SUBROSA

SIMPLE USER BASED RESOURCE ORIENTED SEGMENTATION ARCHITECTURE

Eliminate Vulnerabilities Associated with Password Based Authentication

On a typical day, users access 25 password protected networks, applications or sites. It's a losing battle: Either they create different, complex passwords that are difficult to remember for each account (leading to insecure password storage) or they use a few simple passwords across many accounts, increasing the risk of a single stolen or broken password resulting in multiple breaches. Social engineering and phishing attacks compound the problem. These vulnerabilities exist because of the basic characteristics of passwords as human-readable shared knowledge.

SUBROSA™ solves this challenge by decoupling users and keys. SUBROSA™ creates long, extremely complex, non-human readable cryptographic keys that can only be reproduced through a combination of unique data resources and semantics. SUBROSA™ authentication routines are easily memorized and support any environment requiring password authentication. SUBROSA™ all but eliminates vulnerabilities to brute force attacks, shoulder surfing, social engineering and phishing. Additionally, SUBROSA™ seamlessly integrates with other authentication factors (e.g., tokens, biometrics, geolocation, etc.) as well as enterprise identity management and single sign on mechanisms.

Secure Channels SUBROSA™

SUBROSA™ is a cryptographic key generation and validation solution that overcomes the vulnerabilities associated with password authentication. Its unique Idiomatic Recognition™ technology facilitates memorization and eliminates insecure password storage. SUBROSA™ segmentation architecture defeats password cracking, shoulder surfing, social engineering and phishing.

Advantages:

- Integrates seamlessly with OS, app or device authentication workflows
- Eliminates the need for insecure password storage
- Defeats cracking, shoulder surfing, social engineering and phishing
- Interoperable with enterprise key management systems
- Integrates with possession/token, biometric and location based authentication factors

"The reality is, we have a system that not only is insecure but it's totally unusable. Most people just throw up their hands and don't bother with good password hygiene. It's good to have that complex 12- to 18-character password, but from a usability perspective, most people don't have the patience. Instead, they have one or two passwords that they use everywhere."

- Jeremy Grant
  Senior Executive Advisor
  National Strategy for Trusted Identities in Cyberspace

SUBROSA™ creates secure, zero-knowledge cryptographic keys

- **Semantically Meaningful Key Generation Eliminates Memorization Problems**
  SUBROSA™ users choose unique data resources to generate their keys and establish a personal interaction pattern with the resource. This relationship is intuitive and easily memorized, but not readily shared or stolen.
- **Threats Posed by Brute Force Attacks Are All but Eliminated**
  Without the original, unchanged data resource and knowledge of the personal interaction pattern, replication of a user's key(s) isn't feasible. As keys are very long and not human-readable, dictionary and exhaustive key search attacks are futile.
- **Defeating Social Engineering: You Can't Tell What You Don't Know**
  Conventional passwords are user generated and are generally 8 – 20 characters. They are easily shared and easily stolen by social engineers and phishers. SUBROSA™ keys are derived from long binary strings the user never sees. They can't be shared, stolen or phished.
- **Integrate Anywhere Authentication is Needed and Extend Your Authentication Factors**
  SUBROSA™ easily integrates with operating systems, applications and devices, providing stronger authentication anywhere a password is required, and integrates with other authentication mechanisms such as tokens, biometrics and geolocation to provide a complete authentication solution.

SECURE CHANNELS

16400 Bake Parkway, Suite 100
Irvine, California. 92618, USA

contact@securechannels.com
+1-855-825-6766 or +1-949-679-5777

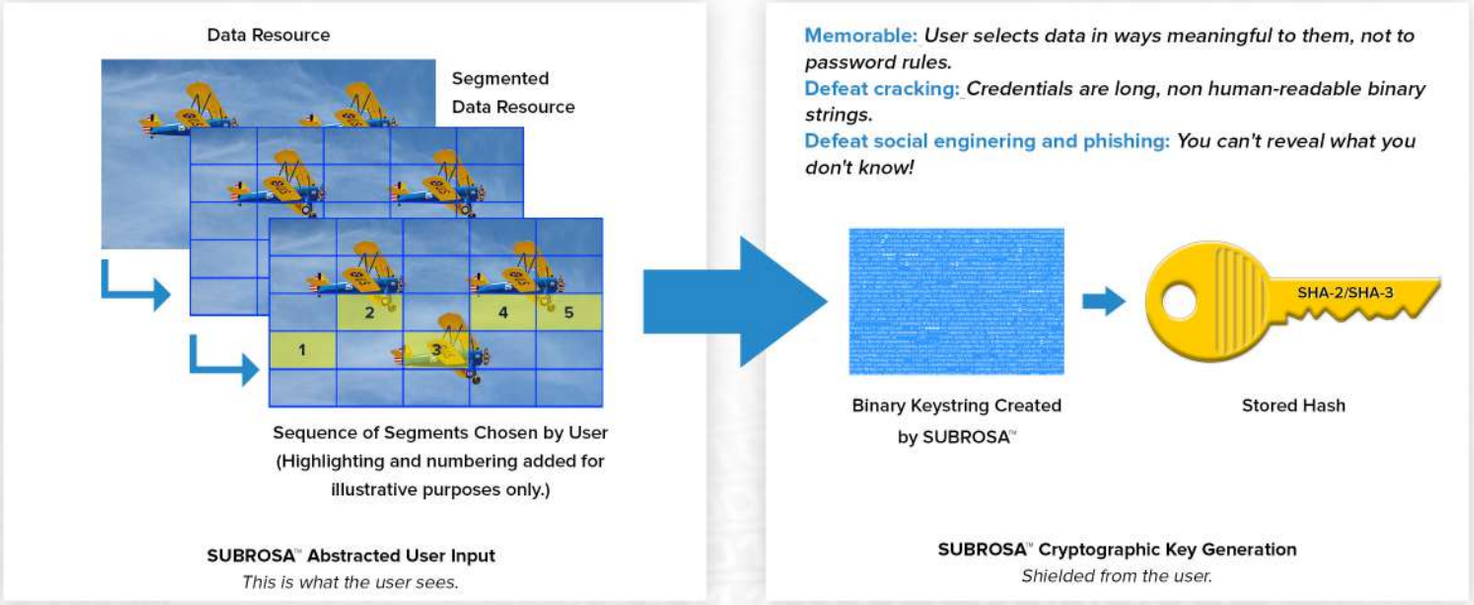
SUBROSA

SIMPLE USER BASED RESOURCE ORIENTED SEGMENTATION ARCHITECTURE

Breakthrough User Authentication Technology

SUBROSA™ Idiomatic Recognition™ technology simplifies the generation and validation of credentials from the user perspective while creating keys of such length and complexity that traditional attacks (cracking, phishing, shoulder surfing and social engineering) are frustrated. Unlike a password, which is conceived and generated directly by the user, SUBROSA™ decouples conception from generation, minimizing user burdens while ensuring keys are unique, complex and cryptographically secure.

When generating a key, users select a data resource (e.g., an image, document, video or audio file, etc.). SUBROSA™ grids the image into a number of segments, where each segment represents a discrete portion of the file's binary data. Users then choose a sequence of segments. SUBROSA™ concatenates the data from selected segments into a single, long string. This string is the key, which is then hashed and stored. Since the data resource and selection sequence have personal semantic meaning, memorization is simplified. As the key is built from the file's binary data (and only a hashed representation stored), the user is decoupled from the key generation process and the actual keystring remains unknown to the user. As a result, the user cannot be tricked into revealing a secret that she doesn't know.



Find Out More

Operating Systems, Desktop	Windows 7, 8, 8.1, 10
Operating Systems, Server (future)	Windows Server 2008, 2012
Development Libraries	.NET, Java, APK, C#

SECURE CHANNELS

16400 Bake Parkway, Suite 100
Irvine, California. 92618, USA

contact@securechannels.com
+1-855-825-6766 or +1-949-679-5777