Intralinks® Best Practices in Security: Risk-Based Multi-Factor Authentication

With an increasing amount of critical information living online, risk-based multi-factor authentication has become a business imperative for most banks, financial and government institutions.

In addition to the usage of a password, which is a form of single-factor authentication, multi-factor authentication can leverage two forms of verification to reconfirm the identity of the user, acting as a shield to protect users and customers from unauthorized access to their content and information. This paper will discuss Intralinks' approach toward risk-based multi-factor authentication

Adaptive Authentication

Intralinks' risk-based multi-factor authentication is powered by RSA® Adaptive Authentication, an authentication technology that conducts a risk assessment of user's activity behind the scenes. A unique risk score is assigned to each activity, and users are only challenged when an activity is identified as high-risk and/or an organizational policy is violated. This transparent authentication enables organizations to increase security without compromising user convenience.

How it works:

RSA Adaptive Authentication assures a user's identity by comparing the profiles of an activity with their typical profile pattern. It requires a profile building period, during which time the technical parameters of the users' computers and their behavioral patterns are recorded.

Adaptive Authentication makes extensive use of device fingerprints to make determinations about the risk of a user's actions. A key aspect of Adaptive Authentication is the registration and usage of user devices, such as laptops and personal computers that initiate requests for services.

Device fingerprinting enables strong authentication while continuing to use the hardware that users already possess, without requiring them to purchase new hardware tokens.

Along with other important user-identifying parameters, device fingerprint information is fed to the RSA Risk Engine for assessment and user profile building.

Device fingerprint information includes:

- The user's browser (type, version, etc.)
- The user's screen display (width, height, color depth, etc.)
- Installed software — software versions of commonly installed programs such as media players, flash players, java and others
- User's system time zone settings
- User's regional and language settings

If the device information does not match or a new request is outside of the usual behavioral pattern, a higher risk score will be reported and additional challenges may be presented to the user. Rules within the Risk Engine can be configured to add weight to different parameters such as, their IP address range, time of access, days since last access and so on. Additionally, the Risk Engine has a feed from the eFraudNetwork, RSA's database dedicated to sharing and disseminating information on fraudulent activity. The eFraudNetwork is engineered to proactively identify and track fraudster profiles, patterns and behavior across more than 65 countries.

Example:

A user consistently accesses an Intralinks exchange from the same computer at the same time using the same connection speed. When this user's profile is first created in our system, the Risk Engine does not have enough information to evaluate the user's 'normal' behavior. Over time, information is collected, and the risk score gets lower. Now, any deviation from the user's typical behavior will cause a spike in the risk score.

If the user in our scenario decides to do some work while vacationing, the Risk Engine will report an elevated risk score because the computer, the source IP, usual time of access and many other parameters, will be different. The application, then can present the user with additional challenges, also known as second factors. Those factors can be varied and if the risk is assessed as fraudulent, the request can be summarily rejected on the policy server.

Authenticating Users

Electronic systems rely on the information presented by users to make decisions as to whether to trust them as authentic (they are who they say they are). This information is created by a combination of 'tokens' that fall into one of the following three categories:

- Something you know — User IDs, passwords, passphrases, personal information, etc.
- Something you have — PCs, laptops, hardware tokens (e.g., SecurID), smart phones, etc.
- Something you are — fingerprints, iris scans, retina scans, etc.

Multi-factor authentication systems rely on two or more of the tokens listed above to authenticate the user.

RSA Adaptive Authentication uses the following token types in standard access scenarios:

- What you know — Memorized Secret Token: Username/password controlled by the deploying organization
- What you have — Look-up Secret Token: Device identification and forensics conducted by RSA. When users cannot be positively authenticated using device identification, step-up authentication is applied.
- What you are/do — Behavioral Analysis: RSA uses a sophisticated set of behavioral analytics, including IP Geo location and ISP Velocity, to determine "what a user does/is".

If the combination of the above listed tokens do not provide positive authentication, the RSA Adaptive Authentication requests Step-up Authentication tokens as follows:

- One-Time Password: An RSA generated code that Intralinks delivers to the user's email address
- Memorized Secret Token: Challenge questions (also known as secret questions) that the users enter on their profile page

Intralinks Multi-Factor Authentication

While Adaptive Authentication provides the best opportunity to balance security and usability, Intralinks also offers the exchange manager the following forced challenge options – One-Time Password or Security Question. These options will necessitate the user to provide a One-Time password or an answer to a question for each exchange access request. The exchange manager can choose from six available security options to assure appropriate protections for data according to sensitivity of the information stored in the exchanges.

- Standard — one-factor security that does not take advantage of risk engine
- Risk-Assessed Challenge Question then One-Time Password — this option will challenge all users with high risk scores with a security question, and after three failed attempts will escalate to a One-Time Password
- Risk-Assessed Challenge Question — this option will challenge all users with high risk scores with a security question, and after three failed attempts will lock out the user. A call to Client Services is required to unlock the user.
- Risk-Assessed One-Time Password — this option will challenge all users with high risk scores with a one-time password
- Always Challenge Question — this option will challenge all users with a security question every time they access the exchange
- Always One-Time Password — this option will challenge all users with a one-time password every time they access the exchange

Intralinks requires no additional downloads or registration to take advantage of this additional security. If the security setting of the exchange or a high risk score requires an additional challenge, a pop-up will instruct the user to enter the additional factor (a challenge question/answer or the One-Time Password delivered to the user's email account). The user experience may differ from one exchange to another in that some may be set up for no additional security factors, while others may be configured to require additional factors each time a user enters the exchange.

Intralinks and RSA

RSA is a well known, trusted and time-tested brand in the electronic security realm. It offers a number of key advantages:

- Supports a promotional model for security. A customer can choose the strength of second factor.
- Provides existing device-based (customer PCs and laptops) authentication risk assessment
- Minimize the 'pain' for users. No hardware to distribute, no plug-ins to install and no extra registration
- Provides administrative web-based interface to set up policies, monitor risk profile and conduct manual user management
- Adaptive Authentication is used in the majority of online banking applications, and the 'look and feel' is known to the large user population.

The Intralinks Advantage

Intralinks provides enterprise-class solutions, which facilitate the secure, compliant and auditable exchange of critical information, collaboration and workflow management inside and outside the enterprise. Our on-demand solutions help you organize, manage, share and track information, enabling you to accelerate your workflow, optimize your business processes and realize new profit potential.