



vidloop secure™

White Paper

Proving Identity

How do we prove our identity online? Typically a user and an authenticator agree upon two pieces of information: a unique identifier for the user, and a shared secret, a piece of information that only those two parties know. Conventionally, this is a username and password: the unique identifier and the shared secret are explicitly stated by the user for the authenticator, and if they match, identity is proven.

This is certainly an intuitive and effective implementation, but it is loose-lipped. When we state our shared secret aloud, we invite the world to listen in and to become us. What is needed is a means of proving identity without compromising identity.

Vidloop rejects the notion that you must state your secret aloud in order to prove that you know it.

How Vidloop Works

Vidloop Secure™ is a software-only, multi-factor user login technology based on categorized images. When a user enrolls, he chooses a specific or variable of image categories from a bank of possible image content (such as airplanes, cars, or keys). This constitutes the shared secret. Then, upon proof of receipt of an access code transmitted out-of-band by e-mail or phone, the user's computer is activated with a software token. At the time of login, if the token is found, the Vidloop Dynamic Image Grid, which includes pictures belonging to the user's chosen categories, is displayed. The user selects these images by typing the randomized letter associated with his images, forming his one-time access code.

Furthermore, the Vidloop Secure™ system can deactivate a computer if it fails enough times on the grid. The number of allowed consecutive failures is configurable on a per-implementation basis.

Cognitive Decryption

Because Vidloop Secure™ requires human-level cognition to associate images with category names, a computer cannot use the grid to login. This element of cognitive decryption exempts Vidloop Secure™ from the host of automation-related problems that plague systems protected by standard passwords.

Not only does this allow systems protected by Vidloop Secure™ to be safe from irritating bots and automatic logins, but it also creates an additional barrier against hacking, because automated tools can no longer be used to discover the shared secret or even log in at all.

Resistance to Attack

Vidloop Secure™ is resistant to prevalent forms of hacking, providing increased effectiveness over passwords when subjected to brute force, keystroke logging, phishing, and man-in-the-middle attacks.

Brute Force

Ordinary passwords are susceptible to repeated guessing, which can be augmented with look-ups to find common passwords. Because Vidloop requires device activation to even see the grid, a remote attacker will not be able to start to guess possible access codes unless he first activates his computer.

A brute force attack against the device activation step is difficult but still a remote possibility; however, a brute force attack against the Vidloop Secure™ system as a whole is unrealistic. The attacker would have to send off a request for an activation code, then guess that random 6-digit activation code, then guess perhaps 3 times on

the grid before being deactivated, and start over again. Meanwhile, the system would be repeatedly notifying the legitimate user that an activation attempt is in progress, giving the user an out-of-band notification that is unrivaled in conventional login security.

Keystroke Logging

If a Vidoop user's system is compromised by keystroke logging software, his shared secret is still safe. Because the user never explicitly states that secret, all that the keystroke logger receives is the random access code, which will not be valid next time, since the images and associated characters have both randomly rearranged.

Even if the keystroke logging software includes screen capture, there are two significant barriers to the attacker's compromising of a user's secret. First, as a human is required for cognitive decryption of the grid, a computer cannot automatically collect users' secrets, as is possible with passwords, drastically increasing the overhead required to steal access credentials. Additionally, even if the attacker has a human to decrypt the grid and discovers the victim's categories, he cannot access the grid to log in, because only the legitimate user's computer has been activated with his software token.

Phishing

A conventional phishing attack is not viable against a user of Vidoop SecureTM; phishing is only possible when combined with a man-in-the-middle attack. Because the phishing site must be able to serve up a Vidoop Image Grid convincingly, and there is no guarantee that the phishing site will be able to present the categories that the user expects, phishing attacks are deterred.

With passwords, phishing can be conducted en masse, and the results parsed by computer and stored in a useful format; the information can then be exploited automatically. In a system secured with Vidoop SecureTM, a human must be involved both in the parsing of the results into a useful guess at the user's secret (his categories) and in the exploitation process by identifying the categories in the login process. This adds an enormous amount of overhead, making phishing a much more costly prospect.

And, again, even if a phisher manages to steal a user's categories, he will be unable even to attempt to log in as the user unless the attacker has a software token valid for that user.

Man-in-the-Middle

Vidoop SecureTM offers several effective deterrents to man-in-the-middle attacks. The first is that the user being served the grid must be activated with a software token, which the man in the middle must first intercept in order to be able to forward the grid. Then, assuming the man in the middle can intercept both the grid itself and the user's access code, human level cognitive decryption is needed in order to guess the user's categories and attempt to login as the user again. This, again, adds considerable overhead to the attacker when compared to a man in the middle attack against passwords.

Man-in-the-middle attacks cannot be automated efficiently against Vidoop SecureTM.

Sample Use

Alice wants to manage her funds at her online banking site, which is secured by Vidoop SecureTM. She hasn't logged in yet since her bank switched over to the new login system.

- Alice begins to enroll in her bank's Vidoop SecureTM system.
 - The enrollment process shows her 25 image categories and sample images from those categories and tells her to choose three. Because she likes boating, astronomy, and cats, she chooses boats, outer space, and cats.
 - The bank has Alice's phone number from when she opened the account, and they may also have her phone number – this allows her to receive activation codes.
 - Alice attempts to login to her bank's Vidoop SecureTM system for the first time.

- The system cannot locate her software token informs her that her computer has not yet been activated, and asks her how she'd like to receive an activation code
- Alice chooses to receive her activation code by voice phone call; the system calls Alice, and a recorded voice tells her a randomly generated activation code.
- Alice enters the code, and her computer is activated on the system with a software token.
- Alice is presented with a grid of 16 images, each associated with a randomly chosen letter. Among them are a picture of a cat with a letter X, a picture of a sailboat with a letter P, and a picture of a planet with a letter D.
- Alice types PDX as her access code, confirming her identity, and she receives access to her online banking account.

Next time she wants to log in, the process has changed just enough to foil many types of attacks on passwords:

- Alice enters her account number or user name on the bank's website.
- The Vidoop Secure™ system finds the software token, confirming that her computer has been activated.
- Alice is presented with a grid of 16 images, each associated with a randomly chosen letter. Among them, in different positions than last time, are a picture of a kitten with a letter A, a canoe with a letter Q, and a galaxy with a letter T.
- Alice types ATQ as her access code, confirming her identity, and she receives access to her online banking account as usual.

Secure User Configuration

Passwords are insecure. Not only are they readily vulnerable to the attacks described above; they also suffer from the simple problem that memorable passwords tend to be easy to guess. A long password made up only of the lowercase letter "a" is an easy password to guess, as is any password, however long, made up only of dictionary words; even passwords that replace letters with lookalike numbers are much easier to guess than random, unmemorable garbage. And regardless of how difficult passwords are to guess, easily available software enables even the most complex passwords to be stolen and used successfully by unauthorized parties. How many users know this, and how many know enough about the consequences of insecure passwords to care?

Secure configuration of a password system is in the hands of the wrong party: the user, who may not be technically savvy enough to devise a password that is both memorable and safe. However, with Vidoop Secure™, no one user configuration is less secure than any other -- a set of categories that's easy for a user to remember is no easier for an attacker to break than any other set of categories. A secure secret is no longer more difficult to remember.

In addition, a login configuration's security level is objectively demonstrable without the need for costly or time-consuming password audits. Because the difficulty of a Vidoop Secure™ login to guess depends only upon settings that an implementer can choose, it is unnecessary to allow a user to make a poor configuration choice and compromise security. Protecting the user from himself is easier than ever.