Il Giornale dell'Ingegnere
Mensile
Tiratura: 22.439
Diffusione: 21.885

"Ponte sullo Stretto di Messina, la porta principale per entrare in Europa"

Il ponte sullo Stretto di Messina sarà "un'opera avveniristica", come molti stanno ripetendo da tempo. Una sfida di alta ingegneria, con l'inizio dei cantieri che – si spera – avverrà entro l'estate 2024

PAG. 2

INTERVISTA |

La rivoluzione digitale passa anche dal merito

Silvia Lucia Sanna, 3^ classificata del Premio tesi di laurea Ingenio al femminile 2022 con "A Risk Estimation Study of Native Code Vulnerabilities in Android Applications"

PAG. 16

Il Giornale dell'Ingegnere
Mensile

INGENIO AL FEMMINILE

La rivoluzione digitale passa anche dal merito

A tu per tu con Silvia Lucia Sanna, terza classificata del Premio tesi di laurea Ingenio al femminile 2022

DI DANIELE MILANO

"Quando ho ricevuto l'e-mail di Guido Rozzano del CNI con cui mi comunicava di essermi aggiudicata il terzo premio di *Ingenio al femminile* l'ho istintivamente chiamato, pensando 'Non vorrei mai ci ripensassero!'. Non immaginavo davvero che la mia tesi venisse considerata tanto interessante e utile da ottenere un così prestigioso riconoscimento: aveva ragione il mio relatore (Davide Maiorca, che ringrazio molto) a sostenere la 'bontà' del lavoro! E poi, sogno nel sogno, la cerimonia di premiazione a Roma, una delle città che più amo al mondo!". È ancora notevolmente entusiasta e orgogliosa Silvia Lucia Sanna (per tutti Silvia), "medaglia di bronzo" al Premio "in rosa" promosso dal Consiglio Naziona le Ingegneri.

A Risk Estimation Study of Native Code Vulnerabilities in Android Applications è il titolo della sua tesi di laurea, discussa nell'ambito del corso di Ingegneria Informatica dell'Università di Cagliari, e rispondente alla "Missione 1" del PNRR "Digitalizzazione, innovazione, competitività, cultura e turismo", e, nello specifico, alla "Componente 1: digitalizzazione, innovazione e sicurezza della pubblica amministrazione".

... MA LE APP SONO SICURE?

La tesi di Silvia Sanna analizza le vulnerabilità nel codice nativo delle *app Android*. Attualmente Android è il sistema operativo mobile più diffuso, perciò le sue app sono le più scaricate. La maggior parte delle applicazioni necessitano di librerie scritte in C/C++ per interagire con attività o componenti nativi come la fotocamera e, infatti, molte delle librerie riguardano l'elaborazione di immagini, usate nei *social network* o app di *gaming*. Il codice C/C++ talvolta può presentare specifiche vulnerabilità in alcune funzioni che, elaborando male un *input* o fornendo un input malevolo, consentono di entrare nella memoria e leggere, modificare, inserire dei dati, talvolta anche del codice malevolo. Un notevole numero di vulnerabilità è pubblicato in diversi *database* sotto il nome di CVE e, secondo uno studio recente, in media gli sviluppatori impiegano 2 anni per aggiornare e rendere sicure le app. Le librerie C/C++ nelle app Android non sono puro codice bensì file ELF (binari), dunque un codice compilato che non è facilmente leggibile senza opportuni *tool* di *reverse engineering* come Ghidra.

Lo studio ha avuto l'obiettivo di identificare innanzitutto i binari presenti nelle app e associarli a una lista di 15 librerie (prodotti) molto note, vulnerabili e diffuse nel nostro *dataset* (100.000 app scaricate da Androzoo). L'identificazione è stata possibile grazie a una chiara e univoca sintassi presente nelle stringhe e nel nome delle funzioni, direttamente associabile a ogni prodotto. In più, ogni funzione per essere definita vulnerabile deve essere accessibile e quindi chiamata da almeno un indirizzo del binario. I database pubblici di CVE non contengono tutte le informazioni utili allo studio in modo accessibile: abbiamo dovuto perciò creare un database contenente per ogni CVE il nome e la versione del prodotto vulnerabile, il nome della funzione vulnerabile, la data di rilascio e i punteggi di vulnerabilità (impatto e sfruttabilità) definiti dal CVSS. La versione e la funzione vulnerabili non compaiono in un campo specifico e unico come gli altri valori bensì nella descrizione, scritta in inglese naturale. Sono dunque necessarie delle tecniche di *Natural Language Processing* applicate all'informatica, usando i criteri *standard* con cui noi programmatori chiamiamo le funzioni e come noi umani le riconosciamo. Per accertare la presenza di una CVE nella libreria e, quindi, anche nell'app analizzata, abbiamo confrontato che la versione della libreria appartenesse alle versioni vulnerabili pubblicate nella CVE e che anche la funzione fosse presente. A causa delle tecniche di offuscamento e per via dei binari senza simboli di *debug*, talvolta non è facile riconoscere il nome delle funzioni, dunque è necessario un approccio probabilistico che valuti il rischio. Dalla norma ISO 27005:2008 abbiamo indicato il rischio come il prodotto di minaccia, vulnerabilità e impatto. La minaccia è la facilità con cui un attacco può essere svolto, quantificato nel CVSS dal valore sfruttabilità senza considerare le capacità dell'attaccante; la vulnerabilità possiamo identificarla come la CVE stessa ma in termini quantitativi come la sua probabilità, con valore massimo 1 se la versione e funzione compaiono nel database di CVE e nell'app; l'impatto è il danno causato al sistema se la vulnerabilità viene sfruttata, indicato da CVSS.

Nello studio del rischio abbiamo analizzato circa 5.000 app e nessuna di queste ha presentato forti criticità: mediamente le app sono sicure. In più lo studio è stato applicato a un dataset di app di pagamento (infrastruttura critica) dove in una sola app su 7 è presente una vulnerabilità. Se l'app non fosse sufficientemente protetta probabilmente un attaccante potrebbe reperire anche informazioni sensibili. Lo studio sarà sicuramente ampliato sulla parte di attacco non affrontato nella tesi.

FORMAZIONE & MERITOCRAZIA, PRIMA DI TUTTO

25 anni, nata a Sassari, Silvia è una ragazza poliedrica: "prima di scoprire nell'intelligenza artificiale e nella sicurezza informatica le mie grandi passioni, pensavo, una volta conseguita la laurea triennale, di realizzare effetti speciali per videogiochi e film, complice il mio amore per questi due 'mondi'. Da 3 anni, dopo aver seguito il progetto '*CyberChallenge.IT*', partecipo, con il *team Srdnlen*, a diverse '*CTF* (*Capture-The-Flag*)', gare di sicurezza informatica, ispirate ai giochi 'sparatutto', in cui - tramite la modalità ludica - vengono proposti problemi più o meno complessi della sicurezza informatica con l'obiettivo di trovare un segreto (*flag*) nascosto. Principalmente mi occupo di *Digital Forensics*, una serie di tecniche utilizzate anche nella vita quotidiana dagli esperti per recuperare informazioni dai dispositivi digitali a seguito di un incidente informatico (nelle gare viene simulato). Lo scorso anno durante i *training* di *openECSC* (la competizione europea di sicurezza informatica aperta a tutte e tutti, senza distinzione di età, etnia e sesso) mi sono classificata in *top 3 women*".

Sul fronte lavorativo Silvia dimostra già di sapersi re-inventare: "Il mio grande sogno è sempre stato quello di fare la poliziotta *hacker*, il 'genio dei *computer*' e di arrestare criminali, ma purtroppo sono celiaca e al momento chi è affetto da questa patologia non può partecipare ai concorsi per le forze armate o, meglio, potrebbe ma non verrebbe giudicato idoneo. Così sto ridisegnando il mio futuro, prendendo un dottorato in modo da poter giocare più carte. Di sicuro uno dei miei obiettivi è lavorare per il mio territorio, che, credo, abbia tutte le potenzialità per diventare un centro di eccellenza, sfruttando al meglio le sue capacità, specialmente il Nord (la mia zona di origine), molto spesso sottovalutato, dimenticato e lasciato a sé stesso".

La tesi di Silvia Sanna è "tangenziale" al tema della transizione *digital*: una recente ricerca dell'Osservatorio Agenda Digitale della *School of Management* del Politecnico di Milano ha evidenziato come, nonostante i piani del PNRR, l'Italia rimanga sotto la media europea sul fronte della PA digitale, attestandosi in 22^ posizione su 27 Paesi europei per sforzi compiuti nell'attuazione dell'Agenda Digitale e 20esima per risultati ottenuti. Quale potrebbe essere quel *quid* in grado di far uscire il nostro Paese da questa situazione di stallo? "Purtroppo c'è molta arretratezza tecnologica: non solo da parte degli 'utenti cittadini', ma anche degli 'utenti aziende, imprese ed enti pubblici'. È sotto gli occhi di tutti che l'insegnamento dell'informatica e della tecnologia dovrebbe partire sin dalla scuola elementare: come riconoscere e difendersi dai pericoli informatici, l'abc della *cyber security*... adattati ovviamente a seconda del *target*. In generale, la tecnologia, come tutte le invenzioni, va saputa usare: ovviamente non possiamo svegliarci un giorno e pensare di digitalizzare tutto se non abbiamo le infrastrutture, preposti e utenti formati sia per la gestione che per l'uso".

Un altro limite, riguardo i tecnici, sta nella (sempre tristemente in voga) fuga di cervelli e Silvia parla per esperienza diretta: "un anno fa ho conseguito la laurea magistrale, in lingua inglese, in *Computer Engineering, Cybersecurity and Artificial Intelligence*, ottenendo il massimo dei voti. Per diversi mesi ho ricevuto offerte di tirocini a 700 euro netti al mese (senza giorni di ferie, malattia, permessi, né contributi), per giunta in città dall'altissimo costo di vita come Milano e Roma. Come, avendone l'occasione, non trasferirsi all'estero? Ecco, anche la digitalizzazione delle PA passa dall'evitare la fuga di giovani e capaci menti; quando in Italia verranno finalmente riconosciute e apprezzate molte qualità, si potrà pensare a innovare il Paese, svecchiandolo concretamente. Senza dimenticare un'altra strada percorribile per aumentare l'evoluzione digitale: coinvolgere maggiormente le donne in ambito tecnologico-ingegneristico, ascoltando i loro bisogni, istituendo opportuni premi, compensi, diritti".