CYBRUS

Security overview

Overview

CYBRUS was developed for companies with highly confidential communications. The secure system ensures that personal data, history, files and voice and video calls and group calls are encrypted end-to-end. Data is encrypted both in transmission and when stored on devices and on servers. This protects data from unauthorized access and leaks. The core feature of CYBRUS security system is that only the users have access to the keys for decrypting their data.

All types of data in CYBRUS are encrypted with strong encryption algorithms such as AES-256 and RSA-3072. Diffie-Hellman secure key exchange and Transport Layer Security create additional protection levels.

Encryption in CYBRUS is modular, allowing companies to protect communications with third-party encryption technologies that meet corporate safety regulations.

CYBRUS users own their encryption keys, and the only one who may have access to them is the system administrator, if administrator control is required for compliance. Only the user and authorized contacts can decrypt shared messages and files. The only way to get access to information is to know the exact secret phrase. Brute force are unable to break the system due to strong encryption. The influence of human factor is minimized, and system administrators control the way users authorize, interact, share data.

CYBRUS encrypts everything:

- Personal data
- Messages
- Files of all types
- Voice and video calls
- Voice and video conferences

The data in transit, on devices and on the server is impossible to decrypt due to system architecture and key management scheme.

Communication channels and network traffic

Transport Layer Security (TLS) protects all client-server-client connections in CYBRUS. End-to-end encrypted data is transmitted through secure channels so that only authorized users with necessary permissions can decrypt it. Data is encrypted on devices, and it is encrypted when it gets to the server. CYBRUS protects all types of transmitted data with special methods.

Protection of text messages and files

- Text messages and files are packed in encrypted containers before they are sent to the receiver. Only the sender and the receiver of the data can decrypt these containers.
- One-time asymmetric encryption keys are created using the public encryption key of the receiver.

Protection of voice and video calls

- Audio and video calls are performed by data streaming that is encrypted before transmission at the network traffic level with the keys that are known only to the information sender and receiver.
- Session encryption keys are generated for voice and video calls and a secret token is used for every conversation.

CYBRUS server

Data is transmitted to CYBRUS server encrypted and is stored there encrypted:

- All user information, including history and files, is stored on servers encrypted with the public key infrastructure.
- Only the users who own the keys can access this data. Access of third parties is impossible, unless the administrator of the corporate communication system is empowered to manage the keys of the team.

For file transfers and audio and video conversations, the technology of network tunnels is applied that allows to encapsulate the packets of the applied network traffic inside the transport network traffic packets. The network tunnel acts as an intermediary in the transmission of user traffic between CYBRUS client applications.

Network tunnels of CYBRUS servers are used as:

- The intermediate network node through which CYBRUS users exchange data when they cannot establish the direct communication channel.
- The replicating network node that sends received network packets to multiple network nodes participating in the tunnel, for example, during multiuser audio and video calls.

Encryption at all nodes

Data encryption in CYBRUS is performed on desktop and mobile devices, and encryption keys are known only to data owner. Data is transmitted encrypted to the web and to the server, and only the user and authorized contacts can decrypt it.

Strong cryptographic algorithms protect data:

- AES-256 is used for symmetric encryption;
- RSA-3072 is used for asymmetric encryption.

The original message is encrypted symmetrically (AES-256) using a one-time encryption key. The one-time encryption key is then encrypted asymmetrically (RSA) using the sender’s and the receivers’ public keys. Therefore, only the sender and the receivers can decrypt the one-time key with their private keys and then decrypt the message.

All messages are sent to the server and stored there in secure CYBRUS containers that include symmetric and asymmetric encryption blocks and are developed using the principle similar to S/MIME e-mail protection algorithm.

- Shared data is encrypted with the symmetric algorithm using a one-time key of the container symmetric encryption;
- For CYBRUS ID of the sender, a one-time symmetric encryption key is encrypted with the asymmetric algorithm using the public key of the sender
- For CYBRUS ID of the recipient, a one-time symmetric encryption key is encrypted with the asymmetric algorithm using the public key of the receiver.

Secure data transmission

CYBRUS protects all transmitted data from interceptions and eavesdropping. Along with transferring data in secured containers, CYBRUS additionally protects data transmission channels.

Two types of channels are used in CYBRUS:

- **Client-server connections** – basic connection to CYBRUS server, enabling all client-server interactions;
- **Direct user-to-user channels** for voice and video transmission.

Secure data storage

CYBRUS stores all user data encrypted both on devices and on the server. Chat history, files and account information are stored in local encrypted databases on users’ devices.

Database encryption master key is generated when a database is created and is stored only on the device. The key is stored encrypted; and to decrypt it, the secret phrase and the private key of the user are necessary. Each part of the user profile database is encrypted with the AES-256 symmetric encryption algorithm using a one-time key.

CYBRUS ensures security of transmitted and stored user data, both account information and files. Files are stored encrypted on devices which makes them inaccessible to third parties even if devices are compromised. On every device, users can always check whether their data storage is encrypted. For working with encrypted files on user devices, CYBRUS virtual drives are used. These drives decrypt files when users work with them on devices.