MobileTrust™ Whitepaper

StrikeForce Technologies, Inc.
1090 King Georges Post Road #603
Edison, NJ 08837, USA
http://www.sftnj.com
Tel: 732 661-9641
Fax: 732 661-9647

Table of Contents

Executive Summary

Today mobile devices are starting to augment/replace the corporate desktop especially in the light of Bring Your Own Device (BYOD). In this new role, the mobile device becomes the focus of attackers for stealing corporate usernames and passwords leading to data breaches, which leads to large dollar losses and unwanted headlines. Hence, protecting these credentials in a mobile framework becomes critical. MobileTrust™ is the only application for iPhone/iPad and all Android devices that contains essential security "must-haves" for protecting your credentials and your identity.

The purpose of this paper is to introduce the MobileTrust solution developed by StrikeForce Technologies, Inc.

Mobile security threats

The top security issues can be grouped around –

- *Device loss* – Loss of a mobile device, whether accidental or due to theft is one of the top concerns. Fortunately, mobile device vendors have included capabilities to locate the device and wipe the data remotely.

- *Application privacy* – Rogue applications can trick a user into granting them privileges that enable them to access various data sources on the device. These can include device identification data, call and message history, contents of the address book, geo-location data and browsing history. In addition, mobile OS's including iOS, log keystrokes to help in auto-completion.

- *Malware* – Malware can be disguised as a rogue application and steal confidential data using attack modules such as a keylogger.

The defenses against these threats are limited due to the restrictions imposed by the mobile OS. Thus it is hard to detect malware and defend against it.

The MobileTrust™ Solution

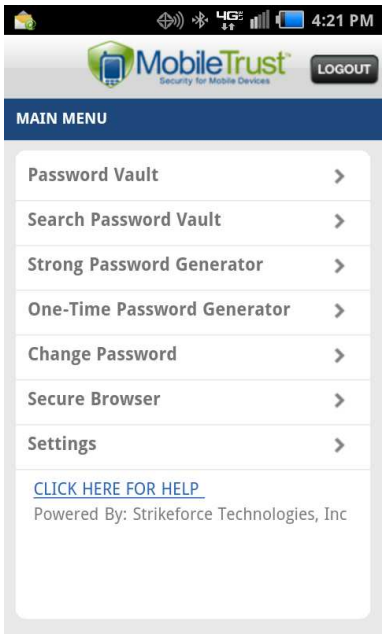
The StrikeForce solution focuses on securing the user credentials rather than trying to detect the malware. The application is available for iPhones/iPads and all Android devices (smart phones and pads). The application is secured by a password, which is protected by a secure keyboard.

The solution components include –

- **Password Vault** – Securely stores an unlimited number of passwords with associated websites.

- **Strong Password Generator** - This useful feature creates strong passwords based on user-defined preferences, and then stores the strong passwords in the password vault for future usage.
- **ProtectID® Soft Token -** One-Time-Password (OTP) Generator for the industry leading ProtectID authentication platform. Features “one touch” user enrollment.
- **Support for other OATH compliant Soft Tokens –** Works with other OATH compliant authentication systems.
- **Encrypted Database** – Store notes and other data in user defined fields in an encrypted database.
- **Secure Keypad** – Custom keypad that provides secure input by encrypting keystrokes and preventing the mobile OS from logging the keystrokes.
- **Secure Browser** – Custom secure browser.

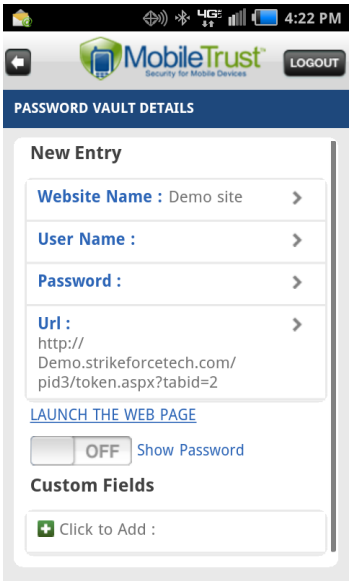
The following screenshot depicts the main menu –



Password Vault

The Password Vault enables the secure storage of user credentials required to access websites or corporate networks. The credentials are stored in encrypted form. The user can also launch the website into a Secure Browser protected by a Secure Keyboard.

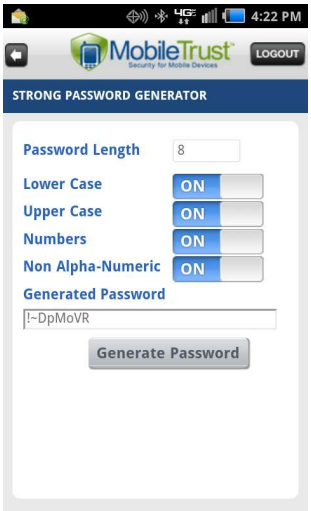
The following screenshot depicts an entry in the Password Vault –



Strong Password Generator

The Strong Password Generator enables the generation of very hard to guess strong passwords, which can be pasted into the Password Vault.

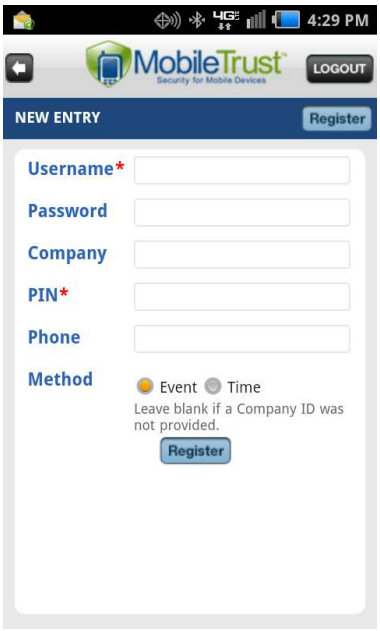
The following screenshot depicts the Strong Password Generator –

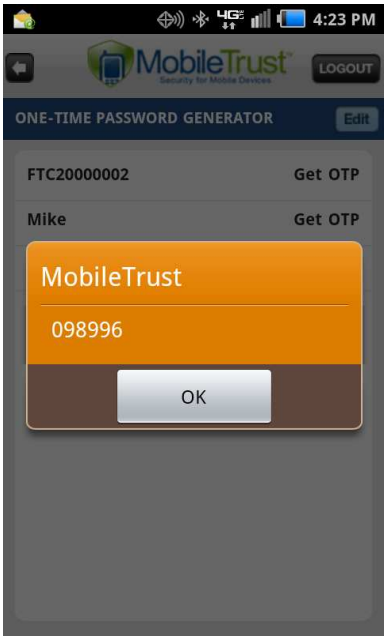


ProtectID® Soft Token

One-Time-Password Generator for the industry leading ProtectID authentication platform. Features “one touch” user enrollment.

The following screenshot depicts PID token provisioning and OTP generation –

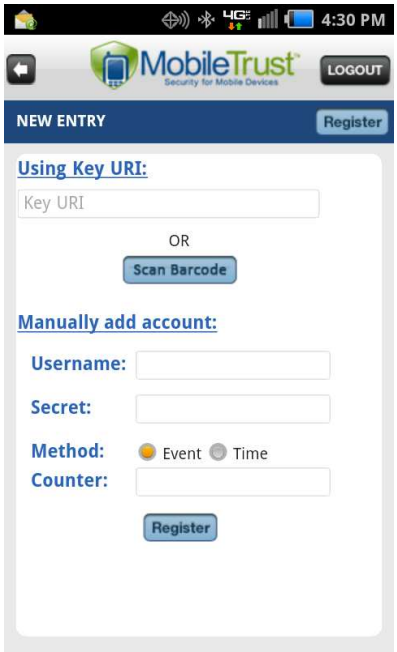




Third Party Soft Token Support

One-Time-Password Generator for the third party OATH compliant soft tokens, such as the Google Authenticator. The provisioning is either manual or via a QR code.

The following screenshot depicts token provisioning –



Encrypted Database

Enables the storing of notes and other data in user defined fields in an encrypted database. This is accessible via the Password Vault which allows the user to create their own data fields.

Secure Keypad

Mobile OS's such as iOS, log keystrokes to help in auto-completion. These keystrokes are stored in databases that can be accessed by rogue applications. In addition, malware may be able to capture the keystrokes entered on the default soft keyboard.

The Secure Keypad is a custom keypad that provides secure input by encrypting keystrokes and preventing the mobile OS from logging the keystrokes.

Secure Browser

The Secure Browser is a custom secure locked-down browser that provides secure input by encrypting keystrokes. Secure input is indicated by coloring the background of the input box green.

The following screenshot depicts the Secure Browser with the Secure Keypad –

Conclusion

Mobile devices have become the focus of attackers for stealing corporate usernames and passwords leading to data breaches. Hence protecting these credentials, in a mobile framework, becomes critical. MobileTrust™ is the only application for iPhone/iPad and all Android devices that contains the essential security "must-haves" for protecting your credentials and your identity.