Programma Operativo Nazionale 2014-2020
Dottorati di ricerca su tematiche dell'innovazione e green
D.M. n. 1061 del 10 agosto 2021

Università degli Studi di Napoli Federico II
Dottorato di Ricerca in Information Technology and Electrical Engineering XXXVII CICLO
TEMATICHE INNOVAZIONE (AZIONE IV.4)

BORSA N. 2 - Dottorando NICOLA D'AMBROSIO

Titolo del progetto:

"Rilevamento della presenza di entità malevole all'interno di reti sociali"

SETTORE SNSI: Agenda Digitale, Smart Communities, Sistemi di mobilità intelligente
SETTORE PNR: Sicurezza per i Sistemi Sociali

Motivazioni

Internet svolge un ruolo sempre più determinante nella società contemporanea. Le reti sociali, che rappresentano una delle cosiddette *killer application* in rete, continuano a mostrare un tasso di crescita di tipo esponenziale. Non è un caso, dunque, che siano proprio le reti sociali l'oggetto di preponderante interesse da parte di utenti cosiddetti "malevoli". Le Online Social Networks (OSN) sono, a tutti gli effetti, uno dei principali vettori di attacco sfruttati dagli hacker, nonché un fondamentale strumento di aggregazione anche di quelle comunità di utenti accomunati da intenti criminosi, o, più in generale, il cui comportamento si discosti in modo significativo dai comuni principi dell'etica. È bene ricordare che questo tipo di attività non ha ripercussioni esclusivamente nel contesto delle reti informatiche. Il crimine informatico, infatti, come riportato nel documento *quadro strategico nazionale per la sicurezza dello spazio cibernetico* pubblicato dall'AgID, è una piaga che può decretare il fallimento delle aziende e la sottrazione del loro patrimonio tecnologico. Per tale ragione, risulta fondamentale individuare delle strategie di difesa innovative ed efficaci per i nostri sistemi, favorendo l'individuazione di attività illecite o, comunque, malevole.
Le tecniche in questione dovranno essere in grado di individuare in maniera proattiva eventuali minacce informatiche all'interno delle reti sociali e, quindi, garantire la sicurezza e l'integrità della collettività (come chiaramente espresso nelle Linee della Strategia Nazionale di Specializzazione Intelligente - *Azione IV.4, area di specializzazione regionale n. 10 "Smart, Secure and Inclusive Communities"*).

b. Obiettivi

L'obiettivo del progetto di ricerca, a causa dell'elevata eterogeneità delle minacce informatiche che si possono individuare all'interno delle reti sociali, deve essere raggiunto lavorando su più fronti contemporaneamente.
Innanzitutto, devono essere individuate delle tecniche automatizzate per la raccolta ed il trattamento dei dati provenienti da fonti pubbliche. Con il termine trattamento si fa

riferimento all'individuazione di correlazioni di interesse tra i dati raccolti, che possano permettere l'individuazione di pattern comportamentali malevoli all'interno delle OSN (Online Social Network). Questi legami possono essere individuati attraverso l'utilizzo di strumenti appartenenti alle aree tematiche dell'Intelligenza Artificiale, del Machine Learning e del Natural Language Processing (NLP).
Inoltre, all'interno del progetto di ricerca, si intende porre l'attenzione su tecniche che permettano la raccolta "proativa" di informazioni relative alle potenziali entità malevole. Questo risulta possibile attraverso l'implementazione dei paradigmi di *Active Deception*. In particolare, si intende realizzare una infrastruttura informatica vulnerabile fittizia, denominata *honeynet*. Tale architettura permetterà di raccogliere informazioni sugli attaccanti e sugli strumenti offensivi da essi utilizzati. La conoscenza acquisita può essere utilizzata per mitigare eventuali nuove azioni offensive ed eventualmente, attraverso operazioni di ricerca, scoprire reti sociali appositamente utilizzate da entità malevole. In aggiunta, tali strumenti possono essere utilizzati anche per distogliere l'attaccante dal perseguire i propri obiettivi malevoli all'interno di una organizzazione, guadagnando quindi tempo per predisporre e mettere in campo i meccanismi di difesa più opportuni.
Infine, le informazioni ottenute mediante le attività precedentemente descritte possono essere utilizzate per individuare appositi indicatori del tipo TTP (Tactics, Techniques and Procedures) capaci di identificare, in modo standard ed affidabile, comportamenti anomali in reti sociali, nonché di agevolare le operazioni di cosiddetta attribution in presenza di crimini informatici negli ecosistemi oggetto di studio.

c. Cronoprogramma

Il cronoprogramma dell'attività di ricerca può essere suddiviso anno per anno:

- Durante il primo anno lo studente di dottorato si porrà come fine l'acquisizione di tutte le competenze fondamentali per il raggiungimento degli obiettivi prefissati dal dottorato e descritti precedentemente in questo documento. Al termine del primo anno è prevista la stesura e relativa pubblicazione di un articolo scientifico, nonché la presentazione del lavoro svolto nell'ambito di un workshop o una conferenza di caratura internazionale.
- Durante il secondo anno di attività si prevede un maggiore consolidamento delle attività di ricerca rispetto all'anno precedente. Le competenze acquisite nel contesto di riferimento della ricerca durante i primi dodici mesi di studio consentiranno, infatti, di elaborare i primi contributi originali, caratterizzati da un livello di innovatività via via crescente. Tali contributi culmineranno, auspicabilmente, nella pubblicazione di un primo articolo scientifico su rivista di riconosciuta qualità nell'ambito del settore scientifico disciplinare di riferimento (ING-INF/05), nonché la partecipazione ad almeno due conferenze o workshop, anch'essi di livello internazionale. Inoltre, nella seconda metà del secondo anno di dottorato si prevede la conduzione, da parte dello

studente, di una esperienza di studio e ricerca all'estero, presso uno dei laboratori di ricerca di Accenture.

- Durante il terzo ed ultimo anno di dottorato si prevede la maturazione definitiva delle attività di ricerca del dottorando, con il raggiungimento di tutti gli obiettivi previsti dal progetto di ricerca, i cui risultati saranno consolidati in una visione integrata e coerente. Dal punto di vista della disseminazione, si prevede la partecipazione da parte dello studente ad almeno due conferenze di alto livello qualitativo in ambito internazionale, nonché, auspicabilmente, la pubblicazione di un ulteriore lavoro scientifico su rivista di riconosciuta qualità nell'ambito del settore scientifico disciplinare di riferimento. Nella prima metà dell'anno è prevista la presenza dello studente in uno dei laboratori di ricerca di Accenture sul territorio italiano.

d. Risultati attesi

Una infrastruttura informatica vulnerabile fittizia, denominata *honeynet*, che consentirà di raccogliere informazioni sugli attaccanti e sugli strumenti offensivi da essi utilizzati.

e. Impresa

Si prevede, come indicato nel cronoprogramma, per un periodo di 6 mesi, la presenza da parte dello studente di dottorato presso la società Accenture Italia. Scopo di questo periodo di permanenza in azienda riguarda l'approfondimento, in collaborazione con i ricercatori di Accenture, delle tecniche di Active Deception attualmente oggetto di sperimentazione anche in ambito aziendale, basate sull'impiego della virtualizzazione, nonché di paradigmi quali IaC (Infrastructure as Code) ed SDN (Software Defined Networking).

f. Istituzione ospitante all'estero

Si prevede, come indicato nel cronoprogramma, la presenza del dottorando presso una delle sedi estere della società Accenture, per un periodo di sei mesi. In tale contesto si intende studiare, sfruttando, tra le altre cose, l'esperienza maturata sul mercato da parte dei consulenti Accenture, l'applicazione delle moderne tecniche Machine Learning e di Natural Language Processing al dominio della sicurezza informatica.

g. Prodotti misurabili della ricerca, comunicazione e disseminazione

Il dottorando si prefiggerà l'obiettivo di divulgare i risultati della propria ricerca all'interno della comunità scientifica internazionale, mediante le seguenti pubblicazioni:

- N. 2 articoli su riviste di caratura internazionale e di riconosciuta qualità nell'ambito del settore scientifico disciplinare di riferimento (ING-INF/05);

- N. 4 articoli a conferenze e/o workshop di livello internazionale nell'ambito del settore scientifico disciplinare di riferimento (ING-INF/05).

Durante il periodo di dottorato è prevista la partecipazione da parte dello studente a conferenze e workshop, sia a livello nazionale che a livello internazionale, con il fine di presentare alla comunità scientifica i risultati del proprio lavoro di ricerca. Il dottorando si farà anche promotore della organizzazione di seminari su argomenti legati alle sue attività di ricerca, da erogare presso corsi selezionati di Laurea Magistrale della Federico II e/o presso laboratori di ricerca, in ambito sia accademico che industriale, in Italia ed all'estero.