NETWORKWORLD
The Leader In Network Knowledge
www.networkworld.com September 8, 2016

NuData Security adds 'unspoofable' dimensions to the identity process

By Linda Musthaler, Principal Analyst with Essential Solutions Corp.

In 2012, the social networking site LinkedIn suffered a data breach in which username/password combinations were stolen. Four years later, in 2016, at least 117 million sets of credentials from this breach were available for purchase online. MySpace suffered a similar data breach, and years later 427 million sets of credential were posted online.

These events have prompted e-commerce companies that have not suffered a data breach to urge their customers to change their passwords as soon as possible.

If Amazon and Netflix didn't leak their customers' credentials, why are people receiving notices to change their account passwords? It's simply because people tend to reuse their usernames and passwords on numerous websites, and these e-commerce companies don't want to see an increase in fraud from their customer accounts.

According to TeleSign, 73% of online accounts are guarded by duplicate or reused passwords. 47% of people use passwords that are at least five years old, making them vulnerable when an old stash of stolen credentials turns up online.

The use of stolen credentials is a critical problem these days, especially for e-commerce companies and financial institutions that are experiencing increased fraud rates. When a person using John Doe's username and password is logging into an online banking application, how can that bank be certain it's really John Doe logging in and not someone who bought the credentials off the Dark Web? A second authentication would certainly help, but many businesses are hesitant to force multifactor authentication (MFA) on customers due to the inconvenience factor.

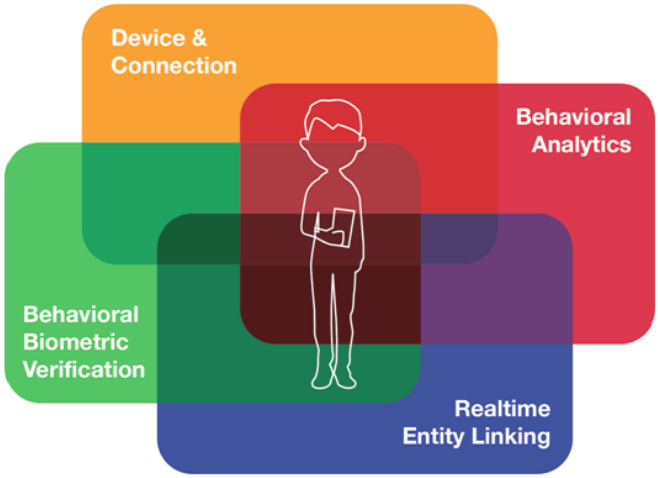
One vendor that offers a unique method of user verification for web-based and native mobile applications is NuData Security. The company specializes in distinguishing one human from another in a digital world so customers gain confidence about whether or not the person using John Doe's credentials really is the legitimate John Doe.

When somebody is interacting with a web or mobile application – e.g., logging in, opening a new account, making a purchase or conducting a financial transaction – the company behind that app needs more than just credential data to build confidence about who the user is. NuData monitors that user across a number of different layers in order to build a profile that gets associated with the user identity.

As that user identity has repeated interactions with the application, NuData uses analytics to determine if it is the same human behind the actions each time, or if a different human is now utilizing the account. All of this is done in real-time so NuData can provide a confidence score to the application owner in time to challenge the login or other activity of someone who is abusing a legitimate user identity.

NuData's solution, called NuDetect, is implemented in a customer's web or native mobile application environment. The web environment uses JavaScript, while the mobile app is implemented with a software development kit (SDK). In both cases, the implementation is totally within the application; there's nothing to download or install on end user devices.

For each user that creates an account on a protected application, NuDetect builds a profile based on multiple dimensions, including behavioral analysis, passive behavioral biometrics, and device and access intelligence. Creating and using this user profile is transparent to the user, which in itself is part of the security of this solution. If an attacker doesn't know how a user account is profiled, he finds it harder to spoof the attributes of the profile.



One of the more interesting dimensions of the profile is the passive behavioral biometrics. This has to do with the person's interaction with their device. For this reason, NuData builds a profile for each type of device that a user account uses; for example, a PC, tablet or smartphone.

For a PC, NuData looks at things like how a person uses the keyboard. What is their type speed and deviation? Do they use a touchpad or a trackball? Do they appear to be left or right handed? On a mobile device, the profile would include how the person holds the device spatially. Is it the same way the person has held the device in the past? How do the person's fingers plot on the screen? Those kinds of attributes are pretty personal and would be hard if not impossible for an attacker to mimic.

NuData's differentiator is its ability to pull together all of those attributes about how someone is interacting with their device. This helps to build a profile for that particular user and how they typically interact with the application. NuData can then look at the probability that it is the same user and that they are interacting in the same way each time they come back. NuData has the ability to not just say that the data points are correct and the behavior is correct, but given the way that the user actually entered their authentication details – the username and password – it really appears to be the same human on the other side of that machine entering those data points.

If the username and password is correct, but the input profile is different, then it can be determined with a high level of probability that it is a different human trying to interact with that account.

Here's how it works in practice. When someone accesses an application using an existing user ID, NuData analyzes the profile attributes in real-time. Within milliseconds, NuData delivers a confidence score to the application owner which indicates the probability of the user being the legitimate account holder. If the probability is low, the application owner can take various actions; for example, require a second form of authentication to login such as typing in a code that is sent to the registered user's cell phone or email. In some cases, the application owner might choose to block the login or deny a transaction that is likely to result in a fraud event.

NuData can submit the results of its analysis directly into a SIEM if desired. This enables the information to become part of the larger scope of security data that the application owner utilizes.

The NuDetect solution uses machine learning to continuously refine its user profiles. This is helpful in situations where the collected attributes of the legitimate user might change; for example, if a person injures their hand and types differently or holds the smartphone differently. If all other attributes appear to be on track according to the stored profile, the solution can adapt the profile with the new traits.

Though they remain the top method of identity verification today, user credentials alone are no longer trustworthy. NuData adds many other unspoofable dimensions to the identity verification process for online and mobile applications.

NU DataSecurity

999 Canada PL #550
Vancouver, BC V6C 3T4
+1 (604) 800-3711

www.nudatasecurity.com