A Framework of User Identification from Network Traffic

Gaseb Alotibi, Nathan Clarke, Steven Furnell and Fudong Li

Centre for Security, Communications and Network Research, Plymouth University

Gaseb.alotibi@plymouth.ac.uk

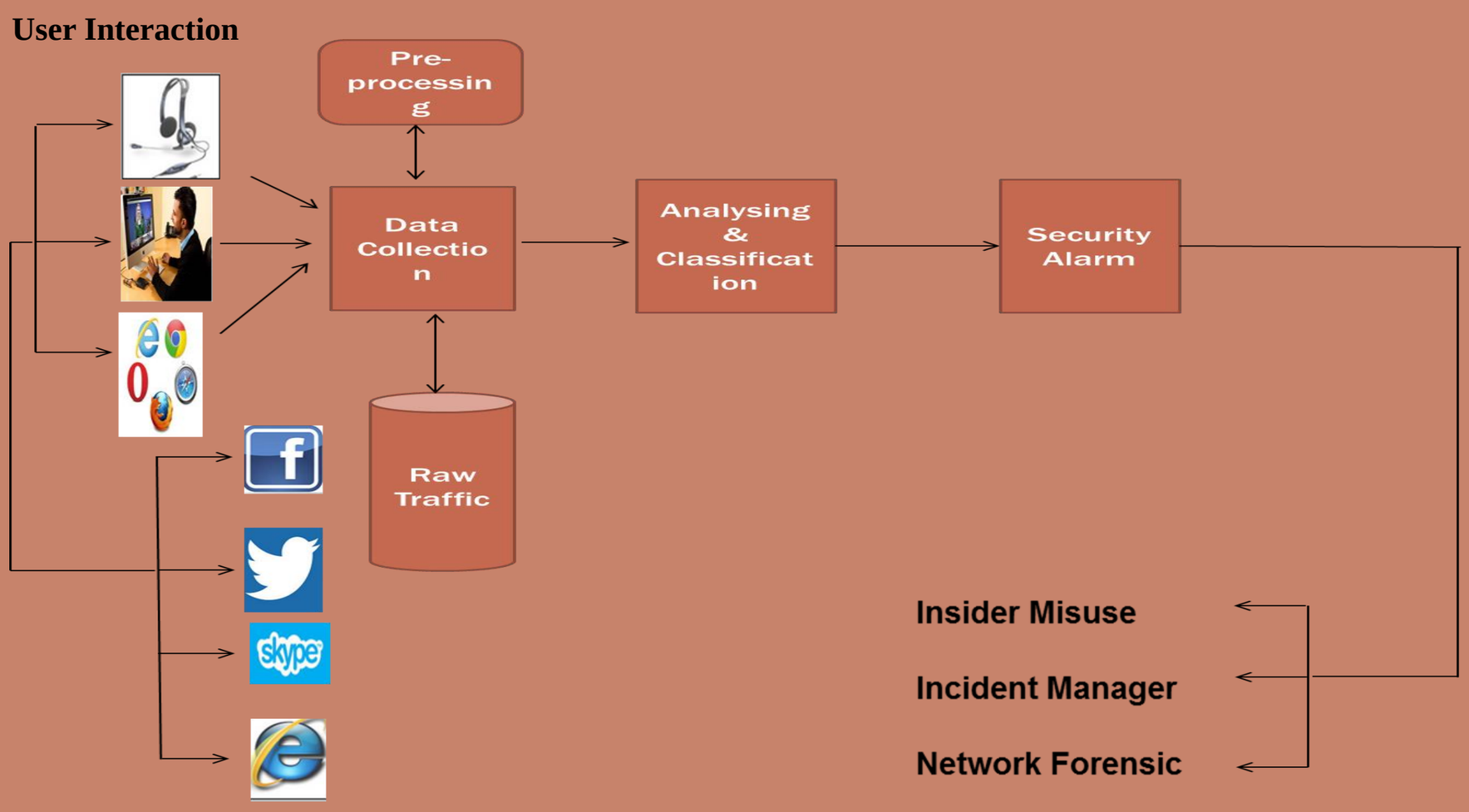
Introduction

People are the principal factor in the use of computer systems; however they are also considered a major threat. Misuse of computer systems, deception and information leakage are all notable examples [1, 2]. Indeed, a recent survey has highlighted insider misuse, leakage of sensitive information and unauthorised access to the system represent 78%, 49% and 66% respectively of all threats for large organisations [2].

Current Problems

In recent years, research has become more focused upon developing security tools to enable organisations to mitigate information misuse, for example, Security Information and Event Management (SIEM) and Data Loss Prevention (DLP) tools [3]. However, such approaches still suffer serious limitations, such as reliably identifying misuse [4]. Unfortunately, the fundamental limitation of these tools is that they provide information resolved to IP addresses rather than people. IP's are unreliable due to their dynamic allocation and thus the assumption that an IP belongs to one individual fails. This is merely exacerbated when you consider the range of devices a single user will use (e.g. mobile, laptop, desktop, phablet, tablet, watch).

User Identification from Network Traffic



Conclusion

This research project seeks to provide security tools and analysts with a resolution of the network traffic based upon people through applying biometric-derived design methodologies to network traffic. In comparison to previous studies, that have utilised the raw protocol data as a means of classifying usage, this project seeks to derived high-level user characteristics from meta-data at the network level and utilise these as a basis for identifying the user.

Future Work

As this proposed framework evolves, further research will be undertaken to recognising and extracting all user interactions features from metadata that could be useful in the identification of individual.