IT-Architektur state-of-the-art

Vorhandene Lösungen wie Jitsi oder BBB arbeiten teilweise auf Basis überholter XMPP-Technologie (einem erprobten, aber ebenso uralten System zur Chat- und Videokommunikation) und sind auch technologisch nicht auf Skalierbarkeit und Leistungsfähigkeit ausgelegt. Sie erfüllen nicht die modernen Anforderungen an Sicherheit oder bieten nicht die notwendige Architektur für den aus heutiger Sicht gewünschten Funktionsreichtum.

Für OpenTalk wurde eine von Grund auf neue Architektur entwickelt, die den heutigen Stand von Sicherheit, Authentifizierung, Verschlüsselung, Skalierbarkeit und Flexibilität abbildet – sprich: **Eine state-of-the-art-Architektur aus dem 2020er-Jahrzehnt.**

Ein zentraler „**Controller**“ regelt Anmeldung und Authentifizierung aller Nutzer und prüft deren Zugriffsberechtigung. Nach erfolgreicher initialer Authentifizierung erfolgt die weitere Autorisierungsprüfung des Nutzers bei jedem Zugriff erneut auf Basis eines **OpenID-Connect-Tokens**: sei es der Abruf von Videostreams aus seiner laufenden Konferenz oder die Übermittlung von notwendigen Steuerinformationen, Chat-Nachrichten, Abstimmungsteilnahmen oder allen anderen Funktionen im Rahmen seiner Teilnahme. Nichts findet ohne Token-basierter Berechtigungsprüfung statt.

Erst nach seiner Anmeldung wird der teilnehmende Client intern an die spezifische Video-Bridge weitergeleitet, auf dem die jeweilige Konferenz durchgeführt wird. Diese erhält damit stets **nur autorisierte RTC-Verbindungen,** so dass von vornherein sichergestellt werden kann, dass nur Audio-/Video-Daten verbreitet werden, die vertrauenswürdig und autorisiert sind. Die internen Systeme können so vor **unbefugten Zugriffen als auch Denial-of-Service-Angriffen** durch ein mehrstufiges System („Zwiebelschalen“) geschützt und gehärtet werden.

Steuerbefehle, wie z.B. Mikrofon an/aus und Kamera an/aus, werden vom Nutzer-Client zunächst autorisiert an den Controller gesendet und dann von diesem Mithilfe eines sog. Messages-Brokers an die zuständige Video-Bridge weitergeleitet. Der verwendete Message-Broker ist auf hochperformante Skalierung ausgelegt und kann auch die bei Konferenzen mit extrem hohen Teilnehmerzahlen auftreten Nachrichtenmengen simultan verarbeiten.

Für jede gestartete Konferenz wird dabei eine eigene **Videobridge-Instanz in einem Container** gestartet, die alle sensiblen Daten lokal im Container verarbeitet. Dies schützt vor unbefugtem Zugriff aus anderen Installationen/Konferenzen und stellt durch den Abbau des Konferenz-Containers zugleich sicher, dass nach Konferenzende **alle zur Laufzeit gespeicherten Daten sicher und zuverlässig wieder gelöscht** werden.

Und auch die Qualität der Konferenz ist sichergestellt: Moderne Standards und lizenzfreie Open Source-Videocodecs wie VP8, VP9 oder AV1 sind effizient im Datenverbrauch und ermöglichen **gute, latenzfreie Konferenzen auch bei geringen oder verändernden Bandbreiten**. Die Verbindungsqualität wird fortlaufend überwacht und die Verbindungsparameter dynamisch abhängig von der verfügbaren Bandbreite angepasst.

Das **Frontend** bzw. die Benutzerschnittstelle von OpenTalk wird mithilfe von **React** bereitgestellt, einer effizienten JavaScript-Bibliothek, die mit hierarchischen Komponenten arbeitet. Zur Absicherung gegen Cross-Site-Scripting-Angriffe (XSS) maskiert React automatisch alle durch Benutzer eingegebenen HTML-Daten. Die Bibliothek **Redux** sorgt dafür, dass Laufzeitdaten nur lokal gespeichert werden, sofern sie nicht von anderen Benutzern benötigt werden und erlaubt somit einen datensparsamen Betrieb.

Sicherheitsexperten wissen die für OpenTalk genutzte und als besonders sicher geltende **Programmiersprache Rust** zu schätzen: Sie ist sicher und für die Verarbeitung vieler paralleler Aufgaben geeignet, wie sie bei Videokonferenzen mit sehr hohen Teilnehmerzahlen notwendig sind. Der Rust-Compiler erkennt Fehler in der Programmierung, die zu bösartigen Speicherzugriffen und Pufferüberläufen führen können und bietet bereits von Grund auf Schutz vor modernen Angriffsvektoren.

Die Bereitstellung als Open Source Lösung erlaubt jederzeit eine Auditierung der Lösung, um Sicherheitsfunktionen bewerten zu können. Zudem ist eine BSI-Zertifizierung der Lösung vorgesehen, ein wichtiges Merkmal, welche Lösungen wie Zoom oder MS Teams nicht bieten und nicht bieten werden.

OpenTalk ist in konsequentem Pair-Programming und regelmäßigen Code-Reviews erstellt worden, um einen **gleichbleibend hohen Code-Standard** zu gewährleisten.

Kontakt

OpenTalk GmbH
Schwedter Str. 9a
10119 Berlin

Tel: +49 (0)30 40 50 51-0
mail@opentalk.eu
https://opentalk.eu