How to secure modern business and governmental communication

Secrets and national security in video conferences

Transport Encryption and Video Conferencing

Just Sound & Audio?

- Video
- Audio
- Chat

- Files
- Whiteboard
- Minutes
- Votes and Polls

Transport Encryption and Video Conferencing

Who has the data?

- Browsers typically send data as a WebRTC stream
    - Fat clients can use proprietary protocols
- This data can be transport encrypted using TLS
- Since peer-to-peer doesn't scale well, data typically runs through a central videobridge
- At that endpoint, however, TLS is terminated
- Whoever has the bridge, has the data

What is possible today...

AI und video data

- Every modern phone can do Speech2Text
- Complete text logging and summary
- Image/Person/Face recognition
- Emotion detection
- Translation of sign language into text

WHO talks HOW with WHOM about WHAT.

Well – then just do End-to-End-encryption!!!

End-to-end-encryption

Why video conferences struggle with this

- E2EE with asymmetric keys scales poorly with a high number of participants
- Number of keys is „n*(n-1) / 2“
- 100 participants = ~5000 keys

- A symmetric session key?
- How do we protect both historical and future data of the conference?

- Participants join, participants leave
- Permanent key rollover
- For a conference with real-time-streaming

What’s possible today..

E2EE in commercial solutions

- Some claim to have E2EE
- But E2EE only for a small group of participants?

- The implementations are not open source
- Quality and potential backdoors might not be verifiable
- Zoom already lied once https://news.ycombinator.com/item?id=22757697

- Zoom has only an EAL2 certification
- And only for the client, not for the backend

- US based videobridges are always involved
- Either way, certain metdadata („who“) remains exposed

Well…

August 2023: Zoom changes its T&C

New terms and conditions from Zoom are causing a stir:

> *10.4: You agree to grant and hereby grant Zoom a perpetual, worldwide, non-exclusive, royalty-free, sublicensable, and transferable license and all other rights required or necessary to redistribute, publish, import, access, use, store, transmit, review, disclose, preserve, extract, modify, reproduce, share, use, display, copy, distribute, translate, transcribe, create derivative works, and process Customer Content and to perform all acts with respect to the Customer Content, including AI and ML training and testing.*

Zoom COO Aparna Bawa retracts it (https://news.ycombinator.com/item?id=37034980), and the T&C were changed again:

> *We currently do not use audio, video or chat content to train AI models and we would not do so without customer consent.*

Well…

- Which content is used instead?
- Currently?
- Consent?

What do we conclude from this?

What is possible?

What do we conclude from this?

Where is the interest?

What do we conclude from this?

It could have worked.

What do we conclude from this?

Nice try.

What do we conclude from this?

Let’s see what’s possible tomorrow.

Digital sovereignity = national security

Communication must not only be secure, but also available!

- Geographically/physically autonomously available
- Infrastructure, Hardware and also Software!
- Free from political influence ("MAGA! Old Europe!")
- Short distances, own data centers, full control

- No country can win a conflict without the Internet
- It used to be the oil pipeline, now it's the data cable
- (Ooops. Didn't that just happen on October 8th near Sweden/Estonia?)

- Would we survive a conflict "on the wrong side"?
- Friend or foe?
- Yes, I have an issue when vital services or systems of national security rely on US cloud-based or foreign infrastructure, services or software

Let’s take a look...

So where do we stand today?

Status quo: cloud based video conferences

True performance and stability only as SaaS?

- Cloud services like Zoom, Teams & Webex dominate
- Stability and performance are on point
- Device support beyond Microsoft varies

- Services are SaaS, some with vendor lock-in
- Data processing in foreign countries & data centers
- Code and security are not transparent

- Services are oriented towards business meetings
- No industry-specific supporting features
- Not designed for politics or education

Status quo: OnPrem-Videokonferenzen OSS

Digital sovereignity only with open source?

- Jitsi and BBB are the most well-known representatives
- Open-source solution for self-hosting
- Limited feature set and usability

- Long-standing, deserving veterans
- Software stack + architecture partly more than 10 years old
- Doesn't meet today's IT design goals (security/scalability)

- Not explicitly developed for video conferences (XMPP)
- True (cloud) scalability not provided
- Little to no API for integration and management

Sorry. I forgot to introduce myself... :-)

Experts in secure and free communication.

For 30 years.

- 100% subsidiary of Heinlein Support GmbH
- Linux Consulting and Linux Academy in Berlin
- We have our own ISPs and data centers in Berlin

- Owner of award-winning mailservice "mailbox.org"
- Operator of some public/gov video conference services in Germany

- Our DNA: Data protection and digital sovereignty
- Expertise from a team of ~75 employees
- Thorough open source and server experts

- https://www.heinlein-support.de
- https://opentalk.eu

We need a state-of-the-art video conferencing solution for the year 2022.

What would be „state-of-the-art“?

- Open Source
- Secure programming (Rust!)
- Container-based
- Scalable (Kubernetes)
- Zero-Trust concept
- User-friendly for young and old
- Features also for education and public sector
- Approved for classified secret communication (CC-EAL4)

So… we developed exactly that.

✓ Everything „from scratch“

✓ Clean concepts, clean architecture

✓ Published as Open Source (EUPL)

✓ 3 years of developement time, 20 developers

Video conferences „state of the art“

Video conferences reimagined and fully realized.

- Engages users and focuses on comfort
- Tailored for specific audiences and child-friendly (elementary school!)
- Optimizes workflows for non-tech-savvy users

- Redefines the function of a video conference
- Supports moderators, speakers, and teachers
- Capable of hosting plenary and panel discussions

- Powerful features with unique selling points
- Accessible via browser, dedicated apps & dial-in

- "Video conferences are more than just a sales meeting."
- Our goal: Redefine "state-of-the-art video conferences"

Technology „state of the art“

On-premises.
Scalable.
Open Source.

- Installable on-premises or SaaS from GER/Europe
- Video conferencing system also for >500,000 users
- High-performing, scalable, secure & stable

- Open Source IT architecture and today's security
- Quality and scale-out of cloud-based solutions
- Optimal successor to Jitsi, BBB, Nextcloud-Talk

- Integrable into (learning) platforms, governmental data networks, telephone systems, existing provider products, and more

- Zero-Trust concepts and video bridges in selectable IT security zones for conferences

Thank you for your attention.

Want to see and test OpenTalk live?
Want to join the community?

Feel free to do so.
Start with a free trial:
https://register.opentalk.eu/en

Opentalk

Let’s talk about it. ☎

Peer Heinlein

Tel: +49 30 40 50 51-42
p.heinlein@opentalk.eu

OpenTalk GmbH
Schwedter Straße 9a | 10119 Berlin
https://opentalk.eu
https://demo.opentalk.eu