Jason: Just Another Spy On Network

New Ways to Verify Humans Online – Adaptive Authentication

When you imagine an adversary infiltrating your cyber security – do you think of a Jason Bourne movie?

Maybe you should. The plots for this movie series are riddled with a plethora of cyber security mishaps that closely resemble real-life scenarios that take place in global enterprises every day.

The set-up for Jason Bourne is that he had been with his agency for over 10 years and, for a host of reasons, becomes disenfranchised. As a trained spy, he can create multiple personas impersonating various characters. Mysteriously, he can create synthetic personalities and spoof real identities to access restricted, sensitive information. These types of attacks are exactly what happens every day in multinational corporations and government organizations who are deploying critical human assets to sensitive areas around the globe. The safety of these individuals is dependent on classified information remaining classified. It is challenging to ensure that it be impossible for the wrong individuals to access classified information while simultaneously making it easy for the right people to access that same information, from anywhere, at any time, from any type of device.

Historically this has been done by issuing credentials to individuals that serve as digital proxies for identity authentication in cyberspace. These credentials fall into three categories – something you know, something you have, and something you are. We recognize them respectively as passwords, tokens, and biometrics. The problem is they can all be stolen, replicated, and compromised.

As a spy, Jason Bourne takes advantage of this constantly, and is able to access information without anyone's knowledge. Therefore, adaptive authentication of the individuals trying to access information is critical. How do you ensure only the right people have access to the right information all the time?

While information technology ("IT") security is still principally focused on static credentials as the primary means of authenticating people, the techniques that fraud management have been using for decades are now beginning to be applied to IT security and authentication. These techniques include **contextual attributes, advanced analytics, machine learning, profiling, and supervised and unsupervised learning.**

If ID Dataweb's Attribute Exchange Network (AXN™) had successfully authenticated Jason Bourne 5 minutes after he had hacked his way into the network indicating that he was in New York City, and then we see another authentication request from Jason Bourne that he is now in Hong Kong, we would have known there is a problem. There is no physical way Jason could have gotten from New York City to Hong Kong in 5 minutes, so one or both of those two transactions was fraudulent.

Adaptive authentication relies on several factors, such as how often the user typically accesses an account from a mobile device or PC, and whether it is from a previously known device. In addition, this service is used to check how quickly the user types in their username and password/PIN, and from what geographic location they most often access their account. By continuously monitoring these behaviors and patterns, organizations substantially improve their ability to detect when an unauthorized user is trying to access the network, or whether an account has already been compromised and now needs to be locked down. Additional security mechanisms are then proactively enacted to ensure access is given only to approved users.

AXN™ Gateway Model

ID Dataweb's AXN™ enables customer access to over 40 Identity Providers (such as Microsoft, LinkedIn, and enterprise credentials) and Attribute Providers (such as credit bureau, enterprise directory, device identity and biometric services). We anticipate having 80+ Attribute Providers available by 2018.

The AXN™ identity service will securely federate logins (BYOId - bring your own identity) for users with partner high assurance credentials (e.g., CAC, PIV, PIV-I) and verify user contextual attributes (e.g.,

clearance, employment, device identity, location, etc.) based on dynamic policy using any number of partner attribute services.

In addition, AXN™ customers create and manage access policies and preferences dynamically to deliver trusted and scalable federated Attribute Based Access Control (ABAC). Because attributes are evaluated and policies are modified in real-time, the AXN™ responds simultaneously to changes in threat levels at the individual, program, organization or coalition level. Should the user's credential and contextual attributes satisfy the ABAC policy requirements, they will be granted selective access to data using coalition policies for information labeling and handling that are stored in one or more data repositories.

Integrating the necessary data protection technology into this environment significantly advances the evolution of federated identity management and data access controls. ID Dataweb is part of the Aerospace & Defense community in using the AXN™ to implement a trust framework to establish the appropriate governance around secure identity federation and information labeling, handling, and data sharing.

We are particularly excited that customers realize savings with the AXN™ while significantly enhancing security, privacy and usability. There are substantial business benefits to deploying adaptive identity authentication and advanced analytics in making authentication and authorization decisions. Some of the more impactful include:

- Creates seamless end-user experience through adaptive authentication
- Reduces fraud and builds transaction trust significantly through fine grained attribute based access control
- Enables enhanced, secure user access from a wide variety of devices
- Leverages and interoperates with existing enterprise infrastructure
- Insulates complexity and lowers costs through high availability cloud services and integrates in hours
- ID Dataweb provides a single contract through which all attribute provider T&C's, opt-in and consent requirements have been harmonized

ID Dataweb's cloud platform is typically deployed and fully functioning within days, thereby saving time, money, protecting assets, and building trust. The AXN™ open API connect capability enables any organization to leverage data records of employees to begin the verification process while implementing identity services that enhance the privacy and security for an enterprise to interoperate effectively.

Continued reliance on traditional credential based authentication will not meet either the security or usability requirements of today's hostile cyberspace environment. For mission-critical operations, the extreme downside risk of data loss and enterprise breaches is that people could be drastically impacted, and in some cases, human lives are at risk.

Jason Bourne adventures often sound unrealistic. However, the daily terrorist activities happening around the globe prove otherwise. Making the decision to increase the security you currently have for screening the individuals accessing and using information within your organization is indeed your first and primary perimeter of defense for your enterprise.

Andy Grove, American businessman, engineer, author and a science pioneer in the semiconductor industry once said, "Success breeds complacency. Complacency breeds failure. Only the paranoid survive."

To learn more about ID Dataweb's AXN™, please contact sales@iddataweb.com or visit www.iddataweb.com.