Digital Forensics - Project Report

Eugen Saraci
eugen.saraci@studenti.unipd.it

January 9, 2019

Chapter 1

Introduction

In the last years the expansion of SSL/TLS has made it harder for attackers to collect clear text information through packet sniffing or, more in general, through network traffic analysis. The main reason for this is that SSL/TLS provides a cryptographically secure payload encryption, which means that even though packets can still be easily captured, no useful information can be inferred from the payload content without having the encryption keys. It is worth mentioning that the endpoints of the communication (i.e. source and destination IP addresses) are transmitted in clear text for routing purposes; by performing a DNS lookup of the addresses and attacker could easily infer what site a user is visiting. valutare rimozione We can still try to hide these information by using a VPN (or a proxy server), but for many users this issue does not represent a relevant privacy problem, therefore no countermeasures are usually adopted in non privacy-critical environments.

The authors of [1] and [2] showed that by training a machine learning algorithm with encrypted traffic data, one could correctly classify the user actions performed on the most common Android applications such as Facebook, Gmail, or Twitter, which could easily lead through a correlation attack to the full deanonimization of fake, privacy preserving identities.

The aim of this work is to replicate and possibly improve some of the results achieved in the cited papers.

1.1

1.1.1 Inferring user actions

In this chapter we show that by using a combination of machine learning techniques we can correctly infer user actions through encrypted traffic analysis. It needs to be noticed that we totally ignore the payload contents (which are encrypted and therefore useless), while we focus more on the length and structure of the packets exchanged between the the endpoints.

1.1.2 Threat model

In our model, *Eve* the eavesdropper, has managed to intercept the traffic between *Alice*'s phone and her favourite social network called

Bibliography

[1] Mauro Conti, Luigi V. Mancini, Riccardo Spolaor, and Nino Vincenzo Verde. 2015. Can't You Hear Me Knocking: Identification of User Actions on Android Apps via Traffic Analysis. In Proceedings of the 5th ACM Conference on Data and Application Security and Privacy (CODASPY '15). ACM, New York, NY, USA, 297-304. DOI: https://doi.org/10.1145/2699026.2699119

[2] Conti, M., Mancini, L. V., Spolaor, R., & Verde, N. V. (2016). Analyzing android encrypted network traffic to identify user actions. IEEE Transactions on Information Forensics and Security, 11(1), 114-125.

Chapter 2

The Model

Chapter 3

Chapter 4

Evaluation

4.1 Experimental Setup

4.2 Experimental Results