Protecting User Data in Large-Scale Web Services

by

Frank Yi-Fei Wang

B.S., Stanford University (2012)
S.M., Massachusetts Institute of Technology (2016)

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

September 2018

Author . . . . . .
Department of Electrical Engineering and Computer Science
June 25, 2018

Certified by . . . . . .
Nickolai Zeldovich
Professor
Thesis Supervisor

Certified by . . . . . .
James Mickens
Associate Professor
Thesis Supervisor

Accepted by . . . . . .
Leslie A. Kolodziejski
Professor of Electrical Engineering and Computer Science
Chair, Department Committee on Graduate Students

Protecting User Data in Large-Scale Web Services

by

Frank Yi-Fei Wang

Submitted to the Department of Electrical Engineering and Computer Science
on June 25, 2018, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

Abstract

Web services like Google, Facebook, and Dropbox are now an essential part of people's lives. Users willingly provide their data to these services because these services deliver substantial value in return through their centralization and analysis of data, such product recommendations and ability to easily share information. To provide this value, these services collect, store, and analyze large amounts of their users' sensitive data. However, once the user provides her information to the web service, she loses control over how the application manipulates that data. For example, a user cannot control where the application forwards her data. Even if the service wanted to allow users to define access controls, it is unclear how these access controls should be expressed and enforced. Not only is it difficult to develop these secure access control mechanisms, but it is also difficult to ensure these mechanisms are practical. To address some of these concerns, I have built three systems, Splinter, Riverbed, and Veil, in this thesis.

Thesis Supervisor: Nickolai Zeldovich
Title: Professor

Thesis Supervisor: James Mickens
Title: Associate Professor

Acknowledgments

Contents

List of Figures