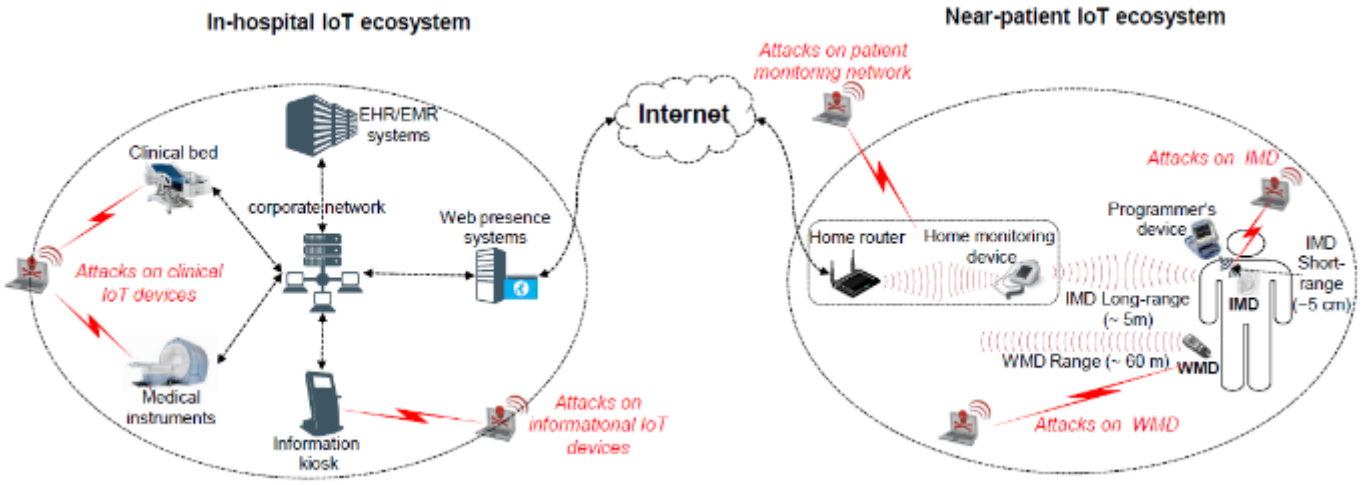


*Fonte: Ioannis Stellios, Panayiotis Kotzanikolaou, Mihalis Psarakis, Cristina Alcarazy, Javier Lopezy, A Survey of IoT-enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services accepted for publication in the online magazine IEEE Communications Surveys & Tutorials – 2018

Scenari di attacco Cyber ai servizi e alle infrastrutture sanitarie

Le tecnologie IoT stanno diventando ampiamente utilizzate nel settore sanitario sia all'interno degli ospedali che nei dispositivi medici vicini ai pazienti. Questo tipo di tecnologie può essere utilizzato direttamente nei trattamenti medici o può essere utilizzato per monitorare, raccogliere e inviare dati riguardanti le condizioni del paziente.

Le principali vulnerabilità rilevate sono la rete non segmentata all'interno delle infrastrutture ospedaliere e la mancanza di crittografia / autenticazione nei dispositivi medici. Per questi tipi di scenario, la **superficie di attacco** più frequente è rappresentata dai **Dati**.



*Fonte: Ioannis Stellios, Panayiotis Kotzanikolaou, Mihalis Psarakis, Cristina Alcarazy, Javier Lopezy, A Survey of IoT-enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services accepted for publication in the online magazine IEEE Communications Surveys & Tutorials – 2018

Grazie per l'Attenzione

Per ulteriori informazioni

AIIC
Ing. Luisa Franchina (blustarcacina@gmail.com)
Presidente AIIC / Partner Hermes Bay
Francesco Ressa
Membro di AIIC / Security Analyst in Hermes Bay
Angelo Socal (angelo.soc@gmail.com)
Membro del Consiglio Direttivo di AIIC / Security Analyst in Hermes Bay