Sistemi autonomi simbiotici e sicurezza

Francesco Flammini

Sommario

Il presente articolo indirizza la sicurezza dell'interazione tra macchine ed esseri umani nel contesto dei sistemi autonomi simbiotici (Symbiotic Autonomous Systems, SAS). In particolare, verranno affrontate brevemente le tematiche di sicurezza informatica e dei dispositivi interconnessi, la sicurezza cibernetica ("cybersecurity") e quella dei sistemi cyber-fisici (CPS, Cyber-Physical Systems). Si accennera' infine ai recenti sviluppi della sicurezza in relazione al paradigma dell'Internet delle cose (Internet of Things, IoT).

Abstract

This paper addresses the security of the interactions between machines and humans in the context of Symbiotic Autonomous Systems (SAS). In particular, the paper will provide an overview of the security in interconnected devices, including cybersecurity and Cyber-Physical Systems (CPS) security. We will also mention some recent security developments related to the Internet of Things (IoT).

Keywords: Autonomous Systems, Artificial Intelligence, Internet of Things, Security, Safety, Resilience

Introduzione

Importanza della sicurezza nei SAS

Il nostro ecosistema è molto complesso. Nei sistemi dinamici complessi, piccole modifiche nell'input possono produrre effetti di grandi dimensioni. L'ecosistema può minimizzare molti degli effetti, ma non tutti. Anche i sistemi biologici sono estremamente complessi, in cui i sistemi immunitari mostrano comportamenti molto intelligenti ed adattativi, in grado di combattere la maggior parte degli attacchi di elementi patogeni quali batteri e virus. Tuttavia, accade talvolta che

un microorganismo invisibile possa far oscillare l'omeostasi di un corpo in modo anomalo, fino a debellarlo completamente.

La nostra esistenza non è scontata ed è soggetta ai cambiamenti naturali e indotti dell'ecosistema. Ad esempio, il nostro pianeta sta affrontando una crisi senza precedenti dovuta ai cambiamenti climatici. Sono in fase di avvio massicci programmi di ricerca e sviluppo per realizzare tecnologie e infrastrutture finalizzate alla riduzione delle emissioni di gas serra. Nel celebre incontro del 2009 a Copenaghen, si è concordato di mantenere l'innalzamento della temperatura media al di sotto dei 2°C rispetto al livello preindustriale. Nel 2014, il gruppo intergovernativo sui cambiamenti climatici ha dichiarato che fare ciò richiederebbe una riduzione delle emissioni di gas serra del 40-70% rispetto al livello del 2010 entro il 2050. Si tratta di una sfida molto difficile in termini di impatto sui principali artefici dei cambiamenti climatici: generazione di energia elettrica, trasporti, cibo ed agricoltura [1]. Purtroppo, ognuno dei nuovi sviluppi tecnologici proposti per affrontare tale sfida può potenzialmente essere attaccato e modificato per capovolgere il suo scopo, accelerando così il danno. In passato, era necessario impiantare un agente (di solito una persona) nell'ambiente in modo da realizzare un danno. Oggi l'attacco può essere effettuato tramite Internet (“cyber-attacchi”), e l'Internet of things (IoT) incrementa il rischio di cyber-attacchi quali i tristemente celebri DOS (Denial of Service).

Più specificamente, la scienza della sicurezza informatica affronta i seguenti attributi principali [2]:

- Disponibilità (permanenza del sistema in condizioni di operatività)
- Integrità (dati del sistema non modificati in modo indesiderato)
- Riservatezza (dati riservati non divulgati a persone non autorizzate)

Nel dominio SAS, la disponibilità è estremamente importante poiché i sistemi autonomi simbiotici supportano l'uomo nell'esecuzione di compiti essenziali che potrebbero non essere in grado di effettuare senza l'ausilio di macchine. Ciò è particolarmente rilevante nel campo biomedico (protesi o altri dispositivi di supporto vitale come pompe per insulina intelligenti, pacemaker, ecc.), dove la conseguenza degli attacchi ai SAS può severamente colpire la salute degli esseri umani.

Anche l'integrità è di fondamentale importanza, dal momento che la correttezza dei dati nei SAS può essere molto più critica della loro disponibilità. In molti casi, infatti, risulta preferibile spegnere una macchina, in modalità sicura (es. prevedendo procedure di emergenza manuali), piuttosto che lasciarla funzionare in modo erroneo con conseguenze potenzialmente gravi. Basti immaginare un’automobile o un treno a guida autonoma in presenza di violazioni di integrità: è sicuramente meglio optare per una frenata in sicurezza piuttosto che continuare ad operare in condizioni non sicure.

Infine, la riservatezza è qualcosa di più della semplice “privacy”: tenere i dati sensibili fuori dalla portata di utenti non autorizzati e possibili terroristi può impedire il perpetrarsi di minacce quali furti di identità, frodi e altri attacchi

all'integrità e alla disponibilità dei SAS, eseguiti sfruttando le informazioni sottratte.

Nella valutazione del rischio per la “security”, tali attributi sono affrontati dal punto di vista di minacce esterne o intenzionali. Tuttavia, guasti sia intenzionali che casuali sono affrontati nel quadro più generale della “computer dependability”, tramite le tecniche tradizionali quali ridondanza e tolleranza ai guasti (fault-tolerance), oltre che quelle oggetto di ricerca come l’autoriparazione (self-healing).

A rendere le cose più difficili, i SAS diventeranno sempre più complessi e al tempo stesso critici per la nostra vita ed il nostro benessere [3]. La loro complessità è l'effetto di diversi fattori, tra cui:

- Elevate dimensioni del software necessario per realizzare dispositivi intelligenti ed autonomi, con modalità di guasto non banali e difficili da diagnosticare
- Distribuzione, dovuta alla connettività Internet e alle caratteristiche di mobilità, ubiquità e pervasività (si pensi ai dispositivi indossabili connessi a servizi cloud)
- Eterogeneità dell’hardware, del software, delle connessioni di rete wireless e cablate, dell’impiego congiunto di componenti open-source e COTS (Commercial Off-The-Shelf) insieme ad implementazioni proprietarie e personalizzate.

La criticità deriva dal fatto che i SAS saranno sempre di più impiegati in applicazioni delicatissime per il business, l’ambiente e la salute. Mentre i tradizionali sistemi di sicurezza basati su elaboratori sono mantenuti semplici per facilitarne la verifica ed il collaudo, nonché la certificazione rispetto agli standard internazionali (ad esempio, ISO / IEC 15408 - Common Criteria, IEEE Std 1686-2013 - Standard for Intelligent Electronic Devices Cyber Security Capabilities [4]), la complessità e la limitata prevedibilità dei SAS rappresentano un serio ostacolo. Al tempo stesso, gli ingegneri potranno sfruttare vantaggiosamente l'intelligenza artificiale ed altri paradigmi rilevanti per i SAS (ad esempio, quello dei Digital Twins) per prevenire e combattere le minacce in modo più efficace, basandosi su concetti di proattività, predittività e collaborazione.

Contromisure e loro efficacia

La comunità di ricerca sta facendo un grande lavoro per sviluppare contromisure efficaci per fronteggiare le diverse classi di attacchi informatici. La necessità di competenze nel settore della sicurezza è in costante aumento. Si tratta di competenze fortemente interdisciplinari, che comprendono scienza dei dati, ingegneria elettronica, informatica, analisi del rischio, crittoanalisi, elaborazione dei segnali, intelligence, ecc. È fondamentale, infatti, analizzare non solo le minacce che possono essere generate da determinati individui, ma anche le loro motivazioni, legate ad aspetti umani e socio-culturali che hanno impatto sull’intera comunità.

Tuttavia, poiché il numero di attacchi persistenti aumenta ed è per lo più incontrollato, qualcosa è inadeguato nelle nostre contromisure. In linea di principio, le contromisure basate su osservazioni passate non sono adeguate. Poiché gli attacchi appartengono spesso alla classe dei sistemi dinamici, devono essere combattuti con sistemi dinamici. La ricerca recente in questo settore si basa proprio su tale approccio. In questa breve disanima, passeremo in rassegna alcune tecniche e tecnologie moderne secondo le quali i sistemi autonomi simbiotici dovrebbero essere sviluppati per affrontare le diverse classi di attacchi.

Sicurezza dei sistemi autonomi simbiotici

I SAS sono sistemi dinamici complessi, progettati per esibire comportamenti non banali. Di conseguenza, i SAS sono vulnerabili anche ad attacchi ancora sconosciuti. Proprio come gli esseri umani, si tratta di sistemi complessi, con molti componenti e sottosistemi interagenti e con relazioni non lineari, che operano in un mondo non lineare. Come per gli esseri umani, un semplice virus potrebbe attaccare un SAS e riprodursi rapidamente fino a metterlo fuori uso. Per avere la possibilità di contrastare il virus, il SAS deve possedere una sorta di sistema immunitario in grado di produrre diversi "anticorpi" di test, e quando uno di questi corrisponde all'invasore, il sistema dovrebbe passare alla produzione di un massiccio esercito di "soldati" simili per sopprimere l'invasore in tempo utile.

La sopravvivenza umana è legata alle capacità "intelligenti" che il sistema immunitario mette in atto per sconfiggere gli agenti patogeni. Le difficoltà principali risiedono nella mutazione delle caratteristiche degli agenti patogeni, che li rendono sempre diversi. Proseguendo su tale parallelismo, il sistema immunitario di un SAS può essere ingannato da agenti patogeni mutevoli e deve reagire modificandosi opportunamente. Il problema principale è che i risultati di tali modifiche potrebbero essere imprevedibili e potrebbero portare a fallimenti e comportamenti pericolosi, come quando in un sistema biologico avvengono risposte autoimmuni. Questo è un primo aspetto in cui emerge che l'intelligenza nei sistemi SAS è sicuramente un vantaggio, ma porta con se aspetti di impredicibilità che in sistemi critici devono essere attentamente studiati e validati.

Cybersecurity

La cybersecurity è definita come una "disciplina basata sul calcolo che coinvolge tecnologia, persone, informazioni e processi per consentire operazioni sicure. Implica la creazione, la gestione, l'analisi e il collaudo di sistemi informatici sicuri. È un tema interdisciplinare, che comprende aspetti di giurisprudenza, politica, fattori umani, etica e gestione dei rischi con riferimento agli eventi avversi" [5]. La cybersecurity si riferisce al funzionamento sicuro di un sistema informatico, incluse le reti locali, nazionali e globali. Sebbene si tratti di un business da quasi 100 miliardi di euro, ad oggi poche aziende si sentono al sicuro. Ad esempio, nel periodo che va da giugno a dicembre 2009, giganti come Google, Adobe, Yahoo, Symantec, Northrop Grumman, Dow Chemicals, Morgan Stanley hanno subito attacchi provenienti dalla Cina (nome in codice

"Operation Aurora"). A tal proposito, il gigante dell'informatica Google ha introdotto la cosiddetta politica ZeroTrust: nessuna persona esterna o interna all'organizzazione è considerata completamente affidabile.

Non esiste una serie standard di regole utilizzate per affrontare il crescente numero di minacce provenienti da hacker, ransomware e furto di dati. Negli Stati Uniti, il National Institute of Standards and Technology (NIST) ha pubblicato il Cybersecurity Framework [6] ed una roadmap per migliorare la cybersecurity delle infrastrutture critiche. Il framework identifica cinque funzioni per organizzare un sistema di sicurezza: identificare, proteggere, rilevare, rispondere e ripristinare. Il framework è destinato prevalentemente alle piccole imprese con lo scopo di deframmentare il mondo della sicurezza informatica. Il dipartimento americano della sicurezza nazionale (Homeland Security) identifica 16 settori infrastrutturali critici tra cui reti di telecomunicazioni, difesa, protezione civile, servizi finanziari, alimentazione, sanità, reattori nucleari, sistemi di trasporto e reti idriche [7].

La principale motivazione degli attacchi informatici risiede nelle vulnerabilità del software che possono essere sfruttate dagli hacker. Gli incidenti di cybersecurity più comuni sono dovuti a malware e virus convenzionali (64%), attacchi di ransomware (30%), errori dei dipendenti e azioni involontarie (27%) [8]. Per farsi un'idea dell'entità del problema, basti citare che circa il 40% dei computer con connessione Internet condivisa presenta attacchi ogni sei mesi, la maggior parte delle organizzazioni (61%) hanno una gestione della sicurezza inadeguata, ed il 66% delle imprese manifatturiere non ha budget dedicato alla sicurezza informatica.

Sicurezza cyber-fisica

La sicurezza cosiddetta cyber-fisica si riferisce alla sicurezza di sistemi informatici operanti in stretta connessione con un ambiente fisico, come i sistemi di controllo industriale (Industrial Control Systems, ICS), le auto a guida autonoma ed i droni, in cui i componenti cyber hanno responsabilità di rilevamento, controllo e azionamento, e sono connessi a Internet. A causa della connessione Internet, il sistema diventa vulnerabile alle minacce alla sicurezza che possono verificarsi nelle "reti aperte". La differenza tra la cyber-security e la cyber-physical security è che mentre nella prima le conseguenze si esauriscono il più delle volte nel modo cyber, con eventuali ripercussioni indotte in modo indiretto nel modo fisico, nella seconda le conseguenze sono direttamente impattanti sul mondo fisico, anche se la parte cyber risultasse apparentemente non compromessa. In altre parole, il danno potrebbe limitarsi al mondo fisico, con conseguenti difficoltà in termini di diagnosi e rilevamento nella parte cyber. Alcuni esempi riportati nel seguito chiariranno meglio questo concetto. In entrambi i casi, però, è importante chiarire che la "sicurezza fisica", ovvero la protezione nei confronti di accessi e manipolazioni del sistema di tipo tangibile (es. tramite accesso non autorizzato ai locali tecnici del datacenter di un impianto industriale) rimane un aspetto distinto, per quanto fortemente correlato al concretizzarsi di talune minacce: si

pensi ad es. a connessioni cablate su reti isolate, in cui l'accesso fisico alle reti e ai dispositivi è indispensabile.

Dal momento che i sistemi autonomi simbiotici incorporano dispositivi fisici connessi per interagire con gli esseri umani e l'ambiente, essi appartengono anche alla categoria dei sistemi cyber-fisici (CPS, Cyber-Physical Systems) e sono pertanto soggetti alla valutazione del rischio tipica di questi sistemi.

Rischi, vulnerabilità e conseguenze nei sistemi cyber-fisici

Essendo dotati di componenti sia fisici che cyber, i CPS possono essere soggetti a minacce, vulnerabilità e conseguenze che investono entrambi i mondi.

Un esempio di attacco ad un CPS è quello di una centrifuga la cui operatività può essere modificata causando un rallentamento del processo quasi impercettibile. è quello che è successo con l'attacco del virus "Stuxnet" alle centrifughe iraniane di un impianto nucleare controllate da un sistema SCADA (Supervisory Control and Data Acquisition), che ne causò danni ingenti ed infine l'arresto nel 2010 [9]. Un sistema SCADA è un'applicazione che consente agli operatori umani di monitorare un processo industriale e di archiviare e analizzare i dati di processo corrispondenti. Si tratta di un sistema critico in quanto attacchi di tipo cyber, come quello menzionato, possono avere conseguenze devastanti sui componenti fisici e finanche causare disastri ambientali.

Un altro esempio è quello della cosiddetta "smart-grid" (rete intelligente di distribuzione dell'energia elettrica), in cui è necessario monitorare le utenza al fine di ottenere dati in tempo reale relativi per ottimizzare l'erogazione di energia verso specifiche destinazione. Contatori automatici, intelligenti ed interconnessi (smart-meters), sono utilizzati per misurare il consumo energetico dei consumatori e per fornire una varietà di servizi a valore aggiunto. Poiché le informazioni raccolte possono includere dati sensibili dei consumatori, queste devono essere protette opportunamente, il che rappresenta una criticità di tipo "privacy" comune a molti sistemi cyber-fisici (si pensi ad esempio a quelli impiegati in applicazioni "smart-health" di monitoraggio remoto dei pazienti), e che deve pertanto essere annoverata tra gli aspetti a cui dedicare particolare attenzione nelle analisi di sicurezza di tali sistemi [10].

Altri esempi rilevanti di sicurezza di sistemi CPS sono:

- L'alterazione dell'operazione e l'esplosione di un impianto petrolchimico (evento realmente avvenuto in Arabia Saudita nel 2017).
- Il controllo remoto di un'automobile connessa di ultima generazione, dotata di pilota automatico, con conseguenze potenzialmente letali.
- La modifica del software di una macchina per la risonanza magnetica connessa al fine di generare immagini errate del cervello.
- La modifica di una pompa per infusione collegata a Internet al fine di somministrare una quantità letale di medicinale al paziente.
- La manipolazione di un frigorifero connesso al fine di deteriorare gli alimenti e causare intossicazioni ed infezioni.

- La manipolazione del sistema di controllo di una diga con conseguenze devastanti per milioni di persone (ci sono circa 100.000 dighe solo negli Stati Uniti).
- Lo spegnimento dell'impianto elettrico in una casa, in un distretto o nell'intera città con le conseguenze che è facile immaginare.

Poiché la maggior parte degli attacchi di cui sopra sono stati provati ed alcuni di essi hanno avuto successo, risulta evidente che è necessario incrementare il livello di sofisticazione delle contromisure. è altresì evidente che contromisure puramente reattive non sono sufficienti: i SAS, in particolare, dovrebbero essere sviluppati per affrontare tali attacchi cyber-fisici in modo pro-attivo, predittivo e collaborativo. In altre parole, i futuri CPS dovrebbero essere progettati non solo per essere sicuri ed affidabili nell'affrontare minacce note, ma anche per riconoscere minacce sconosciute, adattarsi ed organizzarsi per fronteggiarle in modo possibilmente strategico e ripristinare il normale funzionamento nel più breve tempo possibile. Ci si riferisce spesso a queste ultime caratteristiche come "self-healing" e "resilienza".

Problemi legati al supporto e all'eterogeneità dei fornitori

I produttori di software forniscono supporto per un prodotto per un ragionevole lasso di tempo, mentre le aziende di hardware forniscono supporto per un periodo di tempo molto più breve (2-3 anni), con la situazione che è iniziata a cambiare nel 2018 (7-10 anni). Si tratta di un problema importante, in quanto i prodotti connessi possono generare piccoli profitti richiedendo anni di aggiornamenti e patch per adeguarne la sicurezza.

Inoltre, molti dispositivi connessi sono assemblati con componenti (hardware, firmware, software) sviluppati da diversi fornitori. Ciò è particolarmente preoccupante perché se il collegamento più debole non viene aggiornato regolarmente, l'intero sistema diventa vulnerabile. Mentre nella maggior parte dei sistemi IT omogenei vi è un processo di aggiornamento regolare del software interamente sotto il controllo di un fornitore, nei sistemi cyber-fisici eterogenei ciò non è ancora regolato in modo chiaro e coordinato. Ciò si riflette inevitabilmente sui sistemi autonomi simbiotici che incorporano dispositivi fisici interconnessi vulnerabili ad attacchi cyber-fisici. è pertanto necessario profondere energie sullo sviluppo di standard, metodologie e strumenti che possano supportare il patching e l'aggiornamento regolare dei SAS eterogenei.

Impatto della sicurezza cyber sulla società

Per tutto quanto scritto precedentemente, è evidente che la cybersecurity può avere un notevole impatto economico e sociale su intere comunità. Le conseguenze di attacchi possono essere ancora più rilevanti e riguardare salute ed ambiente laddove la sicurezza riguardi i sistemi cyber-fisici. Ma c'è di più.

Nella società moderna, gran parte delle interazioni sociali sono veicolate tramite Internet. Si pensi ad esempio all'uso massiccio di motori di ricerca, blog, e social networks. Molti dei contenuti che ci raggiungono, le notizie e gran parte delle risposte alle nostre domande quotidiane sono pertanto "filtrati"

da entità cyber secondo algoritmi a noi sconosciuti e sotto il controllo di altri. Ad esempio, Flipboard e applicazioni simili selezionano gli articoli in base ai nostri interessi. Amazon e sistemi simili di commercio elettronico (e-commerce) suggeriscono acquisti di libri, musica, video e prodotti fisici in base alle nostre precedenti interazioni e ai profili social. Nella società futura, la percezione della realtà sarà potenziata ("realtà aumentata") attraverso dispositivi portatili ed indossabili (si pensi agli smart-glasses) che fungeranno sempre più da vere e proprie "protesi". Già oggi il fenomeno delle "fake news" ed altri condizionamenti indotti sono oggetto di discussione a tutti i livelli, ed è quindi chiaro che tali manipolazioni potranno essere usate sempre più per distorcere la comprensione della realtà, in modo da sviluppare una realtà alternativa secondo la strategia dell'attaccante. L'alternanza di informazioni affidabili con risposte fasulle rappresenta un ulteriore elemento che può sviare la comprensione della realtà. Con un opportuno innesco della realtà distorta, le notizie false possono sembrare plausibili e superare l'ostacolo della capacità critica dell'individuo, tra l'altro destinata tanto più ad atrofizzarsi quanto più le tecnologie sostituiranno i suoi strumenti percettivi.

Nel campo dell'istruzione, il processo di distorsione delle informazioni ha qualche possibilità di auto-correzione per via delle capacità di discernimento degli studenti. Se invece la distorsione viene applicata ad informazioni quali cartelle cliniche, rapporti di produzione, relazioni finanziarie oppure posizioni politiche impiegate nel processo decisionale, le conseguenze potrebbero essere molto più rilevanti. In situazioni basate sulla fiducia, in cui non vi è tempo per la verifica di qualità delle informazioni fornite, l'alterazione potrebbe essere decisiva.

Standard e sicurezza nell'Internet of Things

Questa sezione descrive in che modo l'industria sta rispondendo ai rapidi sviluppi nell'area della connettività della Internet of Things (IoT) e di alcuni sistemi di protezione dei dati.

Il collegamento dei dispositivi IoT ad una rete locale o ad Internet richiede tecnologie cablate e wireless sviluppate molto prima che il concetto IoT fosse introdotto e non sempre adeguate a supportarne i requisiti. Le soluzioni wireless possono comprendere protocolli proprietari a livello di dispositivo, connessioni WiFi, Bluetooth Low Energy (BLE), rete cellulare, ed altre tecnologie. La connettività del dispositivo e molte altre elaborazioni di dati appartengono a ciò che viene definito "edge computing" (livello intra-dispositivo) o "fog computing" (livello area locale o metropolitana), in opposizione al "cloud computing" che prevede l'utilizzo di server in data center remoti raggiungibili tramite Internet, la cui localizzazione non è sempre ben definita. è intuitivamente evidente che il numero teorico di potenziali minacce sale man mano che ci si sposta dal livello locale a quello geografico, su cui si ha meno controllo a livello di infrastruttura, ed è altresì proporzionale al numero di collegamenti wireless impiegati, per via della maggior "apertura" e accessibilità fisica di tali reti. Vi sono però validi controesempi: un provider serio di servizi cloud può fornire maggiori garanzie di sicurezza rispetto ad un

servizio locale mal gestito; un'infrastruttura di rete locale cablata in cui i dati scambiati non sono crittografati (per via di una eccessiva confidenza sul livello di segregazione fisica) può risultare all'atto pratico meno sicura di una rete WiFi dotata di adeguata cifratura; per motivi analoghi, il completo isolamento da Internet può essere un'arma a doppio taglio in quanto impedisce il regolare aggiornamento dei dispositivi con le più recenti patch di sicurezza.

IoT LPWAN

Il LoRaWAN Alliance ha annunciato l'implementazione di un protocollo di rete geografica a bassa potenza (LPWAN) che permette il collegamento wireless a Internet di oggetti alimentati a batterie, a livello di reti regionali, nazionali, o globali. Dispone di comunicazioni dati bidirezionali e di sicurezza end-to-end, servizi di mobilità e localizzazione. Utilizza la topologia "star-of-star" in cui i gateway inoltrano i messaggi tra i dispositivi finali ed il server di rete centrale. Il gateway funge da ponte transponder per convertire i pacchetti a radiofrequenza (RF) nei pacchetti IP (Internet Protocol). è dotata di "Firmware-Over-The-Air" (FOTA) per aggiornare i dispositivi collegati o per distribuire i messaggi. Esempi di dispositivi sicuri LoRa comprendono Cypress PSoC 6MCU, Semtech, e ARM Cortex-M 2MCU.

WiFi IoT (IEEE 802.11)

Se il fattore consumo energetico non è critico, la connettività IoT può utilizzare un'infrastruttura ben consolidata di hub e router WiFi. Ad esempio, nel 2018, NXP Semiconductor ha sviluppato un dispositivo edge-computing IoT-on-a-Chip basato sul processore applicativo ARM iMX 6ULL, completo di WiFi (dual-band 802.11ac) e Bluetooth (4.2). Ha un ingombro ridotto (14x14x2,4mm), è scalabile e facile da usare nei progetti. Sarà seguito da iMX7 e iMX8 nel 2019. L'IoT-on-a-Chip è adatto per l'impiego in robot sicuri, nel rilevamento e gestione manomissioni, e nella crittografia ad alto throughput. Può anche essere espanso con un'interfaccia inter-chip personalizzata.

IoT ZigBee (IEEE 802.15.4)

Per le applicazioni che non esigono trasferimenti dati ad alta velocità, ma richiedono una bassa potenza, i dispositivi di rete auto-organizzanti per ambienti industriali utilizzano spesso il protocollo ZigBee. Ad esempio, la STMicroelectronics ha annunciato un chip wireless a doppio processore, STM32WB System-on-Chip (SoC) per supportare il protocollo ZigBee. È basato sul microcontrollore ARM Cortex-M4 per l'esecuzione dell'applicazione principale. Un altro core ARM Cortex-M0+ viene utilizzato per alleggerire il processore principale. Prevede il Bluetooth Low Energy (BLE) 5 ed una radio ZigBee in grado di eseguire non solo il ZigBee ma anche l'OpenThread e altri protocolli. Un'altra particolarità è il "balun" interno incluso sul SoC per il collegamento diretto all'antenna con risparmio di 6 elementi esterni. La radio a bassa potenza a 2,4 GHz richiede 5,5 / 3,8 mA per trasmettere / ricevere.

IoT Bluetooth Low Energy (BLE) (IEEE 802.15.4)

Le applicazioni in ambito sanitario, fitness, sicurezza e home entertainment richiedono spesso connettività edge IoT a basso consumo attraverso la rete BLE

"personal area network" (PAN). Il BLE va bene per dispositivi che devono rimanere operativi per un anno prima della successiva ricarica. La copertura è regolabile da 3m a 60m circa. Ad esempio, Texas Instruments ha annunciato numerosi dispositivi SimpleLink BLE. Tra questi, lo MCU CC2642R è adatto ad applicazioni Bluetooth 4 e 5 in dispositivi 2.4 Ghz e Sub-1 GHz, con un assorbimento in modalità "sleep" inferiore a 1μA. Ha una CPU ARM Cortex-M4F a 48 MHz, un ARM Cortex-M0 dedicato per il controllo radio, oltre ad un Sensor Controller a bassissimo assorbimento per sensori digitali e analogici, ed acquisizione dati. Il suo ricetrasmettitore può gestire molti protocolli compresi WiFi, BLE, ZigBee, Thread, Sub-1-GHz ed Ethernet.

IoT Cellular Networking

Molti dispositivi IoT richiedono connettività cellulare, tramite GSM, CDMA, LTE in ambienti 2G, 3G, 4G e 5G. Tra le aziende che operano nel settore, Nortfic Semiconductor ha annunciato la sua nRF91 per lavorare con Verizon Wireless Network (USA) e Telia (Norvegia). Il nRF91 è un System-in-Package (SiP) multimodale LTE-M / NB-IoT ultracompatto, a bassa potenza e piccolo ingombro (10x161,2mm). Utilizza il processore ARM Cortex-M33, il processore di sicurezza ARM TrustZone e il GPS assistito. Ha un modem, un ricetrasmettitore SAW-less e un frontend Qorro RF. Il sistema nRF91 è destinato non solo agli attuali smartphone, ma anche a molti altri dispositivi mobili. Esso comprende funzioni di sicurezza per l'hardware ed il software applicativo attraverso l'ARM Cortex-M33 e l'ARM CryptoCell-310. Il TrustZone per ARMv8-M protegge i dati, il firmware e le periferiche.

IoT Near-Field Communications (NFC)

La tecnologia di comunicazione cosiddetta "near field" (NFC) consente di collegare un dispositivo portatile con un terminale in modalità contactless. Viene stabilita una connessione quando il dispositivo portatile viene avvicinato al terminale senza necessità di contatto fisico. Esempi di protocolli utilizzati sono Bluetooth ed il FeliCa. Gli standard utilizzati sono ISO / IEC 14443 (106 kb/s) per le carte d'identità e ISO / IEC 18000-3 per i dispositivi RFID. A titolo di esempio, la STMicroelectronics ha annunciato i tag ST25NF come IC Tag Type 4 (ST25TA), Dynamic Tag IC tipo 5 (ST25DV) e IC Tag 5 (ST25TV), ora certificati.

Oltre a quelli elencati, esistono diverse altre implementazioni di connettività a livello "edge", e tutti prevedono approcci simili di "security by design" (progettazione basata sui requisiti di sicurezza).

Esempi di ricerca in sicurezza

Poiché gli attacchi informatici sono molto sofisticati, non sono applicabili tecniche semplici per il loro rilevamento. Si stanno conducendo ricerche approfondite in tutto il mondo per sviluppare tecniche efficaci capaci di rilevare anomalie su reti connesse attraverso l'analisi dei pacchetti trasmessi, ed altri strumenti finalizzati ad implementare contromisure idonee. Quasi tutti i dati catturati da una rete sotto attacco possono considerarsi non stazionari. Un'analisi approfondita è necessaria per segmentare i segnali in frame adeguati, estrarne le caratteristiche ("feature") più significative,

assemblare le feature in vettori, inserire i vettori in un classificatore, classificare il comportamento della rete in base alle feature, ed infine determinare contromisure appropriate per proteggere la rete ed i dispositivi ad essa connessi. L'acquisizione e la segmentazione dei dati è il prerequisito per l'analisi delle feature. L'estrazione di feature dai dati costituisce la prima grande sfida e viene spesso eseguita utilizzando analisi temporali standard e/o spettrali mono-scala. C'è fermento nella ricerca finalizzata a migliorare l'estrazione delle feature attraverso tecniche di elaborazione del segnale multi-scala e poli-scala [11]. Oltre alle metriche tradizionali basate sull'energia, si utilizzano anche metriche basate sull'entropia in grado di estrarre modelli ("pattern") relativi alle informazioni presenti nei dati [12] [13]. Le metriche devono anche essere adatte per il traffico di tipo burst ("a raffica"), che è caratterizzato da una dipendenza a largo spettro, con distribuzioni di probabilità-massa-funzione dotate di lunghe "code".

Il secondo elemento principale nello sviluppo della tecnica è identificare l'inizio dell'attacco. Il terzo è classificare gli attacchi e lanciare contromisure appropriate. Le fasi di rilevamento e classificazione coinvolgono tecniche di apprendimento automatico ("machine learning") e apprendimento profondo ("deep learning") [14]. Recentemente, sono state condotte indagini sui tali metodi per l'analisi delle reti al fine di rilevare intrusioni, corredate dalla descrizione dei dataset di rete comunemente impiegati [15]. Esempi di tecniche di rilevamento anomalie per contrastare i famosi attacchi DDoS (Distributed Denial of Service) sono forniti nei riferimenti bibliografici [16] e [17].

Sfide e problemi aperti per la sicurezza dei SAS

I SAS sono sistemi basati su computer appartenenti alle classi dei sistemi embedded ed in particolare dei CPS cosiddetti "smart", ovvero dotati di intelligenza avanzata per renderli autonomi ed in grado di operare simbioticamente tra loro, con gli esseri umani e con l'ambiente. In quanto tali, la loro sicurezza eredita la maggior parte delle metriche, delle vulnerabilità emergenti e delle tecnologie di protezione sviluppate per le classi di sistemi a cui appartengono. Sebbene la complessità e la criticità dei SAS possano essere superiori ai più comuni sistemi di elaborazione, il che complica notevolmente la loro progettazione ed analisi, essi presentano alcune funzionalità uniche che difficilmente possono essere ritrovate nei sistemi tradizionali. Tali capacità sono una conseguenza della loro maggiore intelligenza e autonomia, che possono essere vantaggiosamente sfruttate per progettare macchine che si auto-diagnosticano, auto-proteggono e auto-riparano ("self-healing"). Inoltre, essi cominceranno presto a mostrare alcuni aspetti di sicurezza proattiva: invece di assumere che ogni cosa nell'ambiente circostante stia lavorando secondo specifica, essi inizieranno a prevedere i comportamenti anomali nell'ambiente da parte dei loro simili e degli esseri umani [18].

Ad esempio, si consideri il caso di veicoli autonomi dotati di infrastruttura di controllo centralizzata che si avvicinano ad un incrocio. Secondo i tradizionali paradigmi di sicurezza, il sistema di controllo centralizzato consentirà solo ad

alcuni veicoli di muoversi e comanderà agli altri di rimanere fermi. I veicoli autorizzati a muoversi ignoreranno completamente la presenza degli altri veicoli (come nel caso del controllo ferroviario) o al massimo individueranno ostacoli sul loro percorso se dispongono di sensori appropriati o di visione artificiale. Pertanto, negli attuali sistemi critici per il controllo del traffico, comportamenti anomali dei veicoli che non sono previsti nelle specifiche tecniche possono facilmente portare ad incidenti. Immaginiamo ora cosa succede quando noi esseri umani ci avviciniamo ad un incrocio e osserviamo che un veicolo si sta muovendo ad alta velocità lungo una strada laterale verso la nostra traiettoria. Anche sapendo che quel veicolo sarà obbligato ad arrestarsi se abbiamo noi la precedenza, rallenteremo prudentemente in quanto percepiamo un livello di rischio più elevato, associato al fatto che quel veicolo potrebbe non essere in grado di fermarsi. Lo stesso vale per qualsiasi altro comportamento esterno che percepiamo come non sicuro o minaccioso. Ciò non avviene nella maggior parte degli attuali sistemi di controllo computerizzati, a meno che non vi sia un requisito specifico, dal momento che le regole funzionali sono normalmente molto semplici e facili da valutare. Tuttavia, è quasi impossibile prevedere tutto ciò che può accadere in scenari reali, e gli incidenti più gravi possono accadere come conseguenza di situazioni imprevedibili o impreviste; ad esempio, a causa di hacker che assumono il controllo di alcune entità di sistema. La capacità dei SAS di adattarsi e reagire a scenari imprevisti è pertanto una caratteristica che può controbilanciare le debolezze legate alla loro stessa impredicibilità, portando ad un apparente paradosso. Ciò significa che è necessario un cambio di paradigma per passare dal tradizionale controllo centralizzato basato su sicurezza predicibile, ai sistemi autonomi decentralizzati ed adattativi, in grado di reagire a minacce sconosciute e scenari operativi imprevisti.

Analogamente, e in modo diverso dagli esseri umani, i sistemi attuali non sono progettati per, e quindi incapaci di, fare ciò che sarebbe altrimenti desiderabile, come ad esempio:

- Rilevare comportamenti anormali in agenti paritari, ed avvisare prontamente gli altri agenti con cui collaborano.
- Avvisare i loro simili sui pericoli e le minacce che potrebbero incontrare, in base alla loro esperienza e conoscenza accumulata.
- Supportare le altre entità nel difendersi e riprendersi dagli attacchi.
- Cooperare strategicamente e coordinare gli altri per rispondere meglio agli attacchi.

Mentre un simile livello di intelligenza e autonomia può apparire fantascientifico, molto è già stato fatto per raggiungere un livello almeno moderato di sicurezza proattiva, facendo leva sull'apprendimento automatico, sul riconoscimento delle situazioni (“situation awareness”) e sul supporto decisionale. Ad esempio, il rilevamento delle intrusioni nelle reti utilizza approcci euristici per rilevare anomalie nel traffico di rete e nel comportamento degli utenti. Modelli di riconoscimento basati su reti bayesiane o su reti neurali

artificiali possono essere addestrati al fine di mettere a punto le loro prestazioni [19].

A un livello cognitivo più avanzato, il concetto di "distributed reflective architectures" è stato introdotto per la prima volta circa 15 anni fa, ed è stato in qualche modo pionieristico rispetto all'attuale ricerca sui gemelli digitali ("digital twins") [20]. In tali modelli concettuali, gli agenti autonomi presentano una qualche forma di monitoraggio e controllo reciproco. Affinché un SAS possa monitorare i suoi simili e l'ambiente, è necessario che adeguati modelli predittivi siano inclusi nel suo "cervello". Limiti di capacità e prestazioni hanno impedito di gestire tali modelli computazionali complessi in passato, ma in futuro opportune combinazioni di edge, fog e cloud computing consentiranno a dispositivi connessi con limitate potenze di calcolo di gestire le necessarie elaborazioni in modo efficiente, con il miglior compromesso tra precisione, tempi di risposta e consumo energetico. I SAS prevederanno dei cloni virtuali di loro stessi, delle altre entità con cui interagiscono e dell'ambiente, al fine di eseguire simulazioni accelerate "what if?" basate sulla verosimiglianza di minacce, attacchi e altri eventi indesiderati. Proprio come fanno gli umani quando si preoccupano delle implicazioni di un potenziale pericolo, i SAS valuteranno le situazioni, avvertiranno gli umani, prediranno le possibili conseguenze e pianificheranno rapidamente contromisure efficaci. Inoltre, livelli più alti di intelligenza consentiranno ai SAS di impostare autonomamente strategie di sicurezza avanzate, come trappole e mimetizzazioni, al fine di fuorviare gli avversari.

Conclusioni

La cybersecurity, la sicurezza cyber-fisica, e le relative implicazioni sociali sono sotto la lente d'ingrandimento del mondo accademico, della ricerca industriale, dei governi, e di tutti i cittadini preoccupati di quello che sarà il futuro dei propri figli. Si tratta di una delle sfide piu' grandi e avvincenti, che riguarda le fabbriche, la finanza, la sanità e le maggiori organizzazioni, e che ha un impatto su tutti gli aspetti della nostra esistenza, da quelli tangibili (es. salute, protezione) a quelli cognitivi (es. percezione, opinioni). Sono stati pubblicati migliaia di articoli tecnici, libri e riviste che trattano argomenti correlati alla sicurezza dei sistemi SAS, presenti negli archivi dei più noti editori (IEEE/Wiley, ACM, Springer, Elsevier, ecc.), ma nonostante ciò quello della sicurezza dei sistemi intelligenti autonomi è a tutt'oggi un campo di ricerca apertissimo con molte questioni irrisolte, non solo di tipo tecnico, ma anche etico, sociale e legale. Si pensi all'accettabilità sociale dei "cobots" (robot collaborativi che affiancano gli umani nelle catene di montaggio) potenzialmente pericolosi, alle responsabilità legali degli incidenti causati da sistemi autonomi impredicibili (oltre che "indottrinabili"), ed infine ai "dilemmi" che si presentano quando un veicolo stradale a guida autonoma, in una situazione critica, dovrà necessariamente scegliere se sacrificare i pedoni o l'equipaggio del mezzo.

Evidentemente, quello della cybersecurity è un ambito multidisciplinare, richiede una solida base in ingegneria ed informatica, ma non solo. Molte università hanno preso in considerazione l'idea di intraprendere programmi

specifici di cybersecurity. Tuttavia, le conoscenze fondamentali su cui si sta sviluppando tale campo sono frammentate, e pertanto stanno prendendo piede iniziative come quella del progetto CyBOK (Cyber Security Body of Knowledge) allo scopo di stabilire le conoscenze fondamentali e generalmente riconosciute sulla sicurezza informatica [21]. Un'iniziativa notevole in quest'ambito, che ne testimonia l'importanza e l'attualità, è quella dell'IEEE che con il suo Future Directions Committee ha istituito una specifica "IEEE Cybersecurity Initiative", in cui è stato sviluppato il progetto Try-CybSi [22]. Inoltre, nel 2015 è stata istituita una task force congiunta sull'educazione alla cybersecurity ("Joint Task Force on Cyber-Security Education"). Tra le varie iniziative connesse delle organizzazioni di settore, si menziona il comitato tecnico IFIP (International Federation for Information Processing) sull'Information Security Education (IFIP WG 11.8). Nonostante i molti sforzi profusi per specificare un quadro educativo omogeneo per la sicurezza, il materiale didattico differisce sostanzialmente tra le varie istituzioni. Anche i requisiti di formazione dell'industria variano notevolmente e pertanto alcune organizzazioni tecniche hanno formulato delle linee guida a riguardo (vedi ad es. [23]).

Tutti questi sforzi, tuttavia, dovrebbero essere accompagnati dal cambio di paradigma abilitato dalla futura generazione di SAS. Infatti, nel controllo distribuito attuale, le entità sono prevalentemente progettate per:

- Fidarsi incondizionatamente dei propri supervisori
- Non preoccuparsi dei loro simili e dell'ambiente circostante, fatta eccezione per le variabili che sono tenute a monitorare
- Comandare e dimenticare ("set and forget") le entità da loro supervisionate

Al fine di raggiungere una resilienza a 360 gradi, oltre alle funzionalità di autodiagnostica e autoriparazione, i SAS saranno chiamati a:

- Controllare criticamente se possono fidarsi del loro supervisore, proprio come fanno gli umani, verificando se i comandi che ricevono siano ragionevoli e sicuri
- Porre attenzione ai comportamenti dei loro simili e alle evoluzioni dell'ambiente circostante, al fine di rilevare eventuali anomalie e comportamenti anormali che potrebbero essere sintomo di sabotaggio
- Verificare in modo proattivo se le entità supervisionate stiano effettivamente eseguendo le attività che sono state loro assegnate, o se qualcun altro ha preso il loro controllo

Ciò non richiede necessariamente che i SAS siano in grado di riconoscere e classificare situazioni sconosciute. Un modo fattibile per ottenere tali risultati è quello di incorporare modelli (semplificati) di altri SAS interagenti, imitando il comportamento simile degli esseri umani e cominciando ad impiegare in modo strutturato il paradigma dei "digital twin". Una cooperazione intelligente per riconoscere meglio le minacce e rispondere rapidamente ai malfunzionamenti è uno dei principali risultati altamente auspicabili nella ricerca sui SAS sicuri [24] [25].

Riferimenti

1. IEEE, Spectrum Magazine, June 2018. Available Aug 15, 2018 from IEEE at https://spectrum.ieee.org/magazine/2018/June
2. Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, and Carl Landwehr, "Basic concepts and taxonomy of dependable and secure computing," IEEE Trans. Dependable and Secure Computing, vol. 1, no. 1, pp. 11-33, Jan-Mar 2004. (doi: 10.1109/TDSC.2004.2).
3. Francesco Flammini (ed.), Resilience of cyber-physical systems: From risk modeling to threat counteraction. Series: Advanced Sciences and Technologies For Security Applications. Berlin-Heidelberg: Springer, 2019 (ISBN 978-3-319-95597-1, eBook; 978-3-319-95596-4).
4. International Standards Organization (2009). ISO/IEC 15408-1:2009 - Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model. [online] Iso.org. Available at: https://www.iso.org/standard/50341.html [Accessed 24 Sep. 2018]
5. JTFSCSE, Joint Task Force on Cybersecurity Education (CSE). 2015. Available Aug 15, 2018 from IEEE at https://www.csec2017.org/
6. NIST, Cybersecurity Framework. Version 1.1. Gaithersburg, MD: The National Institute of Standards and Technology (NIST), Apr 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
7. DHS, Critical Infrastructure Sectors. Homeland Security. Aug 14, 2018. Available Aug 15, 2018 from IEEE at https://www.dhs.gov/critical-infrastructure-sectors
8. Kaspersky Lab, State of Industrial Cybersecurity 2018 Survey. Kaspersky Lab, 2018. Available Aug 15, 2018 from Kaspersky at https://ics.kaspersky.com/the-state-of-industrial-cybersecurity-2018/
9. Chee-Wooi Ten, Chen-Ching Liu, and Govindarasu Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," IEEE Trans Power Systems, vol. 23, no. 4, pp. 1836-46, Nov 2008.
10. Muhammad Rizwan Asghar, György Dán, Daniele Miorandi, and Imrich Chlamtac, "Smart meter data privacy: A survey," IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2820 - 2835, 2017.
11. Witold Kinsner, “Polyscale analysis and fractional operators for cognitive systems,” in Proc. 13th IEEE International Conference on Cognitive Informatics & Cognitive Computing, ICCI*CC 2014 (London, UK; August 18-20, 2014) Paper KN5, 2014.
12. Witold Kinsner, "Is entropy suitable to characterize data and signals for cognitive informatics?" Intern. J. Cognitive Informatics and Natural Intelligence, vol. 1, no. 2, pp. 34-57, Apr-Jun 2007.
13. Witold Kinsner, “A unified approach to fractal dimensions,” Intern. J. Cognitive Informatics and Natural Intelligence, vol. 1, no. 4, pp. 26-46, Oct-Dec 2007.

14. Ian Goodfellow, Yoshua Bengio, and Aaron Courville, Deep Learning. Cambridge, MA: MIT Press, 2016. (ISBN: 978-026203561-3).

15. Yang Xin, Lingshuang Kong, Zhi Liu, Yuling Chen, Yanmiao Li, Hongliang Zhu, Mingcheng Gao, And Haixia Hou, And Chunhua Wang, "Machine Learning and Deep Learning Methods for Cybersecurity," IEEE Access, pp. 35365-81, July 19, 2018.

16. Jesus David Terrazas Gonzalez and Witold Kinsner, "Zero-crossing analysis of Lévy walks and a DDoS dataset for real-time feature extraction: Composite and applied signal analysis for strengthening the Internet-of-Things against DDoS attacks," Int. J. Softw. Sci. Computational Intelligence IJSSCI, vol. 8, no. 4, pp. 1–28, 2016. (doi: 10.4018/IJSSCI.2016100101)

17. Jesus David Terrazas Gonzalez and Witold Kinsner, "Zero-crossing analysis and information divergence of Lévy walks for real-time feature extraction," Int. J. Handheld Comput. Res. IJHCR, vol. 7, no. 4, pp. 41–59, 2016. (doi: 10.4018/IJHCR.2016100104)

18. Yosra Lakhdhar, Slim Rekhis, and Noureddine Boudriga, "Proactive security for safety and sustainability of mission critical systems," IEEE Transactions on Sustainable Computing, Feb 2018. doi:10.1109/TSUSC.2018.2810092)

19. Qiang Liu, Pan Li, Wentao Zhao, Wei Cai, Shui Yu and Victor C.M. Leung, "A survey on security threats and defensive techniques of machine learning: A data driven view," IEEE Access, vol. 6, pp. 12103-12117, 2018. (doi: 10.1109/ACCESS.2018.2805680).

20. Catriona Mairi Kennedy, Distributed Reflective Architectures for Anomaly Detection and Autonomous Recovery. Doctoral Thesis. Birmingham, UK: University of Birmingham, Jun 2003.

21. Awais Rashid, George Danezis, Howard Chivers, Emil Lupu, Andrew Martin, Makayla Lewis and Claudia Peersman, "Scoping the Cyber Security Body of Knowledge," IEEE Security & Privacy, vol. 16, no. 3, pp. 96 - 102, May/June 2018.

22. IEEE, Try-CybSI, 2018. Available Aug 15, 2018 from IEEE at http://try.cybersecurity.ieee.org/trycybsi/

23. ACM, ACM/IEEE/AIS SIGSEC/IFIP Cybersecurity Curricular Guideline. 2017. http://cybered.acm.org/

24. Hussein A. Abbass, Eleni Petraki, Kathryn Merrick, John Harvey, and Michael Barlow, "Trusted autonomy and cognitive cyber symbiosis: Open challenges," Cognitive Computation, vol. 8, no. 3, pp. 385–408, Jun 2018. (doi: 10.1007/s12559-015-9365-5).

25. Hussein A. Abbass, George Leu, and Kathryn Merrick, "A review of theoretical and practical challenges of trusted autonomy in big data," IEEE Access, vol. 4, pp. 2808-2830, June 24, 2016.

Biografia

Francesco Flammini ha ottenuto la laurea con lode in Ingegneria Informatica (2003) ed il Dottorato di Ricerca in Ingegneria Informatica e Automatica (2006) presso l'Università di Napoli Federico II. Ha avuto esperienze professionali e di ricerca sia nel mondo industriale (tra cui Ansaldo STS, Poligrafico dello Stato) che in quello accademico (tra cui University of Maryland, Linnaeus University). È attualmente membro Senior dell'IEEE, presidente del comitato tecnico IEEE SMC sulla Homeland Security, e coordinatore delle conferenze per l'iniziativa IEEE sui Symbiotic Autonomous Systems. È autore di oltre 100 pubblicazioni scientifiche su libri, riviste e atti di congressi internazionali. Il suo ultimo libro, pubblicato da Springer, si intitola "Resilience of Cyber-Physical Systems: From Risk Modeling to Threat Counteraction".

Email: flamminifra@hotmail.com