

On the Fly Encoded Application Flows Recognition by Relying on Statistical Features of IP Traffic

Gianluca Maiolini¹, Andrea Baiocchi², Antonello Rizzi²,
Sara Ferri¹ and Letizia Gabbrielli¹

¹ AMTEC SpA, Loc. San Martino,
Piancastagnaio, SI, Italy,
{gianluca.maiolini, sara.ferri, letizia.gabbrielli}@elsagdatamat.com

² INFOCOM Dept., University of Roma “Sapienza”
Rome, Italy,
{andrea.baiocchi, antonello.rizzi}@uniroma1.it

Abstract. The secure collaborative judicial workspace (SCJW) has to allow the actors to use a number of communication and scheduling instruments for managing and storing any kind of documentation, video and audio recordings, evidence, among different Judicial offices of different countries. In this scenario is very important to identify encoded application delivering those application services to guarantee secure communication, but at the same time it is important to not compromise privacy of information exchanged. In this paper we aim at identifying application flows encoded within SSH tunnels by relying on statistical feature of IP packets. This will enable SCJW network administrator to identify un-trusted applications without analyze traffic contents.

Keywords: Traffic analysis, statistical traffic classification, SSH, cluster analysis, k-means.

1 Introduction

One of the most critical aspects every government should consider in the context of such a modernization is the field of justice. The most prominent issues is guaranteeing that any information flowing within judicial information systems is treated in a secure manner. In a cross border judicial cooperation during investigations, the information flows between different actors, different systems and at different levels. These information are very sensitive, they should be protected from unauthorized access and should be accessed only by specific people according to their role in the judicial process. Moreover document transfer from one country to another country must comply with the requirements of non repudiation. In a generic request of cross-border judicial cooperation one independent platform will support the country requesting judicial cooperation and other platform will support the country providing judicial cooperation. The secure collaborative judicial workspace (SCJW) has to allow the actors to use a number of communication and scheduling instruments for managing

