

RESEARCH IN SECURE RANDOM VALUE GENERATION

SHAPE SECURITY, SILICON VALLEY 2016

A Major Qualifying Project Report
Submitted to the faculty of
WORCESTER POLYTECHNIC INSTITUTE

by

Miguel Mora

Hoang Ngo

Etienne-Alexandre Scraire

March 4, 2016

Approved: _____

Professor David Finkel, Project Advisor

This report represents the work of WPI undergraduate students submitted to the faculty as evidence of completion of a degree requirement. WPI routinely publishes these reports on its website without editorial or peer review. For more information about the projects program at WPI, please see <http://www.wpi.edu/academics/ugradstudies/project-learning.html>

Abstract

Shape Security stops automated web and mobile application attacks using a combination of obfuscation and transformation using a stateless appliance. This MQP involved security research in random value generation and the development of a prototype to increase the reliability, performance and security of one of Shape Security's Product.