TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

MACROAREA INGEGNERIA

COMUNICATO STAMPA

CYBER4HEALTH

PRESENTATO A INGEGNERIA ROMA "TOR VERGATA"
L'OSSERVATORIO SULLE VULNERABILITÀ CYBER E FISICHE DEI DISPOSITIVI MEDICI

*Un punto di vista **multidisciplinare** sulla **tematica emergente della cybersicurezza** in ambito medico per intervenire by design fin dalla progettazione.*

.

Nell'ambito delle attività di ricerca svolte in collaborazione con il **Centro di Competenza Cyber 4.0**, l'**Università di Roma "Tor Vergata"** ha realizzato l'**Osservatorio "C4H - CYBER4HEALTH",** una **piattaforma per la sicurezza informatica dei dispositivi medici**, tra le prime al mondo nel suo genere, finalizzata a fornire una base di **conoscenze tecniche e legislative** sulla **vulnerabilità dei dispositivi medici**, soprattutto **wireless**, rispetto a eventuali **attacchi informatici** ed **elettromagnetici**.

"CYBER4HEALTH", che si rivolge in particolare a **sviluppatori tecnologici**, **integratori di sistemi, gestori di servizi, ospedali** ma anche ai **pazienti**, è stata presentata **mercoledì 17 maggio** presso la **Macroarea di Ingegneria dell'Università Roma "Tor Vergata"** (Aula Convegni, Edificio Didattica, Piano Terra), nell'ambito del workshop durante il quale sono stati **presentati i primi risultati ottenuti** con una dimostrazione dal vivo dell'utilizzo della piattaforma informatica.

Sono intervenuti, tra gli altri, il **rettore dell'Università di Roma "Tor Vergata"** Nathan Levialdi Ghiron, il **prorettore al Trasferimento Tecnologico dell'Università di Roma "Tor Vergata"**, Vincenzo Tagliaferri, il **presidente di Cyber 4.0**, **Università La Sapienza di Roma**, Leonardo Querzoni.

«Possiamo distinguere due tipi di security, la **Cybersecurity**, che riguarda la protezione nei confronti di attacchi di natura software e la **Sicurezza Fisica**, che riguarda la protezione nei confronti dell'hardware, la parte elettronica dei dispositivi medici», ha chiarito fin da subito Francesca Nanni, **dottoranda in Ingegneria medica all'Università di Roma "Tor Vergata che ha lavorato alla realizzazione dell'Osservatorio Cyber4Health**.

I dispositivi medici, a partire dagli apparati diagnostici ospedalieri fino ai sistemi elettronici indossabili e a quelli impiantabili nel nostro corpo, costituiscono un imprescindibile strumento per la cura e la salute della persona, sia in ambiente ospedaliero sia in quello domestico. La loro rapida evoluzione li ha portati a incrociare le traiettorie delle tecnologie wireless e dei sistemi di Intelligenza Artificiale: se da un lato questo ha permesso di realizzare strumenti sempre più all'avanguardia per la salute dei pazienti, dall'altra moltiplica l'eventualità di possibili **rischi per la sicurezza informatica e fisica dei dispositivi**, rischi legati proprio alla varietà delle interazioni con l'esterno che questi strumenti rendono possibile.

CLASSIFICAZIONE DEI DISPOSITIVI E METODO CVSS, IL PUNTEGGIO DI VULNERABILITÀ

«La piattaforma, il cuore dell'Osservatorio, è stata realizzata anche con la collaborazione del **Laboratorio di Elettromagnetismo Pervasivo di "Tor Vergata"** della **Macroarea di Ingegneria**. Se da un alto intende **offrire un servizio** non solo alle aziende ma a tutti coloro che si occupano dello sviluppo, della certificazione, della manutenzione e della messa in commercio riguardo alle attuali vulnerabilità, dall'altro ha l'obiettivo di **innalzare il livello di consapevolezza** dell'utente finale, ovvero medici e pazienti», ha affermato Francesco Lestini, **dottorando in ingegneria medica a "Tor Vergata" che ha lavorato alla realizzazione della piattaforma**.

L'Osservatorio raccoglie dati sui dispositivi esistenti nel settore medicale proveniente, al momento, da organizzazioni governative e articoli scientifici. e **fornisce in tempo reale il numero delle vulnerabilità dei dispositivi medici** e degli **attacchi informatici rilevati**, assegnando ai sistemi utilizzati un **punteggio di vulnerabilità**, "**Common Vulnerability Scoring System (CVSS)"**: «un metodo che non misura il rischio ma la **gravità delle vulnerabilità** scoperte, con la possibilità per industrie, organizzazioni e governi di definire delle priorità per le attività di risoluzione di tali vulnerabilità», ha spiega Gaetano Marrocco, **professore ordinario di Campi Elettromagnetici, Università di Roma "Tor Vergata" e coordinatore del corso di studi in Ingegneria Medica**, **Dipartimento di Ingegneria Civile e Ingegneria Informatica,** che ha organizzato il workshop e moderato l'evento.

La **piattaforma classifica i dispositivi** rispetto ad alcuni campi individuati dai ricercatori di "Tor Vergata: in base al **distretto corporeo di applicazione** (stomaco, suore, etc), rispetto alla **tipologia di dispositivi** (pacemaker, risonanza magnetica, rete ospedaliera, etc.). al tipo di attacco cyber (eavesdropping, sniffing, accesso non autorizzato, etc,), rispetto alla **tipologia generica del dispositivo** (impiantato, wearable, smartwatch, dispositivi ospedalieri), in base **all'anno** della **vulnerabilità**, al **tipo di vulnerabilità** (cyber o fisica), ma soprattutto sulla base della **gravità della vulnerabilità** (CVSS) e sulla **classe di rischio,** quattro le classi dal punto di vista della sicurezza del paziente.

ATTACCHI INFORMATICI: DAI SISTEMI INFORMATIVI OSPEDALIERI AI PACEMAKER

«Ho chiesto di scrivere a ChatGPT un comunicato stampa datato 17 maggio 2028 – ha aperto così il suo intervento il professor Giuseppe Bianchi, **ordinario di Telecomunicazioni a "Tor Vergata"**. «Lo scenario descritto dall'Intelligenza Artificiale riguardo a probabili attacchi informatici dei dispostivi medici, seppur realistico, probabilmente non si verificherà perché l'attaccante, che in genere agisce per soldi o per distruggere infrastrutture critiche durante, ad esempio, conflitti bellici, sembra avere altri obiettivi rispetto a quello costituito dalla salute dell'individuo. Quello che però potrebbe succedere – continua Bianchi - è **l'evoluzione dei ransomware**, predetto già una decina di anni fa. Nel momento in cui passiamo all'Internet delle Cose (IoT) il rischio è che gli attacchi ransomware, che oggi colpiscono i dati, possano bloccare invece gli oggetti e quindi l'attaccante possa chiedere un riscatto semplicemente per sbloccare una lavatrice, il frigorifero oppure un dispositivo medico».

In campo medico le disfunzioni causate oggi ai **sistemi informativi degli ospedali**, spesso oggetto di attacchi hacker con richieste di riscatto, potrebbero però affliggere in un futuro non lontanissimo anche **neuro-stimolatori**, **pacemaker**, **pompe di insulina** e **defribillatori**, con conseguenze ben più dannose per la privacy e la salute del paziente. «Il tema della **sicurezza cyber-fisica** dei **dispositivi medici** assume una significativa rilevanza per produttori, ospedali e pazienti soprattutto nell'attuale e futuro scenario di crescente interconnessione», sottolinea il **professor Marrocco**. «Inoltre, i dispositivi medici del futuro saranno sempre più biointegrati, pensiamo all'utilizzo di protesi sensorizzate, e questo moltiplicherà la numerosità dei dispositivi medici impiegati».

DIFFONDERE UNA CULTURA DI CYBERSICUREZZA BY DESIGN

L'Osservatorio vuole stimolare una cultura di **"Cyber-Physical Security by Design"** che, partendo dalla conoscenza delle problematiche già accertate o plausibili, possa **mitigare i rischi già nella fase di definizione del dispositivo medicale** e della catena di valore da esso abilitata. Il workshop, che si è articolato in una sessione più tecnica e una più regolatoria, ha fornito un punto di vista **multidisciplinare** sulla **tematica emergente della cybersicurezza** in ambito medico grazie alla partecipazione di relatori e relatrici del mondo scientifico, regolatorio, legislativo e industriale: uno scenario che ben rappresenta la complessità dello stato dell'arte e le tante sfide ancora aperte, offrendo utili spunti di riflessione e discussione.

SAFETY VS SECURITY

Dai numerosi interventi che si sono avvicendati durante il workshop è emerso che tra i **principali motivi di vulnerabilità** nel campo dei dispostivi medici c'è l'obsolescenza tecnologica e la mancanza di aggiornamenti dei sistemi embedded, come ad esempio il macchinario per la TAC, o a livello software (*patching*) e che spesso i dispositivi risultano ingegnerizzati bene per garantire la **safety** ma non altrettanto bene per garantire la **security**. Cosa fare allora? Innanzitutto cominciare a diversificare le reti su cui viaggiano le informazioni e fare in modo che i tempi dei processi di aggiornamento e quelli di certificazione vadano di pari passo.

Il programma del workshop è disponibile alla pagina http://www.pervasive.ing.uniroma2.it/Alab_people_marrocco_files/CyberWorkshop/C4H_workshop.html

Roma, 17/05/2023

Pamela Pergolini
Giornalista - PhD SciComm
Ufficio Stampa e Comunicazione
Università di Roma "Tor Vergata" - Ingegneria
Via del Politecnico, 1 00133 Roma
pamela.pergolini@uniroma2.it
06.7259.7735 + 39 320.4375681
@ing_torvergata @pamelapergolini