Analysis, Design and Simulation of Fraud and Vulnerability Management in Affiliate Marketing

by

Bede Amarasekara

A thesis
submitted to the Massey University of Auckland
In fulfilment of the
requirements for the degree of
Master of Philosophy.

Massey University of Auckland, New Zealand
2016

Abstract

Affiliate Marketing (AM) is a popular marketing model in e-commerce, which provides businesses a greater reach for a lesser cost. It is considered a safe way to spend the on-line marketing budget, as commissions are paid to affiliates only on monetary outcomes. However, there are inherent risks and frauds associated with the browser-cookie based tracking process. Cookie stuffing, load-time clicking, typo-squatting, conversion hijacking are some of the fraudulent methods used by rogue affiliates to earn commissions for sales transactions that were never actually promoted by them. Some of the previous researches discuss the prevalence of the above frauds, but technical aspects of these frauds, as to how they are implemented and what are the different ways to implement the same fraud are useful questions when developing solutions, which are addressed in this thesis. Contradicting results in quantifying the prevalence of fraud, carried out in previous research work has prompted us to use empirical data to ascertain how widespread these threats are in affiliate marketing. An affiliate marketing dataset of a practitioner spanning over a period of more than four years were analysed. Some of the above fraud scenarios were discovered and the prevalence of fraud scenarios verified. This thesis also presents new vulnerabilities that were discovered using AMNSTE (Affiliate Marketing Network Simulation and Testing Environment). AMNSTE implements same HTTP cookie tracking technology that is implemented in real-world Affiliate Marketing Networks. This simulation and testing environment enables researchers and affiliate marketing practitioners to examine frauds and risk scenarios and to test the efficacy and utility of solutions that are developed to mitigate those vulnerabilities. The thesis finally proposes technical solutions that can be implemented by advertisers and by affiliate networks, as we continue on our ongoing quest to make systems secure from online frauds.

Dedication

To my parents, in appreciation of their love, commitment and dedication, for never giving up the hope that this token of academic achievement, though long overdue, would one day be true.

Publications produced

1. Bede Ravindra Amarasekara & Anuradha Mathrani (2015). "Exploring Risk and Fraud Scenarios in Affiliate Marketing Technologies from the Advertiser's perspective", Australasian Conference in Information Systems (ACIS 2015). Adelaide, Australia, Dec 2-4, 2015.

2. Bede Amarasekara & Anuradha Mathrani (2016). "Controlling Risks and Fraud in Affiliate Marketing: A simulation and testing environment", Research paper accepted for IEEE 14th International Conference on Privacy, Security and Trust, Auckland, New Zealand, Dec 12-14, 2016.

3. Bede Amarasekara & Anuradha Mathrani (2017 - in-press). "Revenue Fraud in E-Commerce Platforms: Challenges and Solutions for Affiliate Marketing", Cyber Security and Policy, Auckland, New Zealand: Massey University Press.

Acknowledgements

I would like to thank my research supervisor Dr. Anuradha Mathrani, for her guidance, support and mentoring throughout my research degree and for inspiring me to reach higher goals.

I thank Associate Professor Chris Scogings for having faith in me and guiding me towards my success.

I also wish to thank my sincere friend Owen Ormsby, for providing me help and support, throughout my study.

Finally, I wish to thank all my family, for being there for me and supporting through all my endeavours.

Table of Contents

List of Figures