Multi-factor authentication using device fingerprinting

Multi-factor authentication methods are now essential to access services but are poorly adopted by users due to their extra complexity.
The b<>com [Terminal Authentication] solution introduces a new authentication factor based on cutting-edge device fingerprinting techniques. It adds a transparent layer of protection to authentication processes. By associating a user account with its device's hardware and software configuration, our approach prevents hackers from re-using login credentials acquired from phishing attacks.

{key features}:

- Authentication based on login credentials AND users' devices
- Patented method to prevent spoofing
- Easy to manage devices linked to an account
- OS agnostic and compatible with most popular Internet browsers
- SDK available for Android Apps

{benefits}:

- **Enhance your security with an additional robust and safe authentication factor**
- **Offer frictionless users experience: transparent, no software installation**
- **Integrate it easily into any existing access control service as an extra layer of protection**
- **Lower the TCO of your two-factor authentication solution**

{applications}:

- Internet services
- Subscription services to multimedia contents and account sharing detection
- Asset management
- Fraud detection and prevention services
- Banking

sales@b-com.com

<www.b-com.com>

b<>com [Terminal Authentication]

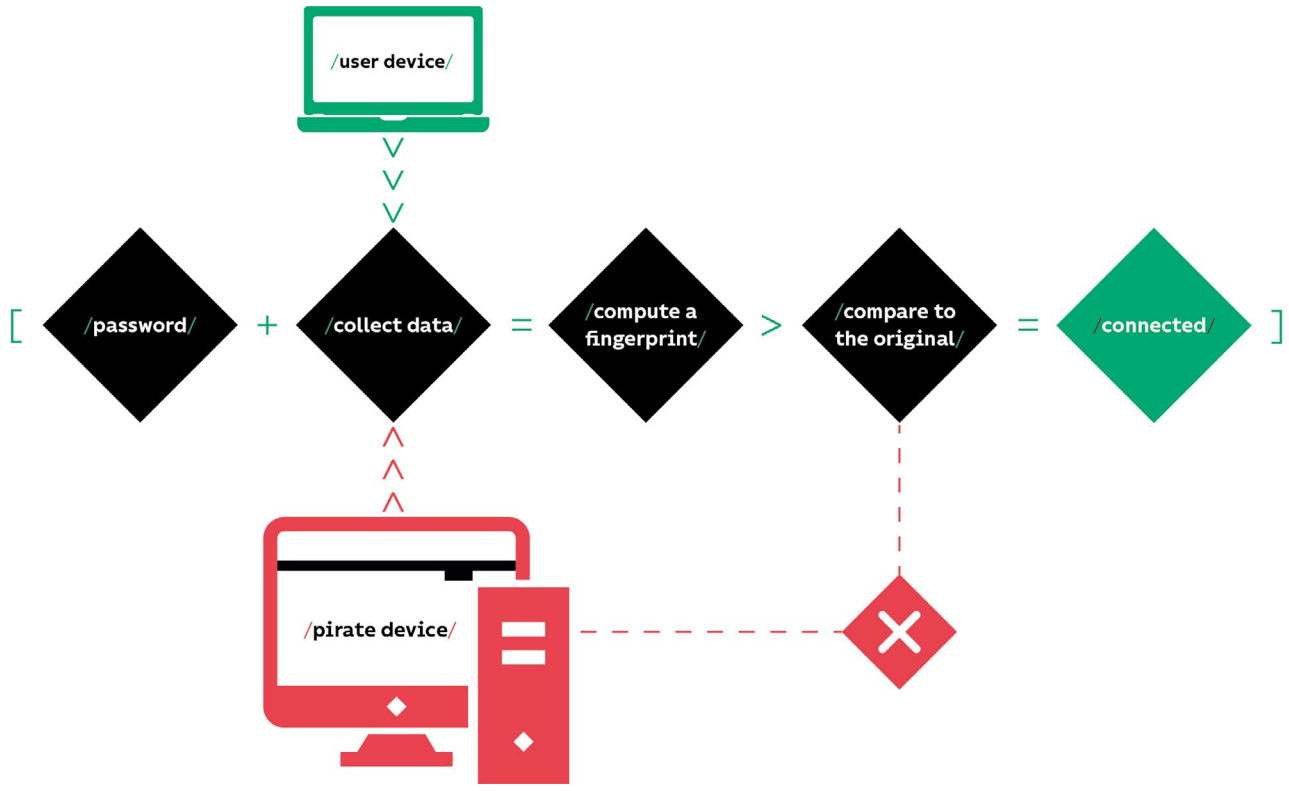
{how it works}:

Our approach uses cutting-edge device fingerprinting techniques to link one or more devices to a user account; only those devices would be eligible to access it. Device fingerprinting is a fairly new method that gathers software and hardware information from users' devices and then aggregates them into a vector called a "fingerprint". **b<>com [Terminal Authentication] gathers more than 200 pieces of information, making fingerprints very likely to be unique (collision rate below 1 out of 500 million)**.

On any connection attempt from a user to a given account, it collects the fingerprint and compares it to previously saved fingerprints linked to this account. The connection is allowed only if there is a match. This prevents hackers from re-using stolen login credentials.

On top of that, a patented solution prevents hackers from spoofing a fingerprint. Our idea is to take advantage of the possibility to customize certain fingerprint elements to create challenges that are in no way predictable for a hacker.

{overview}:



{about b<>com}:

A technology pioneer and provider for companies that want to digitally boost their competitive edge, b<>com addresses several industries: culture & creation, digital infrastructures, health, defence and industry 4.0. Its laboratories bring together talented people from a variety of disciplines and cultures in areas like artificial intelligence, immersive video and audio, content protection, 5G networks, the Internet of Things, and cognitive technologies.
b<>com's researchers and engineers, drawn from the ranks of industry and academia, work at its Rennes campus and at its sites in Paris, Brest, and Lannion.
Thanks to its world-class engineering team, its technology platforms and its unique mix of scientific and industrial knowhow, b<>com offers its clients technology solutions that give them invaluable competitive edge.

01/2020

sales@b-com.com

<www.b-com.com>