Improving Online Security with Strong, Personalized User Authentication

July 2014

"Secure and simplify your digital life."™

Table of Contents

Online Security -- Safe or Easy, But Not Both?

The December 2012 issue of Wired magazine featured the cover story *Kill the Password: Why a String of Characters Can't Protect Us Anymore*. The author of the article, Matt Honan, had his digital life hijacked: "This summer, hackers destroyed my entire digital life in the span of an hour. My Apple, Twitter, and Gmail passwords were all robust—seven, 10, and 19 characters, respectively, all alphanumeric, some with symbols thrown in as well—but the three accounts were linked, so once the hackers had conned their way into one, they had them all."[1] The article's punch line states the opportunity very clearly: "The age of the password has come to an end; we just haven't realized it yet. And no one has figured out what will take its place."[2]

The world is going online, and fraud and identity theft are on the rise. Worldwide unit sales are expected to reach 500M for smartphones[3] and 120M for tablets in 2012, with a projected year-over-year growth rate of over 50% for both[4]. More importantly, easy access to computing devices of all types is driving the explosion of online "apps" for every function you can imagine (and many not even envisioned yet) including online banking, payment services (e-wallet), loan applications, real-time health monitoring, electronic ticketing, electronic identity cards and so on. The problem is that most current online systems are still largely dependent on legacy user authentication via username and password, which can result in identity theft, fraud, financial risk, and increased "friction" for the end user.

Strong user authentication is an important component in any solution seeking to address these issues. The most common form is "two-factor" authentication (2FA), which requires two or more of the following factors to be presented when a user logs in to a protect site: 1) a knowledge factor ("something you know"); 2) a possession factor ("something you have"); and 3) a biometric factor ("something your are"). Typical 2FA solutions have consisted of hardware tokens, key fobs, smartcard tokens, one-time passwords (OTP), biometric readers (fingerprint readers), etc. These solutions have been widely deployed mostly in larger companies to protect enterprise applications.

However, two-factor authentication solutions, while significantly improving security have not been widely adopted outside of large enterprises due to inconvenience, complexity and high cost. When it comes to online security the traditional wisdom has been "you can make it safe, or you can make it easy to use, but you can't do both."

---

1 Wired: http://www.wired.com/gadgetlab/2012/11/ff-mat-honan-password-hacker/all
2 Ibid
3 Strategy Analytics: http://www.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5170
4 Gartner: http://www.gartner.com/it/page.jsp?id=1980115

The Traitware Solution

Traitware is a next generation, patent-pending two-factor authentication platform, which is both secure and easy to use, and can be deployed at a low cost in both consumer and enterprise applications.[5] Traitware takes advantage of the proliferation of smartphones by creating a robust and innovative "smartphone-as-a-token" method of strong, two-factor user authentication. Compared to other solutions, Traitware is unique in several ways that it approaches the knowledge factors used to authenticate the user, as will be described below.

The Traitware solutions consists of three major components which work together seamlessly to add strong, personalized user authentication to almost any online system or application:

- **Traitware PhotoAuth**: PhotoAuth is a new, innovate security method, which requires the user to select a sequence of images on their smartphone to "unlock" the Traitware App. PhotoAuth is both more secure and easier to use than traditional numeric PIN codes and forms the second "factor" in the Traitware strong authentication solution – the "something you know" factor. The PhotoAuth feature is seamlessly integrated into the Traitware App and Traitware Service.

- **Traitware App**: The Traitware App installs on the user's Apple or Android smartphone allowing it to function as a "personalized" security token, which is "bound" to the user's validated identity. The Traitware App, together with the user's smartphone, functions as the first "factor" in the Traitware strong authentication solution – the "something you have" factor. The Traitware App can function as a standalone App or the Traitware authentication functionality can be integrated into a customer's existing mobile app.

- **Traitware Service**: This is the back-end component of Traitware, which handles the authentication process and the interface with the web application or other service being protected by Traitware strong authentication. The Traitware service can be hosted in a secure private cloud or can be integrated into the customer's web application. The Traitware Service uses a simple set of RESTful APIs to allow easy integration into the customer's web application or web-based service.

The following sections provide more details about how the Traitware strong authentication solution works, and also describes other optional features including the "QR-Login" and "Click-to-Login" features.

[5] Several Patents on Traitware technologies including the device-user signature and PhotoAuth are pending.

Traitware PhotoAuth

A patent-pending Traitware feature called PhotoAuth provides Traitware with the "something you know" authentication factor. The "PhotoAuth Key" consists of a sequence of user-selected images, which form a "visual key" which must be selected by the user on their Smartphone to "unlock" the Traitware protected App when it launches. If the user fails to select the correct image sequence (which is pre-selected by the user during the Registration process), the Traitware protected App is not unlocked and the smartphone cannot be used to authenticate the user. PhotoAuth is both safer and easier to use than traditional PIN codes often used for this purpose.

The user selects their personal PhotoAuth Key sequence during the device registration process. The PhotoAuth Key can be configured as either 4, 5 or 6 images, which the user selects from a "set" of 24, 48 or 72 images. The Key Length and Set Size can be configured on a per-user or per-application basis according to the level of security required. The total pool of available PhotoAuth images number in the thousands, but the user only sees a fixed set of 24, 48 or 72 images.

As the following statistical table illustrates, even at the lowest-strength setting of 4 images out of a set of 24 possible images, this provides 33 times more entropy than a 4-digit numeric PIN code. At the maximum security setting, PhotoAuth provides 139,000 times more entropy than an equivalent numeric PIN. This setting can be easily configured to the level of security appropriate to the application being protected, and can even be changed on a per-user basis.

PhotoAuth Key Length	PhotoAuth Set Size	PhotoAuth Key Entropy as 1-chance-in-XXXX	Entropy compared to equivalent Numeric PIN
4	24	331,776	33 times the entropy of a 4-digit PIN
4	48	5,308,416	530 "
4	72	26,873,856	2,687 "
5	24	7,962,624	80 times the entropy of a 5-digit PIN
5	48	254,803,968	2,548 "
5	72	1,934,917,632	19,349 "
6	24	191,102,976	191 times the entropy of a 6-digit PIN
6	48	12,230,590,464	12,231 "
6	72	139,314,069,504	139,314 "

Table 1: PhotoAuth Key Entropy Statistics Compared to a Numeric PIN

The following sample image from the Traitware App shows the PhotoAuth "unlock" screen. This screen is presented to the User when they launch the Traitware App:

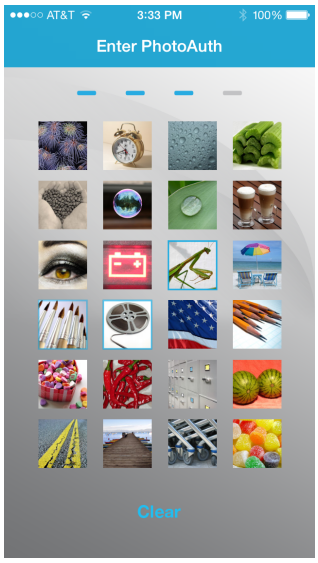

Figure 2: Sample PhotoAuth Unlock Screen

Because PhotoAuth uses easily remembered images instead of numeric or alphanumeric codes, it is more convenient for the user and safer due to the larger entropy of the PhotoAuth Key.

The Traitware App / Traitware ID

Human beings have highly developed recognition skills, which allow them to recognize certain physical and behavioral attributes of other individuals and instantly distinguish one person from another. Further, we subconsciously store characteristics of those individuals in our memory in order to recognize them again based on those attributes. As we get to know them we can connect names, voice traits, visual keys and other individual traits to those individuals and learn to recognize them almost instantly. Additionally, there are other "traits" that do not depend on physical, or behavioral characteristics. For example, artists, writers and musicians can often be identified by the tone, character, or structure of the works they create because of the uniqueness of their interaction with the media in which they work.

In our digital age, this same "interactive" effect comes into play in how we use our smartphones and other digital devices. It turns out each person ends up creating a dynamic "digital fingerprint" which is a highly differentiated, personalized, digital representation of their actual identity.

The Traitware App takes advantage of this fact by using the "digital fingerprint" contained on the user's smartphone as one of the factors in our two-factor authentication process. The App uses this digital fingerprint consisting of various user and device traits to create a "Traitware ID" which uniquely identifies the user-device combination to a very high degree of certainty.

Figure 3 contains a list of some of the traits derived from the smartphone device by the Traitware App and which make up the Traitware ID token.

Device Traits	User Traits
MAC address	Address Book Contact names
Device Type (Apple iPhone or Android)	Address Book Contact phone numbers
Screen Resolution	Song Titles
Device Name	Other user traits as available
Mobile Country Code (mcc)	
Mobile Network Code (mnc)	
Other hardware traits as available	

Table 3: Traitware Device and User Traits

These device-user uniquely identify the smartphone as belonging to the user, are used to generate the Traitware ID electronic signature, which represents the unique user-device pairing. Please note that for security and privacy reasons, personal data is never transmitted off of the device. Only a salted, hashed and truncated representation of this data is transmitted to the Traitware Service for future authentication purposes.

The uniqueness of this digital signature allows Traitware to determine if a given signature came from a specific device-user pair at the time the user is authenticated by the system. Statistics show that these trait signatures can be used to uniquely identity each device-user pair to an accuracy exceeding 99.999999999%, or 1 in 390 billion, a number much larger than the current human population.

User-Device Registration

Using Traitware starts with the user installing the Traitware App on their Apple or Android smartphone device. The App can be installed from a public store (App Store or Google Play) or from a private distribution source. A link to install the App can also be sent to the user via an SMS or email message.

Note: The Traitware App functionality can also be integrated into a customer's mobile app to add strong authentication to an existing app.

After installing and starting the App on their smartphone, the user is prompted to enter a one-time-use "Registration Code" which is required to register the user-device pairing. This code can be supplied to the user in a number of ways by the issuing company such as sending it to a validated mobile phone number via SMS or via a validated email address. The Traitware registration process, including the use of the customer's corporate LDAP or AD-based directory service or a public IA provider such as Experian, can also support other forms of Identity Assurance (IA).

Next, the user is prompted to select their personalized sequence of 4, 5 or 6 images, which make up their PhotoAuth Key which is used to later on to "unlock" the Traitware App. The PhotoAuth Key functions as the "something you know" factor in the Traitware two-factor authentication

process. Please note that the actual PhotoAuth Key sequence is never transmitted off of the device. A hash for the PhotoAuth Key is transmitted instead and stored by the Traitware Service. Because of the high entropy of the PhotoAuth Key, even if the hash was stolen, it would be virtually impossible to reverse it and produce the original PhotoAuth Key using a dictionary-lookup or other cracking method.

The App now registers the user-device pairing with the Traitware Service. The App "fingerprints" the user's device to collect the user and device traits as explained above. These traits are never transmitted off of the device but instead function as inputs to a hashing algorithm, which produces the "Traitware ID" which uniquely identifies the user-device combination as one of the two authentication factors.

Once the user-device pairing has been registered with the Traitware Service, the user can now employ their smartphone with the Traitware App installed as a secure login token as described in the next section.

Using Traitware to Login

Once the user-device has been registered, the user can securely access a Traitware-protected web application using their smartphone as a login token as described below. There are several ways in which this can be accomplished depending on how Traitware is integrated into the customer's application and how the device is used.

QR-Login

The most interesting and useful of the login methods supported by Traitware is called "QR-Login" which works as follows:

- From a web browser on any Internet-connected terminal device (PC, Mac, tablet, set-top box or other) the user navigates to the login page for the web application protected by Traitware. The site displays a QR code, which uniquely identifies the web session/instance. (the QR code is generated by the Traitware Service)
- The user launches the Traitware App on their smartphone and enters their PhotoAuth key to unlock the App. The App transmits the Traitware ID token to the Traitware Service, which authenticates or denies access for the user.
- Using the Traitware App, the user scans the QR code displayed on the web terminal. The App transmits the QR code to the Traitware Service. Scanning and transmitting the QR code associates the web application with the authenticated device-user pair.
- The user is now automatically and securely logged into the Traitware-protected site without a username or password being entered. The user can now use the web application or service, conduction transactions, etc.

Single-Device Login

If the user wants to login to a secured web application directly from their smartphone's browser instead of from a separate device, the "Single-Device Login" method applies:

- The user navigates to the web application login page from the browser on their smartphone and clicks on a Traitware Login button or link. The link on the web page invokes a web method, which launches the Traitware App on the smartphone.
- The Traitware App prompts the user to enter their PhotoAuth Key then transmits the Traitware ID to the Traitware Service, which then authenticates the user.
- The Traitware Service notifies the web application that the user is authenticated and the application logs the user into the web application. The user can now use the web application or service, conduct transactions, etc. from their smartphone.

Push-to-Login

Another method supported by Traitware is called "Push-to-Login" and can be used when it's not practical or desirable to scan a QR code from a web page:

- From a web browser on any Internet-connected terminal device (PC, Mac, tablet, set-top box or other) the user navigates to the login page for the web application protected by Traitware. The user enters a login name or email address in the terminal, which uniquely identifies the User (no password), then clicks on the Submit or Login button on the web application page.
- On the back end, the web application notifies the Traitware Service via an API call that the specified user is attempting to login. The Traitware Service then sends a "push notification" to the user's smartphone to verify the login request.
- The user accepts the login verification by pressing the Push to Login button on the push notification screen. This launches the Traitware App, which prompts the user to enter their PhotoAuth key to unlock the App.
- The App transmits the Traitware ID token to the Traitware Service, which authenticates the user and logs them into the web application by returning a "login approved" message to the calling web application. The user can now use the web application or service, conduction transactions, etc.

The Traitware Service

The Traitware Service is the back-end software component, which handles the authentication process and the interface with the web application being protected by Traitware strong

authentication. The Traitware Service software can be hosted in a secure private cloud or can be integrated into the customer's web application.

The Traitware Service exposes a simple set of RESTful APIs to allow easy integration with the customer's web application or web-based service.

The Traitware Service uses several techniques to provide a secure and reliable authentication process designed to prevent common threats:

- Cryptographic signing of all data sent between the Traitware App and the Traitware Service using asymmetric key cryptography (public/private key pair) to verify the authenticity of each message and prevent man-in-middle types of attacks.
- Cryptographic signing of the Traitware App itself prevents it from being spoofed at a functional level.
- The PhotoAuth Key and Traitware ID codes are transmitted and stored only as complex salted hashes so that no private user information is ever transmitted off of the smartphone or stored by the Traitware Service.

The Traitware solution also includes a back-end component called the Traitware Administration Console (TAC) which is a secure web portal used by a system administrator to configure and monitor the Traitware Service.

Summary

Identity fraud, cyber theft and other threats create tremendous liabilities for companies providing services on the Internet and erode consumer confidence in online services. Despite the increased digital power at our disposal, online security is still grossly inadequate because most systems are still heavily dependent on the antiquated username/password paradigm. This must change in order to avoid a continual degradation of this situation.

While not a "silver bullet" for this problem, strong, multifactor user authentication has been proven to be a significant part of the solution as it plugs a major hole in the wall. The problem with traditional multifactor authentication solutions is that they have been designed for use by large enterprise customers, which tend to be complex and cumbersome for the end user.

Leveraging the widespread deployment of smartphones which can be used as personal authentication devices, the Traitware solution provides a safe and simple to use strong authentication system which can be easily integrated into almost any customer application or system.