UNIVERSITÀ DEGLI STUDI DI SALERNO

DIPARTIMENTO DI INFORMATICA

Corso di Laurea Magistrale in Informatica

Curriculum Sicurezza Informatica

ABSTRACT

Rilevazione di stream nei servizi di Instant Messaging con tecniche di Intelligenza Artificiale nell'ambito della Network Forensics

Relatori:	**Candidato:**
prof. Raffaele Pizzolante	*Egidio Giacoia*
prof. Gianni D'Angelo	*Matr.0522500488*

Anno Accademico 2019/2020

Al giorno d'oggi, con la diffusione degli Smartphone, milioni di persone utilizzano app di Instant Messaging (IM) per comunicare tra loro in tempo reale e condividere oggetti multimediali. Inoltre, questi servizi sono affiancati da una sicurezza in termini di codifica dati che impedisce la violazione delle conversazioni, in maniera tale da garantire la privacy agli utenti. Le misure di sicurezza adottate per i consumatori però, sfortunatamente, proteggono anche i criminali che ne fanno un uso improprio di queste piattaforme, soprattutto in casi di cyberstalking e/o cyberbullismo.

Un modo per individuare delle evidenze digitali è quello di osservare il traffico di rete prodotto dai servizi di Instant Messaging e i relativi client utilizzando gli strumenti della Network Forensics.

Osservando il traffico TCP/TLS non si riesce a dire con chiarezza e non ambiguità che quel flusso identifica, ad esempio, un invio di una foto piuttosto che un file audio o video, in quanto il contenuto dei singoli pacchetti sono cifrati. Per cui un modo per rilevare la tipologia di un flusso di pacchetti è quello di utilizzare tecniche di side channel analysis, ovvero, di estrarre delle caratteristiche temporali/spaziali sul flusso di pacchetti (ad esempio header, protocollo, numero di pacchetto ecc.), in maniera tale da poter classificare il traffico.

Questo lavoro, ovviamente, se svolto in maniera manuale richiede tempo e un notevole sforzo, per cui non risulta fattibile se si vuole analizzare un traffico di rete voluminoso. Per tale motivo è necessario affidarsi a quelle che sono le tecniche di Intelligenza Artificiale per automatizzare tale processo.

L'obbiettivo principale del lavoro di tesi è stato quello di sviluppare un tool denominato Instant Messaging Stream Detector Parser (IMSD Parser) per l'estrapolazione delle features da stream TCP di oggetti (immagini, video, audio e file) nei servizi di Instant Messaging.

Di seguito sono riportate le funzionalità del tool:

- Individuare la presenza di server di Instant Messaging;
- Individuare le connessioni tra client e server di IM;

- Individuare i flussi TCP tra client e server di IM;
- Estrapolazione delle feature da un singolo flusso di rete di una connessione di rete individuata;
- Estrapolazione delle feature di tutti i flussi di una connessione di rete individuata;
- Estrapolazione delle feature di tutti i flussi di tutte le connessioni di rete individuate;
- Salvare le features all'interno di un file CSV nuovo o aggiornare uno esistente;

È stato, inoltre, effettuato un esperimento per la generazione di un dataset di features utilizzando tale tool, il quale può essere utilizzato, ad esempio, come modello di addestramento per il machine learning. Tale esperimento si basa sull'analisi forense di alcune acquisizioni di rete di stream di oggetti tra due utenti WhatsApp.

Da tale analisi si evince che Il traffico dell'invio/ricezione di immagini, audio e file di dimensioni sul MB è rappresentato da un picco TCP, le cui caratteristiche sono quelle di essere breve e alto; mentre il traffico relativo all'invio/ricezione di video, file e audio di dimensioni sui 5MB in su è rappresentato da picchi TCP stretti, lunghi e consequenziali.

Gli esempi e i casi di studio analizzati hanno mostrato la validità del processo e delle linee guida da seguire per ulteriori sviluppi futuri, i quali sono elencati di seguito:

- Analisi di altri servizi di Instant Messaging;
- Utilizzare e sperimentare altre metodologie di acquisizione di rete;
- Analisi approfondita sulla correlazione dei dati/informazioni tra lato inviante e lato ricevente;
- Implementare una rete neurale per classificare gli stream di oggetti;