VU

Device Fingerprint

Identify the fingerprints of the devices.

Datasheet

Android V 1.4 / IOS V 1.4 / Cordova 1.1

What is it?

VU Device Fingerprint is a module of VU Fraud Analysis that identifies device fingerprints by collecting technical data and device properties of users who log on to an online system. It identifies authorized devices, generates rules that detect and prevent online identity the and electronic fraud. The device fingerprint can be used to predict the likelihood of fraud, based on someone's profile information.

Main Function

The main function of this module included in VU Fraud Analysis is to detect the device from which the user logged on to the system, and to obtain about 30 variables (fields can be parameterized) that, as a whole, make it unique.

The information is obtained through JavaScript or through an SDK if it is a mobile application. The device and all features obtained from it are linked to the user's account. For this reason, when accessing the system with a new device, the user has the possibility to add it as a known device, after having validated his identity using a two-factor authentication.

Once the device has been added and linked to the user, when such user wants to access the system again, the Device Fingerprint module compares the characteristics of that user's known device against a predefined list of rules (described later in this document), created from the VU Fraud Analysis administration console.

This process detects login variations and their impact on the similarity percentage
to decide which of the following actions needs to be run:

1. In the case there is no variation, that is, it is identical (100 %), validate the identity.
2. Verify that the device is within the allowed threshold (one considered valid).
3. Determine if a two-factor authentication is required.
4. Run actions previously defined in that module, if the threshold does not exceed the minimum value set.

VUTM Device Fingerprint can be integrated into your applications through the following SDK:

- Android
- iOS
- Cordova

Plugin

VU Device Fingerprint can be integrated into websites using JavaScript.

Noteworthy parameterizable fields

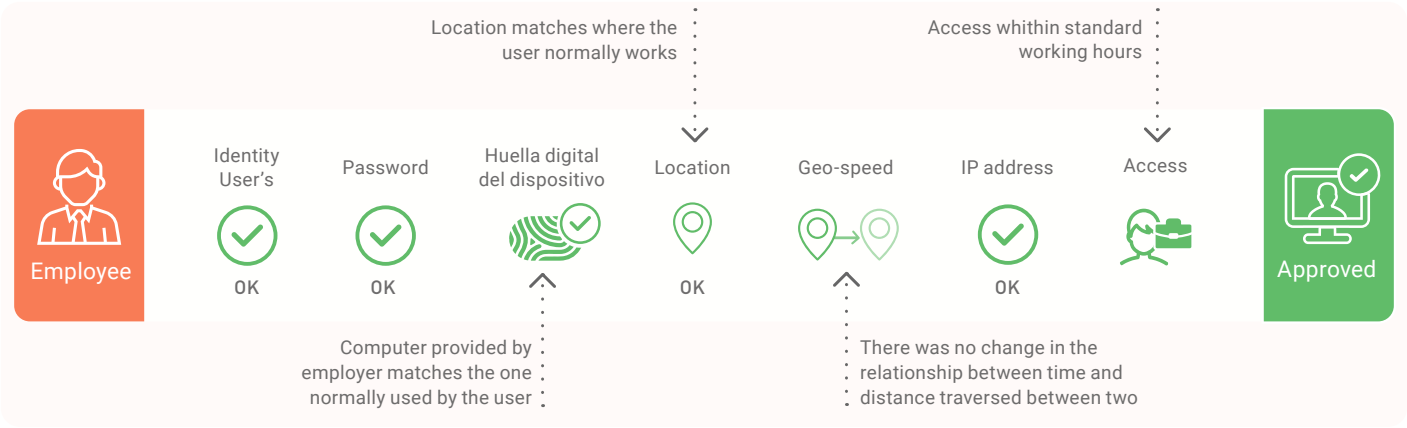
Below there is a list of the parameters that can be set to create the rules and validate whether the action to be performed is fraudulent or not:

Browser Agent	Lenguage	CPU type
Color Depth	**Versions**	**Operating System**
Sessions	**Time Zone**	**“Donottrack” Function**
Installed plugins	**Local Storage**	**WebGL Driver**
Screen resolution	**Fonts**	**Cookies**

Examples of use cases

The diagram below shows three di erent scenarios where Fingerprint obtains the fingerprint of the user's device that wants to access the system, compares it with the user's known devices and executes previously set rules to obtain the similarity percentage and either approve the access or take the necessary actions in case the similarity percentage does not exceed the minimum value already set (explained in the section about rules herein).

Scenario 1



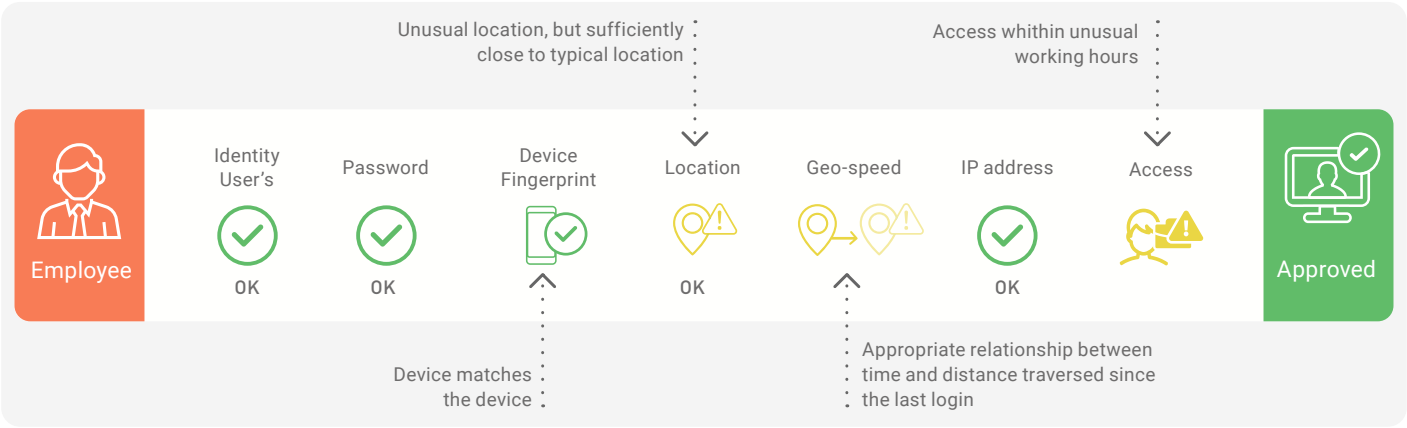
Context:

El empleado legítimo intenta iniciar sesión para acceder a datos de la empresa desde su PC de trabajo en una oficina en el Sur de California a las 9 a.m. PST.

Positive authentication:

The legitimate employee passes all the validations stages mentioned in the image and the Fingerprint similarity percentage of the device is 100 % (identical to a known device) so the risk-based authentication analysis is positive, and the authentication is approved so that the user can continue with the action.

Scenario 2



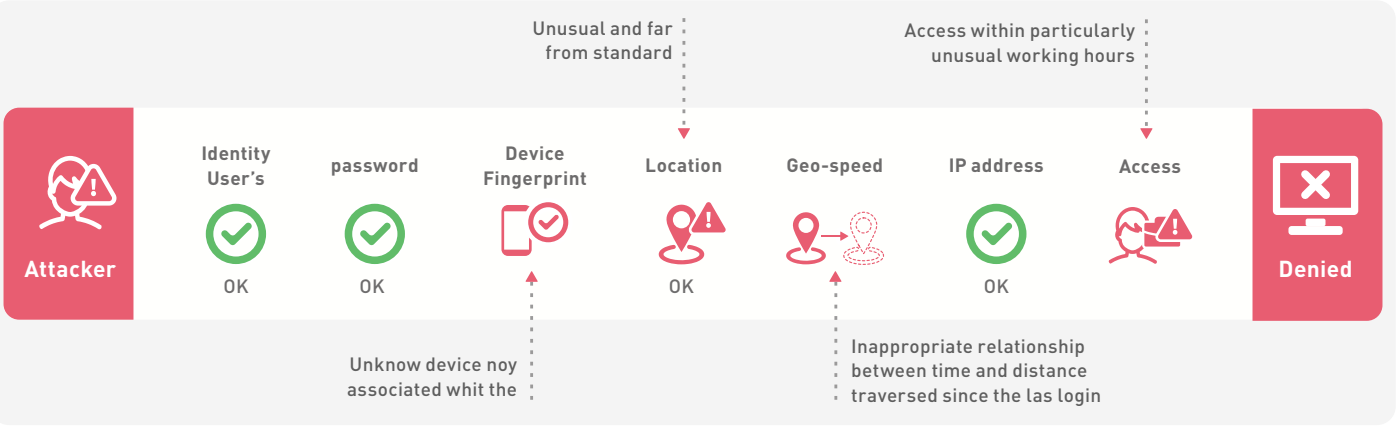
Context:

A legitimate employee attempts to log in to corporate email in San Francisco from a smartphone at 8:30 p. m. PST.

Positive authentication:

The legitimate employee changes location and accesses at an unusual working time; however, he validates his identity and the device fingerprint is validated, too as it belongs to one of his previously known and added devices, so according to previously set rules the risk-based authentication analysis is positive and the authentication is approved so the user can continue with the action.

Scenario 3



Context:

An attacker attempts to log in to access UK corporate data from a personal computer at 2 a.m. PST.

Positive authentication:

The attacker attempts to log in by validating the user's identity, but the device fingerprint does not match any known device for that user and the attacker is trying to access from a geolocation far from the usual one so the risk-based authentication analysis is negative, therefore the authentication fails, and the user cannot e□ect the transaction.

If you need more information or wish to schedule a demo of this solution, please email us at: sales@vusecurity.com