Digital Credit and Data Security

How Secure is Data Used in Digital credit?
Best Practices Guide

Patrick Traynor – CFI Fellow
University of Florida
January 2018
Best Practices Guide

Introduction

The recent release of our security analysis of online credit providers uncovered multiple weaknesses. Our goal is to strengthen the security of these applications, ensuring both strong protections for consumers and their data and the continued growth and success of this emerging industry. Every company in the industry should conduct a thorough discussion and evaluation of their security goals and mechanisms.

This short document provides tips to address the most commonly observed problems found in our analysis. Readers should note that these recommendations are a first step. Instead, they must be viewed as “Step Zero” in protecting their customers’ data and reducing their own liability. Additional mechanisms are possible (e.g., two-factor authentication, intrusion detection systems), but none should claim that the mechanisms we discuss are expensive or burdensome – they are simply the base level of security expected of all responsible online entities.

We expect management to be able to use this document as a checklist to better understand their own security standing.

Privacy Policies

- Privacy policies must be written (at least) in the language of the population using the service.

- Privacy policies must target the expected reading grade level of the population using the service.

- Privacy policies must cover (at least) the principles proposed by the GSMA for mobile applications.

- Privacy policies must explicitly mention all data types (e.g., geolocation) the application requests from users.

Mobile Application Security

- Mobile applications must use strong cryptographic algorithms to protect user data in transit. Developers can seek additional guidance through organizations including NIST. Current recommendations include the Advanced Encryption Standard (AES) in either CBC or CTR modes (with keys of *at leas*t 128-bits in length) and the SHA-256 algorithm.
    - Mobile applications developers should immediately cease using deprecated (i.e., insecure) algorithms, including but not limited to DES, 3DES and RC4.

- Mobile applications must not use static/hardcoded salt values.

- Mobile applications should use the most up-to-date version of TLS (TLS 1.2 at the time of writing). Developers that do not do so must be able to describe specific security property that they cannot achieve via TLS.

- Mobile applications for online credit should not include unvetted third-party analytics and/or advertising libraries. Such code may introduce exploitable vulnerabilities.

- All communications must be cryptographically protected.

Authentication

- TLS must be properly configured to check digital certificates on mobile devices. Android programs do this by default, but some developers attempt to override this functionality. TLS Certificate checking must not be overridden unless stronger mechanisms are put in place (e.g., integration of certificate pinning, use of certificate transparency projects, etc).

- TLS must properly verify host names.

Server Configuration

- All servers should run the most currently available version of TLS (TLS 1.2 at the time of writing). If engineers insist on running previous, vulnerable versions, management should be provided with a report detailing the size of the customer base requiring the use of older versions and a plan to assist that population in migrating to safer standards.

- All servers must use strong cryptographic algorithms to protect user data in transit. Developers can seek additional guidance through organizations including NIST. Current recommendations include the Advanced Encryption Standard (AES) in either CBC or CTR modes (with keys of *at leas*t 128-bits in length) and the SHA-256 algorithm.
    - Systems administrators should immediately cease using deprecated (i.e., insecure) algorithms, including but not limited to DES, 3DES and RC4.

- Systems administrators must patch their systems regularly, especially with regards to updates to TLS.

- Systems administrators should regularly run the Qualys "SSL Test"[1] on all their public-facing servers. The resulting report should be presented to management regularly (e.g., monthly).

Mobile Application Permissions

- Mobile Applications should limit the types of data requested and collected from their users to those necessary to perform their mission. This is known as the Principle of "Least Privilege", and not only helps to respect consumer privacy but also to minimize corporate liability in the case of a breach.

- Every permission requested by the application should be explicitly included in the Privacy Policy.

[1] https://www.ssllabs.com/ssltest/