Digitalizzazione: Nuovi Rischi per la Società e per gli Ingegneri

Bruzzone Agostino - Coordinatore STRATEGOS, Laurea Magistrale in Engineering Technology for Strategy and Security dell'Università di Genova (/autori/bruzzone-agostino) 12/06/2019 1

Parlare di "nuovi" rischi per la Società legati al **cyber space** può apparire improprio, considerando che gli antesignani dei moderni **cyber attack** risalgono alla fine degli anni '80, circa un terzo di secolo fa.

Tuttavia potrebbe non essere così scorretto se pensiamo all'evoluzione del contesto globale.

Infatti, se è vero che "the Great Worm" (ndr. letteralmente il Grande Verme) liberato da Morris nel 1988, senza intento di nuocere, contaminò rapidamente il 10% dell'allora piccola rete Internet (circa 60'000 robusti sistemi Unix), oggi abbiamo una società assai più pervasa dalle componenti cyber che gestiscono funzionalità critiche.

Una rete composta da circa 23 miliardi di oggetti

Infatti, oggi la rete è composta da circa 23 miliardi di oggetti, quindi facendo un confronto rispetto a trent'anni fa, risulta circa 400 volte più evoluta di quanto non lo sia un cervello umano rispetto a quello di una zanzara.

Ovviamente questa complessità cresce, con un tasso già di per se stesso alto, che poi diventa esponenziale considerando il mondo IoT (Internet of Things), ovvero di tutti quegli oggetti dotati di connessione come smartphone, o sensori intelligenti, che vanno dai trova-oggetti ai nuovi controlli di sicurezza, dai sistemi industriali a quelli domotici.

IoE - Internet of Everything

Vi è inoltre un ulteriore concetto che si affianca agli **IoT, gli IoE (Internet of Everything)** che aggiunge, al novero dei device portatili, in primis le persone; queste risultano connesse, non solo tramite il proprio "cellulare", ma anche con la percezione delle loro scelte, azioni ed emozioni condivise in rete (e.g. tono di voce in una videoconferenza per capire le condizioni di salute, post su un social per comprendere l'apprezzamento per un tipo di forma d'arte, visita ad un sito per intuire che si sta pianificando un acquisto).

Questo non è il futuro, ma il presente e tutti noi lo sperimentiamo giornalmente quando cercando su wiki informazioni su una città Europea ci ritroviamo bombardati da inserti commerciali sulle pagine web che ci propongono una visita a quel luogo; tutto ciò ovviamente è destinato ad evolvere ulteriormente e se vi capita di trovarvi negli Stati Uniti con dei giovani universitari, non sarà raro che nel dialogo intervenga in modo naturale anche un assistente vocale intelligente (e.g. il Siri di turno) rispondendo a domande poste apertamente (e.g. ultimo film di maggior successo di Disney).

Perché dico negli Stati Uniti? Anche qui in Italia possiamo fare la stessa cosa, in fondo.

Si, possiamo farlo, ma è un poco diverso: innanzi tutto questi sistemi nascono per funzionare in lingua Inglese, sono addestrati da una popolazione di oltre 300 milioni di persone e hanno raggiunto un livello di affidabilità e precisione molto più elevato rispetto all'utilizzo in Italiano.

Questo comporta che una domanda fatta in USA riesce ad ottenere una risposta nel 70% dei casi e questa risulta completa e valida in oltre il 90%, mentre nel nostro Paese questi tassi sono ancora relativamente bassi rispetto all'utente medio.

Questo esempio serve a comprendere come nuovi sistemi, anche quando già esistenti in forme sperimentali, hanno un impatto minimo fintanto che restano imprecisi, ma non appena diventano realmente affidabili, comodi e/o convenienti, la loro diffusione diventa capillare e si inseriscono nella nostra vita quotidiana, nelle nostre case, nei nostri servizi e nei processi che regolamentano la nostra società.

Ora, in generale, questi sistemi sono fatti per migliorare la qualità della nostra vita, ridurre i costi e rendere possibile fare cose prima improponibili: organizzare una video conferenza tra più persone che si trovano in posti diversi, rendere intelligente un impianto HVAC (Heating, Ventilation and Air Conditioning) senza dover ri-cablare un intero edificio, oppure, ancora, permetterci di mantenere agganciate alla rete e redditizie alcune centinaia di Pale Eoliche distribuite sul territorio, nonostante la dinamica del contesto (e.g. cambi continui nella domanda/produzione di energia e nelle condizioni meteo).

Il successo di queste soluzioni è in qualche modo anche la loro “maledizione”: le porta a diffondersi e a rendere rapidamente insostenibile qualsiasi soluzione che se ne discosti, risultando meno efficace, più onerosa e meno flessibile. Veniamo quindi al perché qui si è utilizzata la parola “maledizione”: nel momento in cui creiamo un oggetto o un servizio di rete è evidente che lo esponiamo ad un rischio, dato che diventa potenzialmente accessibile e modificabile direttamente o indirettamente da terzi.

I rischi maggiori, in genere, nascono non solo dal piano meramente informatico ma anche dalle conseguenze che queste compromissioni comportano su altri piani e spesso su quello reale, con impatti anche sulla Safety oltre che sulla Security. E`evidente che, in questo contesto, le vulnerabilità dei cyber physical sytem, concetto divenuto molto popolare non solo con gli IoT ma anche con l’iniziativa Industry 4.0 in ambito aziendale, spesso possono andare ben oltre il singolo componente e compromettere una rete, un impianto o un sistema complesso.

Questi rischi possono articolarsi in modi differenti e a seconda dei casi possono avere maggiori o minori conseguenze in termini di impatto concreto; non bisogna quindi né diffondere allarmismi, né sottovalutare queste componenti, ma, viceversa, comprenderle, modellizzarle e creare soluzioni robuste che bilancino i rischi con gli oneri.

Si tratta in effetti di un classico esempio di Progettazione Ingegneristica che deve affrontare un mondo articolato che affianca a quello Reale quello Cyber e considera nel suo complesso processi e interazioni. Per fare questo, una soluzione fondamentale è la capacità di studiare i diversi layer che compongono il contesto e collegarli tra loro con dei modelli che ci permettano di considerarne la dinamica e di immettere minacce e difese, sperimentando tramite la simulazione come trovare soluzioni valide, efficaci e sostenibili.

Dal punto di vista delle vulnerabilità è interessante identificare alcuni degli aspetti principali che possono venire compromessi, tra i quali vale la pena di ricordare:

Accessibilità:

ovvero viene reso indisponibile un oggetto o un servizio, per esempio non si riesce più a connettersi ad un sito per fare un biglietto ferroviario (e.g. un DDoS Distributed Denial of Service generato da una rete di macchine attaccanti che costituiscono un botnet che genera una enormità di richieste al server delle ferrovie saturandolo come avvenuto nel maggio 2018 in Danimarca).

Integrità:

ovvero i dati che vengono generati o trasmessi da un elemento vengono alterati con la conseguenza che forniscono indicazioni inutilizzabili (e.g. un data base viene crittato in modo da diventare illeggibile al suo proprietario come nel caso del ramsonware CryptoLocker) oppure fuorvianti come nel caso di un termometro digitale che fornisce un dato completamente errato al sistema di condizionamento e impone di continuare a raffreddare un vano già ben al di sotto della temperatura desiderata.

Confidenzialità:

in questo caso i dati confidenziali sono carpiti da terze parti in violazione dei relativi vincoli, come nel caso di fishing a collaboratori di un alto funzionario che opera su dati confidenziali (e.g. email fasulle che sembrano provenire dal server di posta con la richiesta di cambiare password, ma che in realtà la carpiscono) che a quel punto possono essere raccolti nelle email al fine di darne diffusione.

Privacy:

in questo caso i dati sono personali e resi accessibili (o trasmessi) a soggetti terzi, come nel caso di una serie di smart tv che, con le telecamere interne, riprenda in modo occulto le persone poste davanti allo schermo e trasmetta le immagini ad un’azienda interessata a valutare il target degli spettatori (e.g. distinguendo tra uomini, donne, anziani e bambini) su un campione esteso e nell’arco della giornata.

Gli esempi riportati si sono già verificati a dimostrazione dell’esistenza di queste vulnerabilità e come sempre, viviamo una competizione in continua evoluzione tra la “spada” di chi attacca e lo “scudo” di chi difende, mentre ad ogni nuova violazione corrisponde una correzione delle soluzioni ICT.

Tuttavia, è molto importante comprendere che il problema non riguarda solo l’informatica: l’uomo è spesso un elemento chiave nell’equazione che regola la sicurezza e i rischi conseguenti. In questo contesto si usa il termine Social Engineering, ovvero lo studio dei comportamenti umani che spesso possono agevolmente compromettere anche i sistemi più tecnologicamente sicuri; ricordiamo come esempio più comune il fatto di sapere che le password del computer vengano scritte sotto la tastiera oppure il lasciar cadere nel parcheggio di una azienda una flash memory allettante (e.g. 64 GB) che magari contiene un virus nascosto da un rootkit (programma di mascheramento aree accessibili).

Risulta quindi evidente che oggi vi sono molti rischi emergenti, legati al settore Cyber, i quali colpiscono la Società e le Persone e che crescono nella misura in cui servizi e sistemi diventano sempre più interconnessi e legati ad una supervisione remota, spesso automatizzata da sistemi intelligenti e/o autonomi.

Questi rischi diventano quindi campo di cimento per gli Ingegneri che li debbono affrontare e devono progettare e sviluppare soluzioni efficaci per prevenirli e contenerli tramite un approccio sistemico.

Per conseguire questo risultato è necessario innanzi tutto che gli Ingegneri siano consci di questo pericolo, lo conoscano tecnicamente tramite costante aggiornamento, non solo sugli aspetti informatici, ma anche sugli sviluppi dei nuovi sistemi e relativi cyber physical system. E` altrettanto importante che costoro sappiano sensibilizzare il mondo degli utenti fornendo una visione realistica sia delle minacce che delle possibili soluzioni e relativi punti di forza e di debolezza. Come sempre è altrettanto critico possedere la consapevolezza che i rischi non possono essere eliminati totalmente e che la sostenibilità delle soluzioni deve considerare aspetti legati ai costi, all’affidabilità e convenienza e, particolarmente, alle caratteristiche della componente umana coinvolta e relativa formazione.

Sotto questo profilo (e ad alto livello) oggi si assiste ad una evoluzione verso una visione dove le minacce non sono semplicemente Cyber, ma piuttosto Hybrid: ovvero minacce che agendo su molteplici livelli (quello cyber e quello mediatico sono sicuramente i più dinamici) è possibile attaccare le vulnerabilità di sistemi complessi. Un esempio è il caso delle azioni mediatiche e cyber che hanno afflitto la popolazione dell’Ucraina rimasta più volte con diversi milioni di persone senza corrente elettrica per ore.

Purtroppo, questi eventi sono spesso causati anche dall’impreparazione degli alti responsabili, i quali hanno una visione specifica su alcuni sistemi o reti specifiche, e non comprendono che un attacco trasversale, soprattutto se coordinato su un aspetto particolare, può essere dirompente. Per esempio, congestionare il traffico stradale non richiede enormi sforzi, ma può rendere inaccessibile un’area ai soccorsi, per inciso questo fenomeno tende a verificarsi anche “naturalmente” durante la crisi quindi basta incentivarlo con azioni opportune. In modo analogo, togliere l’energia elettrica mette immediatamente in crisi buona parte delle organizzazioni, anche quelle critiche (e.g. ospedali e strutture militari) dato che molto spesso gli UPS non sono mantenuti operativi ed hanno capacità molto limitate rispetto alle esigenze reali, anche per mere ragioni di tagli del budget occorsi negli anni.

Il contesto ibrido aggiunge alcuni elementi al problema che un ingegnere deve affrontare. Nel prossimo futuro è un elemento che dovremo considerare, non solo per i

casi di mirabolanti azioni terroristiche, che speriamo restino confinate a rare eccezioni, ma anche per gli impatti nelle casistiche di incidenti di routine. Pensiamo infatti al caso ipotetico di un incidente in un impianto industriale che porti a generare una

fumata in città; i social, anche se non manipolati intenzionalmente, reagiscono comunque sulla base delle percezioni delle persone e il loro impatto tende ad aumentare. Quindi la nube, magari non particolarmente tossica, per una sfortunata serie di coincidenze e grazie alla velocità con cui informazioni, immagini e sensazioni si diffondono nella popolazione, può generare il panico. Infatti, se questa viene percepita come pericolosa, tramite false notizie relative alla gravità e tossicità del composto, potrebbe avere un enorme impatto mediatico e di conseguenza sul tessuto cittadino e sui diversi layer (e.g. blocco traffico, saturazione ospedali).

I nostri giovani ingegneri dovranno quindi lavorare sempre più fianco a fianco con i diversi “attori” per fornire sistemi e strumenti capaci di affrontare queste crisi, prevenirle ove possibile e mitigarle: ad esempio, aggredendo le sorgenti di panico con tools e applicazioni efficaci in misura non minore di quelle legate a contenere l’incidente stesso.

Sotto questo profilo, una tecnologia abilitante è evidentemente il ricorso alla Simulazione, con particolare attenzione al paradigma MS2G (Modeling, interoperabile Simulation & Serious Games) che consente di combinare modelli differenti facendoli interoperare all’interno di un mondo immersivo, intuitivo e interattivo come quello supportato dall’approccio tipico dei Serious Games; in questo modo modelli fisici di fenomeni come incendi, esplosioni, diffusioni di composti pericolosi, possono interagire con simulazioni della reazione della popolazione, dei social media e delle azioni di contenimento condotte sul campo dai first responders creando scenari complessi. E’ evidente che questo approccio richiede una capacità di sviluppare la soluzione, impiegare i modelli e conoscere i diversi contesti specifici.

Le immagini fornite rappresentano il caso di modelli capaci di studiare le vulnerabilità di un sistema complesso; nelle figure si fa riferimento al caso di una Infrastruttura critica in un contesto portuale e collegata ad un gruppo aziendale a fronte di possibili minacce sia nel mondo reale che cyber; T-REX consente di investigare gli scenari e testarli per identificare sia dal punto di vista tecnologico che procedurale le soluzioni più efficaci per mitigare questi rischi

Figura 1. Rappresentazione del Cyberspace ove ciascun nodo è caratterizzato tramite una rappresentazione immersiva di flussi e livelli specifici di Accessibilità, Integrità, Confidenzialità e Privacy

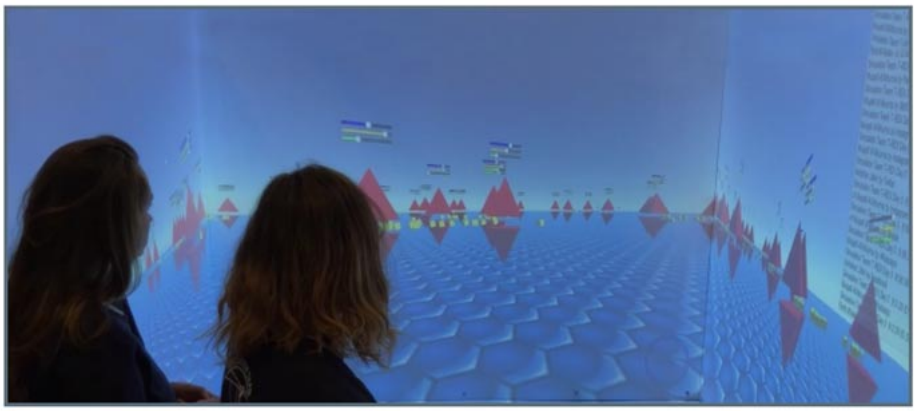

Figura 1. Rappresentazione del Cyberspace ove ciascun nodo è caratterizzato tramite una rappresentazione immersiva di flussi e livelli specifici di Accessibilità, Integrità, Confidenzialità e Privacy

Figura 2. Sistema di Simulazione T-REX che propone un’attacco combinato cyber e con droni ad un infrastruttura critica

Figura 2. Sistema di Simulazione T-REX che propone un’attacco combinato cyber e con droni ad un infrastruttura critica

References

- Balaji, N., (2018). Massive DDOS Attack on Denmark Railway System that Make Impossible to Buy a Train Ticket, GB Hackers on Security, May 16
- Bruzzone A.G. (2018). MS2G as Pillar for Developing Strategic Engineering as a New Discipline for Complex Problem Solving, Keynote Speech at I3M, Budapest, September

- Bruzzone A.G. (2017). Information Security: Threats and Opportunities in a Safeguarding Perspective, Key Note Speech at World Engineering Forum, Rome, November
- Bruzzone A.G., (2017). Smart Simulation: Intelligent Agents, Simulation and Serious Games as enablers for Creating New Solutions in Engineering, Industry and Service of the Society. Keynote Speech at International Top-level Forum on Engineering Science and Technology Development Strategy- Artificial intelligence and simulation, Hangzhou, China
- Bruzzone A.G., Agresta M., Sinelshchikov K. (2017). Simulation as Decision Support System for Disaster Prevention, Proc. of SESDE, Barcelona
- Bruzzone A.G., Massei M., Longo F., Cayirci E., di Bella P., Maglione G.L., Di Matteo R. (2016). Simulation Models for Hybrid Warfare and Population Simulation, Proc. of NATO Symposium on Ready for the Predictable, Prepared for the Unexpected, M&S for Collective Defence in Hybrid Environments and Hybrid Conflicts, Bucharest, October 17-21
- Chen, Y., Kar, S., & Moura, J. M. (2017). Optimal attack strategies subject to detection constraints against cyber-physical systems. IEEE Transactions on Control of Network Systems, 5(3), 1157-1168.
- Eisenberg, T., Gries, D., Hartmanis, J., Holcomb, D., Lynn, M. S., & Santoro, T. (1989). The Cornell commission: on Morris and the worm. Communications of the ACM, 32(6), 706-709.
- Lueth, K.L. (2018). State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating, IoT Analytics, August 8
- Murnan, K. (2018). Dumb And Dumber: Comparing Alexa, Siri, Cortana And The Google Assistant, Forbes, May 3
- Wang, W., & Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. Computer networks, 57(5), 1344-1371.

Leggi anche

» L'informazione nell'era delle reti 5G: cosa ci aspetta? (/23225-linformazione-nellera-delle-reti-5g-cosa-ci-aspetta)
» Sensori e IoT per l'ambiente costruito. Ad Ancona un centro di eccellenza internazionale (/23418-sensori-e-iot-per-lambiente-costruito-ad-ancona-un-centro-di-eccellenza-internazionale)
» AICARR: Sistemi di automazione integrata e reti di comunicazione (/23435-aicarr-sistemi-di-automazione-integrata-e-reti-di-comunicazione)
» Dall'edificio alla Smartcity:come garantire la sicurezza nelle soluzioni digitali per la sostenibilità ambientale (/23463-dalledificio-alla-smartcitycome-garantire-la-sicurezza-nelle-soluzioni-digitali-per-la-sostenibilita-ambientale)
» Dal diritto alla connessione al 5G: viaggio nel Futuro Ultraveloce (/23479-dal-diritto-alla-connessione-al-5g-viaggio-nel-futuro-ultraveloce)

TAGS IoT Internet of Things (/tag/iot-internet-of-things)

Il Magazine

(/23384)

News

Vedi tutte (/Archivio/News)

Premio Ilaria Rambaldi, ecco i vincitori delle tesi più innovative su prevenzione e ricostruzione (/23766-premio-ilaria-rambaldi-ecco-i-vincitori-delle-tesi-piu-innovative-su-prevenzione-e-ricostruzione)

Lombardia: Nuovi indirizzi per la programmazione degli interventi a favore del patrimonio scolastico (/23772-lombardia-nuovi-indirizzi-per-la-programmazione-degli-interventi-a-favore-del-patrimonio-scolastico)

LEGAL BIM: la collaborazione nei Contratti Pubblici spiegata in 10 punti (/23773-legal-bim-la-collaborazione-nei-contratti-pubblici-spiegata-in-10-punti)

IUSS di Pavia: 4 borse di studio per il corso Civil Engineering for Mitigation of Risk from Natural Hazards (/23774-iuss-di-pavia-4-borse-di-studio-per-il-corso-civil-engineering-for-mitigation-of-risk-from-natural-hazards)

Le giornate della prevenzione incendi: opportunità, responsabilità e nuovi traguardi del "Codice" (/23775-le-giornate-della-prevenzione-incendi-opportunita-responsabilita-e-nuovi-traguardi-del-codice)

Indici sintetici di affidabilità fiscale (ISA) dei professionisti: ecco il software per il calcolo preciso (/23755-indici-sintetici-di-affidabilita-fiscale-isa-dei-professionisti-ecco-il-software-per-il-calcolo-preciso)

Autostrade: in arrivo il vademecum del MIT ai concessionari per la sicurezza dei viadotti (/23756-autostrade-in-arrivo-il-vademecum-del-mit-ai-concessionari-per-la-sicurezza-dei-viadotti)

Porticato: quando serve il permesso di costruire? Le discriminanti (/23757-porticato-quando-serve-il-permesso-di-costruire-le-discriminanti)

Modelli organizzativi e certificazione: Strumenti utili per la prevenzione della corruzione? (/23759-modelli-organizzativi-e-certificazione-strumenti-utili-per-la-prevenzione-della-corruzione)

Si assumono architetti, ingegneri e geometri: ecco i concorsi di giugno e luglio (/23760-si-assumono-architetti-ingegneri-e-geometri-ecco-i-concorsi-di-giugno-e-luglio)

Il più importante Portale di Informazione Tecnico Progettuale al servizio degli Architetti, Geometri, Geologi, Ingegneri, Periti, professione tecnica, Albo Professionale, Tariffe Professionali, Norme Tecniche, Inarcassa, Progetto Strutturale, Miglioramento Sismico, Progetto Architettonico, Urbanistica, Efficienza Energetica, Energie rinnovabili, Recupero, Riuso, Ristrutturazioni, Edilizia Libera, Codice Appalti, Progetto Impianti termotecnici, Modellazione Digitale e BIM, Software Tecnico, IOT, ICT, Illuminotecnica, Sicurezza del lavoro, Sicurezza Antincendio, Tecnologie Costruttive, Ingegneria Forense, CTU e Perizie, Valutazioni Immobiliari, Certificazioni.

INGENIO-WEB.IT è una testata periodica di IMREADY Srl registrata presso la Segreteria di Stato per gli Affari Interni di San Marino con protocollo n. 638/75/2012 del 27/4/2012. Direttore Responsabile: Andrea Dari.

IMREADY Srl, Strada Cardio, n.4, 47891 Galazzano, RSM, Tel. 0549 909090
Mail segreteria@imready.it (mailto:segreteria@imready.it)