THREAT STATUS

In Partnership with

data SOLUTIONS

Visit
arc.threatstatus.com
to try the arc demo

Highlights

- Improve B2B and B2C authentication security and reduce fraud attempts to your public facing applications with zero additional user friction
- Instantly check your subscriber logins and signups against billions of already leaked user credentials from 3rd party data breaches
- Supports username and password pair or email and password pair leak checking
- No added requirement for your existing or future subscribers to interact with SMS or 2FA tokens which could result in user drop off
- Complete security and privacy of checked user credentials using known and trusted existing cryptographic algorithms
- Sub-second check and respond API's ensure rapid risk decisions can be made
- Easily integrates in parallel into your existing application authentications processes to remove any risk of application performance impact

Real-time Vulnerable Credential Checking Services

Overview

When it comes to building applications intended for public facing use, high levels of security need to be baked in, but it can be a challenging balance to implement robust security controls without damaging the user experience.

Traditional security controls designed for enterprises often aren't a good fit for consumers. Your customers want to be able to get access to your services and execute their actions quickly and without any hassle. Patience is not a frequently seen consumer virtue when it comes to internet applications and any friction added to a users journey can risks losing you valuable subscribers or worse revenue.

However, the reality is one of the biggest vulnerabilities to internet applications is the user themselves, and specifically their password behaviour.

End users don't understand the risks associated with weak password choices, or that using the same password across multiple applications introduces a security risk to your online service, but more importantly they don't really care.

Weak password choices and password reuse amongst internet applications remains a top security threat to online service providers so Threat Status have designed Arc specifically to minimise that threat with zero impact on the users authentication experience.

ARC

The Problem

Imagine you've developed and launched your online application, everything works perfectly and after extensive independent audits its been confirmed that there are no known security vulnerabilities.

User experience has been carefully planned to make sure your users can get to their desired objectives as quickly as possible, and things seem to be working perfectly. Congratulations!

But then you get reports of strange behaviour on your customers accounts. They're becoming unhappy and publicly questioning your application security on social media. An important client has just found out that a sensitive document has been leaked from your portal and wants answers. Activation codes for software have been purchased through your site but your users are denying making the purchase and asking for refunds. Complaints are coming in that loyalty points are going missing. Player accounts are being seized. Large amounts of unusual betting patterns are suddenly being seen against an unlikely winner.

These are all indications of account takeover and one of the most common methods attackers deploy for account takeover is credential stuffing.

Is Your Application Broken?

Probably not, but when a new client or customer wants to use your service then you're going to ask them to create an account, and during setup you're probably going to ask them to use their email address and chose a password but in many cases their password choices are going to be poor.

Credential Stuffing attacks are effective at taking over your user accounts because your customers frequently make weak security choices when they choose their passwords. To make matters worse you can't tell them that, and if you try to introduce additional complicated security controls you risk losing them altogether.

It's proven that most users will either use something very simple for their password choice, like Passw0rd1 (it meets the complexity requirement) or maybe they'll go for something a little more unique, but then use it over and over again across multiple applications because they struggle with remembering more than a couple of complex passwords.

This means that when a 3rd party application gets compromised and it's data is leaked, it could have usernames and passwords in it that work on your application too. It's a simple and widespread attack method.

Even though your application security remains perfectly intact, usernames and passwords that work on your application are now easily available to criminals, it was your customers password choice that made their account vulnerable but they're going to expect you to keep them safe and they don't want any complicated Multifactor Authentication slowing them down.

It's a complex scenario to address, and Arc is the answer.

How Arc Works

Arc is a service built on top of the Threat Status award winning leaked credential discovery solution.

Behind the scenes our credential discovery processes are constantly searching and examining data from dark markets and closed forums looking for new leaked credential data.

Our highly speed, secure APIs then integrate with login pages on applications like yours and respond almost instantly if the username and password combination input by your customers are already leaked on criminal forums. Knowing this information gives you complete upfront control of what to do next to protect your service and data.

Completely Anonymous And Secure

Arc has been designed from the ground up to protect your customer data while maintaining and improving the integrity of your application with zero added friction to your users journey.

When new username and password pairs are located on criminal forums each pair is extracted, cleaned, converted into a secure SHA256 hash and then encrypted using

homomorphic cryptography before being stored in our proprietary data lake.

For added security the original leaked usernames and password values are not directly retained in Arc and therefore not retrievable under any circumstances by attackers or even Threat Status internal personnel.

Once this leaked data is protected and stored in Arc it can be anonymously “queried” by your application using our API’s.

Due to the way Arc prepares and stores this data your application simply needs to go through a routine of generating a hash of the credentials you user is trying to use, submitting just a few bytes of that hash to Arc, at which point Arc then returns all possible candidates that could be the one your customer is currently using.

Trusted and established homomorphic encryption procedures can then be applied to the data returned by Arc at which point your application can determine with 100% accuracy if the username and password combination being used by your user is one of the billions already in the hands of criminals.

Arc is totally secure, totally anonymous, and 100% false positive safe. You can see it working for yourself by visiting arc.threatstatus.com and trying the arc demo environment.

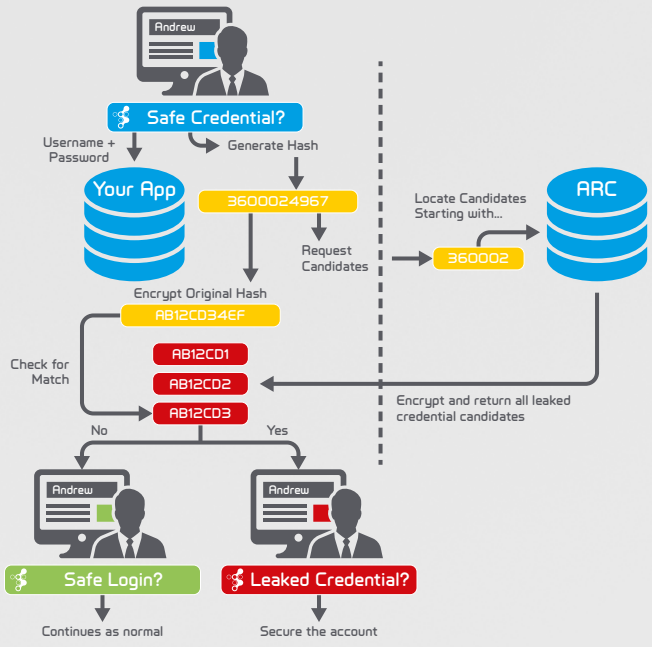

Figure 1 — Simplified Integrated Application Data Flow

Your Risk, Your Decision

Due to the fact that Arc requires no new steps for your customers like sending out tokens, enrolling a mobile number for SMS etc it is completely frictionless and transparent to your users.

Their private data never leaves your application, your application simply gives Arc a protected hint of what it’s interested in and within milliseconds of receiving the request Arc returns everything it knows about possible matches across it’s repository of billions of leaked credentials

If Arc returns a result that matches the one your user has input, what happens next is entirely up to you.

Whether that is blocking the login, notifying your internal helpdesk or turning down the privileges of the user until an investigation has taken place, Arc is invisible, frictionless, secure and gives you total control of your risk decisions.

Business Benefit

Arc helps protect your accounts from your customers own vulnerable security habits which are almost impossible to get them to kick.

A successfully compromised user account can be used by criminals for a wide spectrum of uses which could include financial loss, data theft, price manipulation, ransomware transmission, social engineering and lateral movement.

By integrating Arc into your authentication processes you are instantly adding billions of stolen user credentials to your organisations naughty list and demonstrating to your clients and customers that you are putting their account security first.

To learn more about Threat Status, visit: **www.threatstatus.com**

©2020 Threat Status Ltd, all rights reserved.