ADAPTIVE MULTIFACTOR AUTHENTICATION (A-MFA) SYSTEM

Auth-Spectra is a patented technology (US 9,912,657) for Adaptive Multi-Factor Authentication (A-MFA) that uses a combination of passwords, biometrics, cognitive behavior, and other factors in order to create a trustworthy authentication system that intelligently selects the most appropriate authentication factors. A-MFA does this by selecting modalities based on the device in use and surrounding conditions providing the perfect balance between powerful security and low-maintenance usability creating a secure, highly confident authentication framework that you can trust.

APPLICATIONS

Continuous, high-confidence, identity authentication for:

» Banking, including online funds transfer
» Online testing in education and training settings
» Secure access to Electronic Medical Records
» Access to sensitive sites by government employees and others
» Smart Grid Security
» Internet of Things (IoT) sensory data access
» Use in Blockchain Technology for access verification to open ledger
» Gas pipeline and related industry applications
» General user Internet access & email services
» Opening payslips or sensitive documents using A-MFA
» Specific web services such as PayPal, Netflix and other paid services

Deployable at different levels of Internet Computing:

» Application level (financial applications, email/business/personal applications, social applications)
» User level (root user, administrators, guest user)
» Document level (PDF containing application form, document containing proprietary information, image/video containing confidential and sensitive footage)
ADVANTAGES OF ADAPTIVE MFA SYSTEM

The major advantages of the implemented framework over other existing MFA technologies:

» Assures user identity during an interactive session and beyond the initial log-in.
» If an authentication modality is compromised, the system can adjust to authenticate users with the remaining non-compromised modalities.
» It ensures avoidance of repetitive selections to authenticate users if the operating conditions remain the same.
» Scalable: New authentication modalities can easily be integrated to augment the existing sets of modalities.
» Flexible: Allows for generation of the operating/configuration parameters for the added authentication modalities as they become available.
» Just-in-time selection algorithm chooses optimal authentication modalities for the user’s operating environment.

COMPARISON WITH OTHER EXISTING MFA APPROACHES:

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Vendor</th>
<th>Factors</th>
<th>Features</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecureAuth IDP</td>
<td>SecureAuth</td>
<td>Two factors and SSO (out of 20)</td>
<td>Mobile, cloud, web or VPN</td>
<td><a href="http://www.secureauth.com">www.secureauth.com</a></td>
</tr>
<tr>
<td>RSA SecureID</td>
<td>RSA</td>
<td>Two factors</td>
<td>Software (smartphones, tablets and PC) and hardware authenticators</td>
<td><a href="http://www.nsa.gov/secuirty/rsa-secureid.htm">http://www.nsa.gov/secuirty/rsa-secureid.htm</a></td>
</tr>
<tr>
<td>Safenet</td>
<td>SafeNet</td>
<td>Two factors</td>
<td>Cloud, Password + SMS/Hardware Token</td>
<td><a href="http://www.safenet-inc.com/multi-factor-authentication/?rubinum=2">www.safenet-inc.com/multi-factor-authentication/?rubinum=2</a></td>
</tr>
<tr>
<td>SecurEnroy</td>
<td>SecurEnroy</td>
<td>Two Factor</td>
<td>Tokenless (One-swipe, SMS Preload, Soft Token, Voice Call, Email Preload)</td>
<td><a href="http://www.securenroy.com">www.securenroy.com</a></td>
</tr>
<tr>
<td>Symantec O3</td>
<td>Symantec</td>
<td>Cloud identity and access control</td>
<td>Cloud applications (set policies for groups, persons, devices) [security control point]</td>
<td><a href="http://www.symantec.com/page.jsp?id=03">www.symantec.com/page.jsp?id=03</a></td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>Microsoft</td>
<td>Multi factor</td>
<td>On premises and cloud authentications</td>
<td>azure.microsoft/en-us/services/multi-factor-authentication/</td>
</tr>
<tr>
<td>Deepnet DualShield</td>
<td>Deepnet</td>
<td>Two factors out of 10 different methods</td>
<td>SMS, Voice, Mobile App, Face, Keystroke, Smart Cards</td>
<td><a href="http://www.deepnetsecurity.com/products/dualshield/">www.deepnetsecurity.com/products/dualshield/</a></td>
</tr>
<tr>
<td>Swivel Secure</td>
<td>Swivel</td>
<td>SSO + two factor</td>
<td>Mobile App, SMS, tokens, telephony, Browser</td>
<td><a href="http://www.swivelsecure.com">www.swivelsecure.com</a></td>
</tr>
<tr>
<td>miniOrange Strong Authentication</td>
<td>miniOrange</td>
<td>SSO + two factor</td>
<td>14 different authentication types</td>
<td>miniorange.com/strong_auth</td>
</tr>
<tr>
<td>Duo Security</td>
<td>Duo Security</td>
<td>Two factor</td>
<td>Duo Push, Mobile Passcode, SMS, Phone callback, hardware token</td>
<td><a href="http://www.duosecurity.com">www.duosecurity.com</a></td>
</tr>
</tbody>
</table>
SAMPLE SCENARIO:

Currently use the same authentication method to authenticate the user.

AUTH-SPECTRA FEATURES:

- **CONTINUOUS IDENTITY PROTECTION**: Auth-Spectra is always on, ensuring the user's identity as long as they are connected to the system or service.
- **JUST-IN-TIME DECISION**: Authentication modalities are selected in real-time, providing the optimal decision for any authentication attempt.
- **CLOUD IDENTITY MANAGEMENT**: Auth-Spectra provides a cloud-based solution to administrate your existing services efficiently.
- **BROAD RANGE OF APPLICATIONS**: Auth-Spectra is available for many applications including healthcare networks and online education.
- **MACHINE LEARNING APPROACH**: Auth-Spectra utilizes machine learning techniques to analyze user behavior and select modalities based on intelligent algorithms.
- **BUILT WITH THE FUTURE IN MIND**: The Auth-Spectra framework is robust and flexible enough to meet your current and future authentication needs, such as adding new sensors and modalities.
THE INVENTOR

Dipankar Dasgupta is a Professor of Computer Science at the University of Memphis. He joined UofM in January 1997 and since then he has been significantly involved in research, education and service activities. Dr. Dasgupta is at the forefront of research in applying bio-inspired and machine learning approaches to cyber defense. Some of his groundbreaking works, like digital immunity, negative authentication, cloud insurance model, and Auth-Spectrum put his name in Computer World Magazine and other News media. Dr. Dasgupta is an Advisory Board member of the Geospatial Data Center (GDC) Massachusetts Institute of Technology since 2010 and has worked on joint research projects with MIT.

Dr. Dasgupta published two textbooks, two edited volumes and several co-edited journals and conference proceedings. His latest textbook, Advances in User Authentication was published by Springer-Verlag August 2017 (already having 2730 downloads according to Bookmetrix). Dr. Dasgupta’s multidisciplinary research resulted in more than 250 publications with 15000+ citations and having an h-index of 56 per Google Scholar. He received five Best Paper Awards at international conferences (1996, 2006, 2009, 2012 and 2017) and two Best Runner-Up Paper Awards (2013 and 2014). Among many other university awards, he is the recipient of the 2012 Willard R. Sparks Eminent Faculty Award, the highest distinction and most prestigious honor given to a faculty member by the University of Memphis. Dr. Dasgupta received the 2014 ACM SIGEVO Impact Award and also designated as an ACM Distinguished Speaker. Since 2007, he has been organizing the Symposium on Computational Intelligence in Cyber Security (CICS) at the IEEE Symposium Series on Computational Intelligence (SSCI) and the annual Cyber Security Summit at the University of Memphis. Dr. Dasgupta has received external funding from different federal agencies including NSF, DARPA, IARPA, NSA, NAVY, ONR DoD and DHS/FEMA. He has received continued research support for last 20 years and is one of the faculty members with an excellent funding record in the University.