Cerberus
Towards Zero-Knowledge Advertising

Omnia Protocol

Josh Fourie, josh@omniaprotocol.com

December, 2018

Abstract

This paper explores the prospect of a basic advertising scheme nested within applications secured by Omnia Protocol through aligning zero-knowledge Succinct ARguments of Knowledge (zk-SNARKS), decentralised transaction networks and Secret Handshakes.

1 Background

The Omnia Protocol minimises the imperative for private-sector firms to extract and then secure individual data by substituting the trusted transfer of *data* between firms and individuals for the transfer of *verifiable computations* amongst untrusted parties. We achieve this through deploying basic computations locally to individual devices tasked with iterating over the data-sets accessible through smart-phones and then producing a zk-SNARKS proof affirming the correctness of a shareable and non-identifying output with only a negligible risk of failure (0.4%).

Currently, the value of data is famously extracted and realised in advertising schemes that construct a digital profile from data collected whilst users engage with a service provided, in most cases, as a free product simultaneously offering compensation for the data. A sufficiently sophisticated scheme might enable a client to prove they have viewed or engaged with an advertisement targeted at their group or demographic and thereby nullify the requirement for intermediate firms to handle and secure client data as well as expand the available data for improved advertising. The Omnia Protocol: Cerberus project intends to represent a simple step towards that goal.

The paper will consider a basic technical model wrappable within existing pilot proposals for *Employee* and *Student* Wellness that establishes and then develops the core engine as well as outlines future work and challenges for the Cerberus project. It assumes a general familiarity with zk-SNARKS and decentralised networks.

Requirements. Cerberus should achieve the following amongst the Client ($\mathcal{P}$), the Advertiser ($\mathcal{V}$), and an Adversary ($\mathcal{A}$):

- $\mathcal{P}$ cannot falsely substantiate a claim to to maliciously view an advertisement.
- $\mathcal{P}$ can guarantee remuneration for every advertisement served from $\mathcal{V}$.
- $\mathcal{A}$ cannot identify individual data-inputs or leverage any other attack vectors to harm or otherwise exploit either $\mathcal{P}$ or $\mathcal{V}$.