REDUCING YOUR DATA SECURITY RISKS USING DECENTRALISATION

FIND OUT...

...The problems with central stores of data
...How decentralisation of private data works
...Why rolling key encryption makes data safer
...Ways to improve the user access experience

A CYBERSECURITY GUIDE BROUGHT TO YOU BY

How to improve data security

1. Stop relying on passwords for authentication
2. Decentralise and encrypt all records
3. Restore privacy

READ THIS FIRST
(IF YOU HAVEN'T ALREADY):
What's wrong with passwords?

"What you risk reveals what you value"

– Jeanette Winterson OBE, award winning author

The world's most valuable resource is no longer oil, gold or diamonds – it's data. Everyone wants easy access on demand, wherever and whenever we need it. Unlike the tangible and tradable commodities of previous centuries, data isn't finite. It won't run out.
If you want to create value from data you make it useful yet scarce.

Technology giants such as Google, Apple, Microsoft, Facebook and Amazon have gained incredible power and fortune by amassing more people's data than anyone else. However, for most individuals and organisations the value of data lies in the ability to keep it private.

Yet for the sake of convenience, many people make a few crucial errors:

- **Re-using the same locks and keys** for valuable asset stores
- Storing and securing all their private data in one or only a handful of locations
- **Relinquishing control** of how their personal information is used, stored and protected

Cybercriminals typically attack the weakest access point, whether that's a person, device or gateway, aiming to steal credentials that could be used to compromise multiple accounts.

"Passwords are no longer a paradigm that you can really trust in," warned Google anti-abuse researcher Kurt Thomas in a November 2017 interview with Mashable, adding that too many people disregard advice about not reusing passwords.

Central stores of authentication data are vulnerable

Traditional central authentication stores might be convenient for organisations, but they are very attractive targets for hackers:

- **One breach can yield a very high reward** – once hackers are inside a server holding authentication records they know they can access a wealth of information, including the keys (such as usernames and passwords) to help unlock other systems and records. (81% of all data breaches originate from a weak password being compromised)
- **Multiple attack vectors** – central stores are vulnerable to common attack vectors including password cracking, malware keylogging, shoulder surfing, social engineering and phishing.

So what are organisations doing to remove these vulnerabilities? Many organisations force Two Factor Authentication (2FA) on users because they don't trust the traditional username/password method for authentication. Central stores of data are expensive too: adding new layers of protection on top of old simply increases complexity and cost.

haventec

Central data breaches

A single successful attack on a centralised store of user credentials can impact millions of people – and cause massive damage to an organisation's reputation.

Recent examples of attacks that saw centralised stores compromised include:

- **198 million** US voters' contact data and voting profiles exposed by CNC Contractor
- **150 million** user accounts exposed at My Fitness Pal
- **147.9 million** user records exposed at Equifax
- **57 million** customer records exposed at Uber
- **6 million** customer records and logins exposed at Nice Systems, a Verizon Wireless partner
- **5 million** credit card records stolen from Sonic Drive-in
- **220,000** patient records including Social Security Numbers stolen from Copilot
- **350** high profile clients' records exposed at Deloitte including 4 US government departments, the UN and some of the biggest multinationals
- **US$3.62million** average cost of a data breach to an organisation

1-15 hours

maximum time most hackers need to breach an organisation and steal valuable data

[Source: 2018 Nuix Black Report into hacker trends**]**

What is data decentralisation?

There are two main types of data decentralisation designed to improve security and integrity:

1. **Distribution and storage of copies** of data records across multiple locations (e.g. Blockchain)
2. **Breaking data into multiple parts** and separating those parts across multiple locations

In the first case – **where a copy of a record is distributed to multiple locations** – decentralisation gives each authorised participant an accurate record of activity in the ecosystem.

If one copy is lost, there are plenty of backups; and if a copy of the record is tampered with, it can easily be checked against the 'true record'.

Group consensus on what the true record contains and how it can be used helps prevent exploitation by any one person. It can also prevent one person controlling all records.

In the second case – **where data records are broken into parts and separated** -- decentralisation means no data record is ever stored in its entirety in one place.

Instead, a data record is divided into multiple parts and each part is then stored separately from the others.

By storing data across multiple locations the record is very difficult to steal and exploit. Each part makes no sense without the others.

haventec

Rolling keys encryption

Decentralised data can be further secured with rolling key encryption (single-use), which is especially useful for protecting sensitive information such as:

- Identity – there is no central store or master list of each user's personally-identifiable information and access keys
- Personal (private) information – there are no complete records, so the data can't be analysed and exfiltrated
- Financial records – there are no complete ledgers of transactions (identity of the person transacting; identity of the account/s used for the transaction; amount of transaction; identity of receiver)

How can decentralisation with rolling keys make data safer?

> Eliminates traditional attack vectors

Deconstructing and decentralising valuable data makes common attacks such as phishing, shoulder surfing and social engineering practically impossible to execute.

These traditional attacks aim to steal user credentials in one go, often by tricking the user into sharing access authentication secrets, or by simply observing the user enter that information.

> Makes data harder to find

Ensuring credentials are never stored in one place makes it extremely difficult to find and retrieve any part of a record in the first place. And without all the parts an attacker can't exploit the information contained in the record.

> Removes risk of mass account breach

Mass breaches simply aren't possible if there is no central store of account records. Historically, an attack against a central store of account records (such as an authentication or payment gateway) could reward the hacker with a large set of logins or credit card data.

> Shuts the window of exploit opportunity

Decentralising and encrypting every single part of a data record increases security by making each part unreadable without all the other parts.

Encrypting the data with rolling keys ensures that any authentication data is single-use only. It becomes redundant the next time a user authenticates as the keys are rotated.

So, if a hacker somehow managed to steal some parts from various locations they would have to find, retrieve and recombine all parts to exploit the record – and they'd have to do this for every single user login and/or credit card.

The financial and time costs of conducting an attack are so exponential they likely outweigh the financial benefits of the attack for the hacker in the first place.

Haventec's decentralised authentication with rolling keys

At Haventec our approach is to never store any user secret or private encryption key anywhere.

Each time we authenticate a user we identify the device and reconstruct the single-use private key mathematically.

Once authenticated, we destroy all keys for that user.

We immediately create new keys, deconstruct and distribute them, ready for the next authentication request.

This provides a much stronger mechanism than traditional two-factor authentication. It also protects against common attacks such as phishing, shoulder surfing, social engineering, password cracking and malware keylogging.

haventec

User benefits of decentralisation

- **Confidentiality** – securing private data in every interaction returns control to the user and builds trust. When that trust is mutual, you make it easier for people to do business with you.
- **Easy to use** – allows user to authenticate with an easy to remember PIN and their authenticated device. Authenticate's single-use keys protect the interaction and remove the worry of protecting a password.
- **Faster access** – the user authenticates via their authenticated device and gets on with what they need to do, rather than dealing with multiple layers of security.

Haventec Authenticate decentralised identity login process

1. The user signs into the application* on their mobile phone^ using their username and user secret.
2. The application sends the encrypted user secret and encrypted device authentication secret stored on the phone to the Authenticate server.
3. Authenticate retrieves the server encryption key for that user device.
4. Authenticate regenerates the private key using Haventec's patented algorithm with the encrypted user secret, encrypted device authentication secret and server encryption key.
5. Once the private key is regenerated it is matched against the user's public key and if they match, it is a successful authentication.
6. All the old keys are destroyed.
7. New keys are created.
8. Authenticate deconstructs the private key using Haventec's patented algorithm to create a new encrypted device authentication secret.
9. The new encrypted device authentication secret is sent to the user's mobile phone and stored.

** Any form of application such as a mobile app, website, web application, desktop application etc. ^ The device could also be a laptop, desktop computer or TV*

Find out more: haventec.com

haventec