



Zoom Security Issues

Zoom Bombing

Zoom meeting ID is easily guessed

Leaks of email addresses and profile photos

Zoom automatically organizes participants by email domain in a public folder

Meeting chats don't stay private

1-to-1 private chats are sent to the host with a summary post-meeting

Windows password stealing

Chat functions vulnerable to attack through web-links and UNC paths

Malware-like behavior on Macs

Hacker-like methods used to bypass normal macOS security precautions

Zoom meeting recordings can be found online

Meeting recordings and save-file names are easily identified through meeting IDs

Zoom meeting ID is easy to guess

Randomly generated ID numbers between 9 and 11 digits are easily predictable

Zoom uses their own version of SRTP

Zoom SRTP uses AES-ECB mode, not adopted in SRTP standard

Zoom encryption key is sent to Beijing server

AES-128 key for conference encryption/decryption was sent to Zoom servers outside of the user region

Meeting room vulnerability

Video/audio streams to participants in "waiting rooms"



Solution: IPVideoTalk



The 3-digit checksum reduces the random guessing of meeting IDs



Privacy for meeting participants' email addresses, profile photos, etc.



Privacy for participants' 1:1 chats during and after the meeting



Little vulnerability to attack through the meeting chat functions



Using standard web browsers minimizes risk of malware-like behavior



Meeting recordings and filenames cannot be found online



Random numerical meeting IDs are used to verify validity with a password option



IPVideoTalk uses standard SRTP modes, AES-CTR mode for security



Session encryption: each uses an independent encryption key. IPVideoTalk uses servers in-region



Password option for secure meetings