Safelayer's Adaptive Authentication: Increased security through context information

The password continues to be the most widely used credential, although awareness is growing that it provides insufficient security for most applications. Digital activity on the Web is of great interest to companies, consumers and citizens, with the trio of cloud computing, mobility and social networking driving exponential growth. However, threats and attacks have also increased, especially phishing, pharming and identity theft in general. In this type of environment, a technical solution that dynamically scales security based on popular, albeit not very secure, credentials to high-security credentials based on risk, and simplifies the user experience to the maximum may be the answer.

Context, risk and adaptive authentication factors

La autenticación Traditional authentication is based on one credential that involves one or multiple factors. With at least two factors, high or very high levels of security can be obtained, whereas with only one factor, medium or low levels are achieved. For instance, password-based credentials have only one *something you know* factor, whereas PKI credentials stored on smart cards have two factors: *something you have* (the certificate on a secure device) and *something you know* (the PIN required to use it). In these terms, greater security usually means reduced usability and greater total cost.

A more modern authentication strategy uses different security layers throughout the user's interaction with the system and requires different additional authentication factors as needed. For instance, users authenticate in web applications with a password (*something you know*) and are only prompted for a code they receive by SMS in their

mobiles (*something you have*) for making sensitive accesses. This strategy can be strengthened with additional factors such as behavioral biometrics (*something you are*) and user context information (*something you do*) to provide greater levels of security while maintaining ease of use.

The combination of multiple factors, including observing the user context, helps to detect and mitigate possible risks. For example, the user accessing from an unknown device, impossible changes in location between two consecutive accesses and keystroke patterns that differ from the user's, which may indicate fraudulent use of the device or an automated attack, are all detected. In this case, the adaptive authentication system responds to the anomalous situation that suggests a risk of identity theft by increasing the security requirements and requesting a new authentication factor that the user must present to gain access. This adaptive process is also known as risk-based or contextual authentication.

Increasing security, maximizing usability and reducing the cost of authentication

Based on the combination of factors, the context and a risk analysis, Safelayer's TrustedX Adaptive Authentication provides the following key characteristics and properties:

- **Configurable first line of authentication.** Serves as the start of the authentication process. Usually a credential based on a something you know factor (user password) that can be validated by the system via a connection with a corporate repository (AD/LDAP, etc.) or validated externally by delegation using a plug-in.
- **Context capture and analysis.** Based on policies that determine what context information (device, location, time range, frequencies and correlations) are processed to determine the authentication's level of risk. The capture of this context information is controlled exclusively from the server using Web mechanisms (HTML and JavaScript).
- **Behavioral biometrics.** Transparent to the user. While the user types in their username and password, behavioral biometric traits are captured and processed by the server to determine if they match the keystroke pattern previously registered by the user. This process is also carried out exclusively using Web mechanisms.
- **Trusted devices.** The user can explicitly confirm that a device is personal and trusted so that the device becomes a something you have factor. TrustedX implements a one-time double cookie protocol that helps both in the complex identification of the device, in line with the US Federal Financial Institutions Examination Council's (FFIEC) guide, and in safeguarding against pharming attacks.
- **Intuitive server authentication.** In most cases, the average user lacking a technical background is unable to determine if the connection is secure and performed with the authentic server. The option for users to customize the server interface helps them to recognize it and, therefore, safeguards against phishing attacks because it stops users from submitting their credentials when they do not see the image they set.
- **Configurable second line of authentication.** Executed according to the required adaptive policy, the result of the context analysis and/or the behavioral biometrics. As with the first line, the second line can be performed by the system via a connection with a corporate authentication server that is already deployed (via RADIUS) or via external delegation through the use of plug-ins.

- **Start of unique session.** Single sign-on (SSO) is based on i) the NIST levels of assurance and ii) the accumulation of successfully met factors. This allows deploying access control policies that can be adapted to the user context and thereby maximize usability and security at the same time.
- **Events and intelligence.** The system generates events of any authentication activity that manages: authentication lines, factor processing, capture and context analysis, etc. These events can be centrally analyzed and audited in the graphical console. They can also be sent to an external intelligence system that can use the information to generate correlations and advanced security reports (e.g., for measuring compliance with regulations) and even be integrated with external risk management sources.
- **Direct integration using web technologies (HTML and JavaScript) and RESTful APIs.** OAuth 2.O and SAML 2.0 standards are supported to comply with the Authorization Server and Identity Provider roles. Connectors can be used to integrate adaptive authentication into access control systems such as CAS, IBM Security Access Manager and CA SiteMinder.
- **Adoption of new authentication mechanisms.** Designed for extending, via plug-ins, any current or future method for first- or second-line authentication, e.g., PKI, OTP tokens, out-of-band OTP (SMS, e-mail), etc.
- **Recommendations, guides and regulations.** All the main authentication principles are observed, including the NIST 800-63-1 and ITU-T X.1254/ISO/IEC 2911 guides, the Spanish National Security Framework (Esquema Nacional de Seguridad, ENS), the FFIEC's Authentication in an Internet Banking Environment and other sources including the Cloud Security Alliance (CSA).

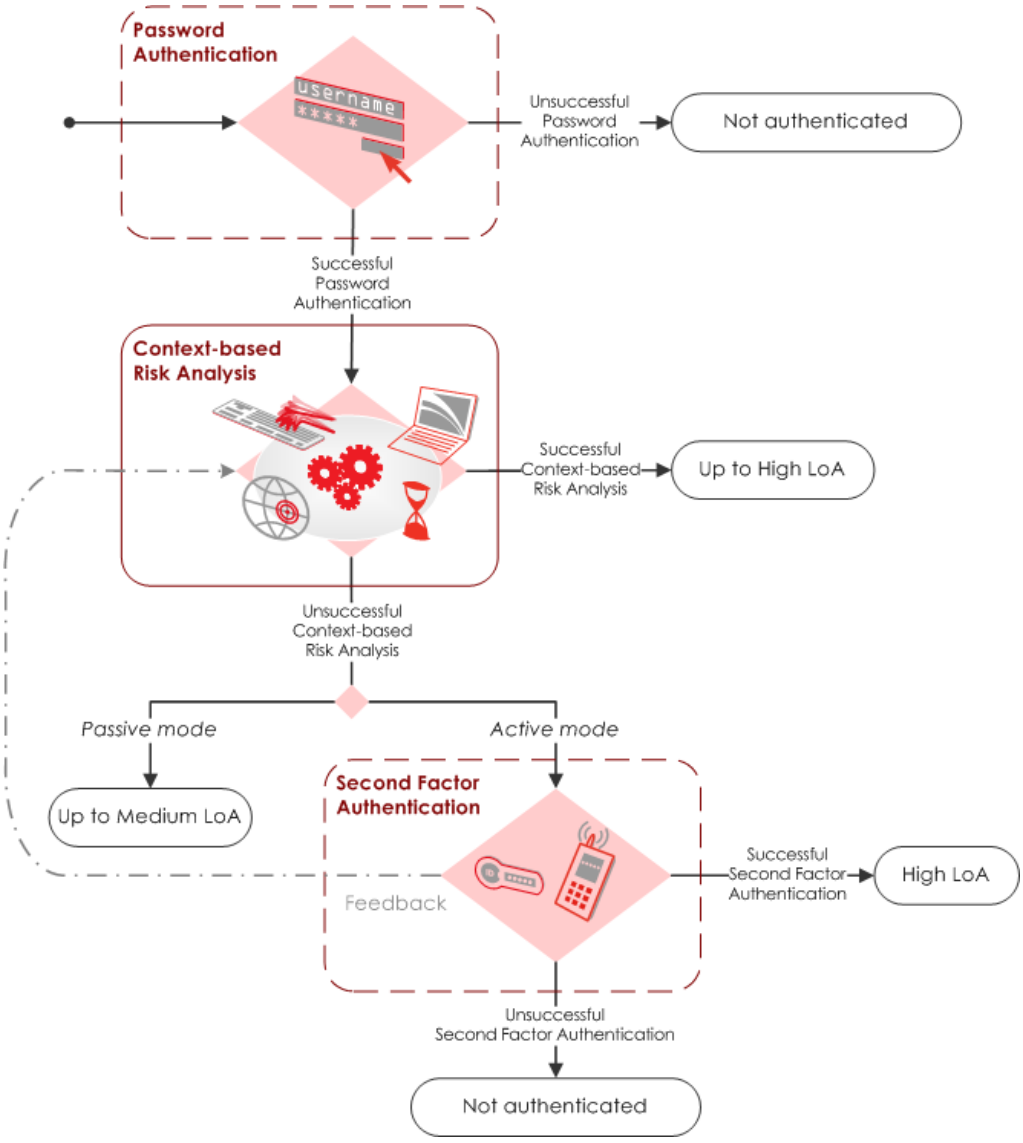

Figure: Adaptive Authentication phases

Use scenarios

TrustedX Adaptive Authentication is a technological component aimed essentially at the world of the Web in which cloud, mobility and social technologies are gaining ground. These technologies are already being used across the ICT ecosystem by all user communities: employees in fixed and mobile locations with access to in-house and cloud applications, consumers increasingly accustomed to e-commerce, government departments aiming to improve the services offered to citizens, etc. The common nexus between all these examples is the tendency towards mobility, consuming services in the cloud and the integration of social networks in all activities. For instance, if employees are already connected to their Facebook or Google accounts, the company can give them transparent access to the corporate calendar from user applications run on their usual devices.

Thanks to the widespread use of Web standards and technologies, it is possible to create a straightforward and uniform user experience that is independent of i) the device being used (desktop, tablet, smartphone, smart TV, video console, etc.), of ii) the application being accessed (an in-house, cloud-hosted or private application) and of iii) which of the multiple identities possessed is being used (corporate or social).

TrustedX uses policies to act as a referee and adapt the security level of each authentication to the level required according to the scenario based on the risk assessment and requests additional factors when required. TrustedX creates an SSO Web experience based on the risk for any device and application environment that supports the Web standards. In particular, the following characteristics are worth highlighting:

- **Cloud access management and SSO.** Thanks to the incorporation of the SAML 2.0 standard, organizations can authenticate their users that connect to business application providers in the cloud such as Salesforce, Google, etc.
- **Mobile awareness.** All current smartphone and tablets have browsers that support the Web standards. These systems also natively have engines for integrating Web technologies in native applications. In mobile environments, certain peculiarities and restrictions need to be taken into account. For instance, where capturing typing speed is not an ideal factor owing to the difficultly involved in entering passwords via a touch screen, this factor needs to be replaced with biometrics based on the recognition of user gestures and movements**.**

TrustedX's Web authentication is horizontal and can be deployed in any environment: in any company or corporation, in government and in service portals providing value to users (employees, partners, citizens and consumers) via the Web. Today, adding value largely entails integrating other cloud services, enabling convenient access independent of device and taking advantage of the boom in social networks. However, this integration must always be performed under the maximum security guarantees while aiming to provide users with best access experience—a requirement for keeping them.