nevisAuth – End-to-End Encryption

Benefits

End-to-end encryption: WhatsApp and Viber have it, Facebook does it; soon Google as well. And NEVIS too supports this feature, by encrypting user login data on its way from the user's device to the server. No third party is able to read the secret credentials that move between the two communicating parties. This

- **prevents potential eavesdroppers from accessing confidential data**, and
- **increases your system's security**, by
- **strengthening its protection against attacks and identity theft.**

What is it about?

End-to-end encryption is a mode of communication where only the communicating parties can read the messages, while any possible intermediary, malevolent or benevolent, cannot. The content is encrypted by means of a special encryption algorithm. Only the sender and the receiver of the data have the keys to decipher it.

Within NEVIS, end-to-end encryption comes as "form encryption". It supports the encryption of the user name, password or any other data entered by the user in a login form. The feature thus protects user credentials on their way from the user to the authentication server in the back end. It also prevents plain text passwords from accidentally ending up in a log file during their transfer from client to server.

Thus, this feature secures your confidential information against attacks from third parties, especially against passive attacks, where someone eavesdrops on and monitors your system to gain information. With end-to-end or form encryption, no one can read your secret data anymore. Not even nevisProxy is able to encipher the encrypted user passwords!

Let's explain why this is important. Suppose a user wants to access a business application in a typical NEVIS setup without form encryption. First, the user's client PC or mobile device connects to nevisProxy. The proxy server stands in between the client device and the business application. It controls user access data and protects your system against internal and external threats.

During the login process, the user sends his credentials to the proxy server over a secure connection. On its turn, the proxy forwards user name and password to nevisAuth, which is in charge of the user authentication. If the user's login data is not encrypted, the proxy is able to read the user name and password when submitting the data to nevisAuth. It possibly might even happen that the plain and un-protected user credentials are stored in a log file.

The above situation constitutes a potential security threat. To better secure the confidential user data, NEVIS introduces the encryption of the user data in a login form. The encryption functionality is incorporated in the HTML-based login page. It is triggered as soon as the user opens the page.

Main features

- Prevents the system from storing plain user credentials in a log file
- Provides protection against passive security attacks such as eavesdropping
- Encrypts each user credential independently to increase security
- Performs encryption automatically in the background without impacting the user-friendliness or accessibility
- Allows for a flexible size/strength of the encryption keys to suit your security needs
- Offers symmetric and asymmetric encryption at the same time, thus combining the advantages of the two encryption techniques. (Symmetric encryption means using the same key to en- and decrypt. Asymmetric encryption takes place when you have one key for encryption and another for decryption.)
- Currently supports the AES encryption algorithm in combination with RSA public and private keys

Switzerland ▪ AdNovum Informatik AG ▪ Roentgenstrasse 22 ▪ 8005 Zurich ▪ Switzerland ▪ +41 44 272 6111 ▪ info@nevis-security.ch ▪ www.nevis-security.ch
Singapore ▪ AdNovum Singapore Pte. Ltd. ▪ 3 Shenton Way ▪ #23-03 Shenton House ▪ Singapore 068805 ▪ +65 6536 0668 ▪ info@adnovum.sg ▪ www.nevis-security.sg
Germany ▪ NEVIS Office Germany ▪ Hubenstein 11 ▪ 84416 Taufkirchen ▪ Germany ▪ +49 8084 41 33 10 ▪ info@nevis-security.de ▪ www.nevis-security.de

Architecture

Figure 1 compares the protection of user credentials with and without encryption. In both cases, the system uses the secure Hypertext Transfer Protocol (HTTPS) and the Transport Layer Security protocol (TLS) to transfer user login data from the client to the nevisProxy server. So, the communication takes place in a secure tunnel (no.1 in the figure).
However, when the credentials are within the proxy, there is no secure tunnel anymore.

Without encryption, the user name and password are relatively unprotected and become vulnerable for attacks (2). If you do encrypt the user credentials, though, the data will be protected during the entire transfer from client device to authentication server (3). It is not until the authentication that the credentials are deciphered and become readable (4).

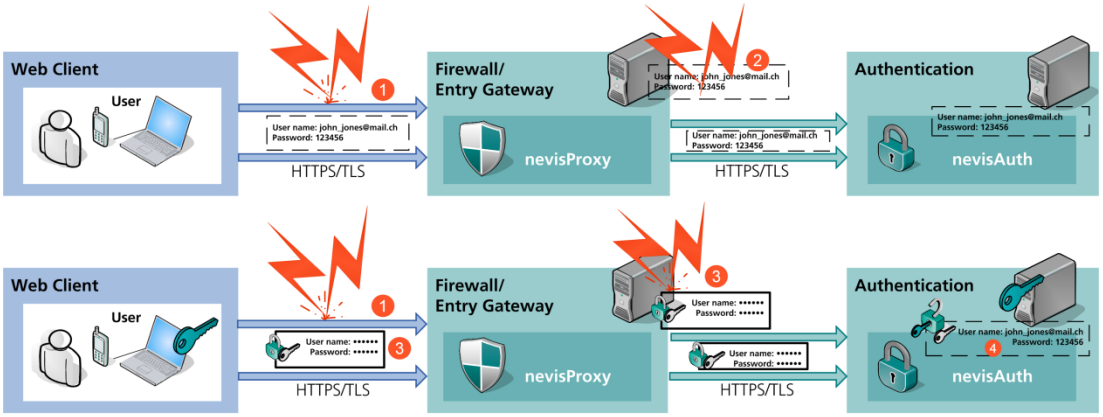

Figure 1 Architecture overview

Switzerland ▪ AdNovum Informatik AG ▪ Roentgenstrasse 22 ▪ 8005 Zurich ▪ Switzerland ▪ +41 44 272 6111 ▪ info@nevis-security.ch ▪ www.nevis-security.ch
Singapore ▪ AdNovum Singapore Pte. Ltd. ▪ 3 Shenton Way ▪ #23-03 Shenton House ▪ Singapore 068805 ▪ +65 6536 0668 ▪ info@adnovum.sg ▪ www.nevis-security.sg
Germany ▪ NEVIS Office Germany ▪ Hubenstein 11 ▪ 84416 Taufkirchen ▪ Germany ▪ +49 8084 41 33 10 ▪ info@nevis-security.de ▪ www.nevis-security.de