



Welcome to

Video Conferencing - trust, security and settings

2020

Henrik Kramselund Jereminsen hkj@zencurity.com @kramse  

Slides are available as PDF, kramse@Github
video-conferencing.tex in the repo security-courses

Goal for today



This presentation will be focused on video conferencing security.

The picture illustrates working together but in these times,
we cannot shake hands and meet in the physical world as we used to.

We need video conferencing.

... but what about security

Paranoia defined



par·a·noi·a

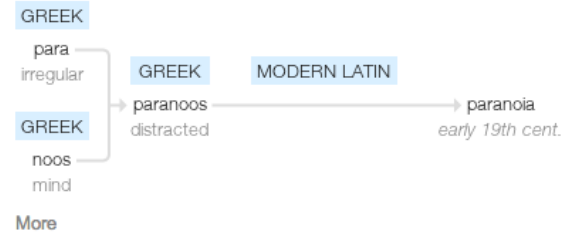
/ˌpærəˈnoɪə/ ⓘ

noun

noun: **paranoia**

1. a mental condition characterized by delusions of persecution, unwarranted jealousy, or exaggerated self-importance, typically elaborated into an organized system. It may be an aspect of chronic personality disorder, of drug abuse, or of a serious condition such as schizophrenia in which the person loses touch with reality.
synonyms: [persecution complex](#), [delusions](#), [obsession](#), [psychosis](#) [More](#)
- suspicion and mistrust of people or their actions without evidence or justification.
"the global paranoia about hackers and viruses"

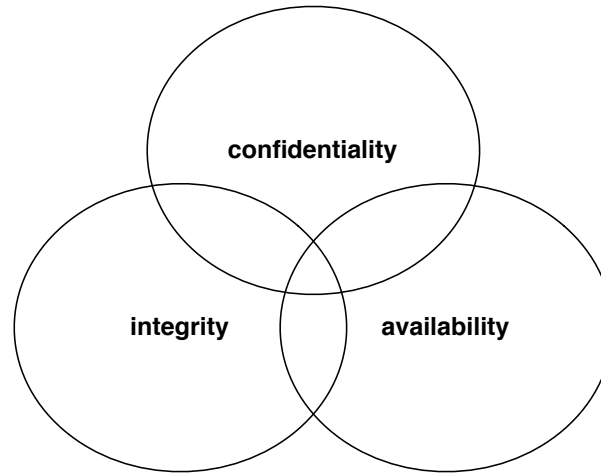
Origin



Source: old google paranoia definition

People WILL try to abuse Video Conferencing

Confidentiality Integrity Availability



We want to protect something

Confidentiality - data is kept confidential, secrets are secrets

Integrity - data is not subjected to unauthorized changes

Availability - data and systems are available for authorized users when they need it

All software has flaws



The Internet Worm 2. nov 1988

Exploited the following vulnerabilities

- buffer overflow in fingerd - VAX code
- Sendmail - DEBUG functionality
- Trust between systems: rsh, rexec, ...
- Bad passwords

Contained camouflage!

- Program name set to 'sh'
- Used fork() to switch PID regularly
- Password cracking using intern list of 432 words and /usr/dict/words
- Found systems to infect in /etc/hosts.equiv, .rhosts, .forward, netstat ...

Made by Robert T. Morris, Jr.

Attacking Video Conferencing



- Sniffing and eavesdropping
- Zoom bombing, joining unauthorized, causing chaos
- Encryption: even if you use AES, do you use it correctly
- Software security: All video conferencing has had security vulnerabilities

Crypto slides here!



Imagine a long presentation inserted here showing:

- HTTPS and Transport Layer Security (TLS)
https://en.wikipedia.org/wiki/Transport_Layer_Security 20 years of security problems
- Elliptic Curve Encryption
https://en.wikipedia.org/wiki/Elliptic-curve_cryptography
- Diffie-Hellman
https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
- Multiparty Crypto is hard https://en.wikipedia.org/wiki/Secure_multi-party_computation
- Recommend *Serious Cryptography A Practical Introduction to Modern Encryption* by Jean-Philippe Aumasson November 2017, 312 pp. ISBN-13: 978-1-59327-826-7
- Stanford Dan Boneh is writing a crypto book <https://crypto.stanford.edu/~dabo/cryptobook/>

Zoom Settings



- Improved a lot during April and May

Problems: Zoom bombing



Problems

- Participants can join, no password, guessable room IDs
- Audio - participants can talk
- Screen sharing - taking over screen

Solutions

- Using passwords for meetings
- Only send link directly to intended participants
- Waiting room - admit people, also have another person monitoring during conference
- Audio - muting
- Screen sharing - security setting, disable - now a default in May 2020

Better team



The company has hired Luta Security, a company specialized in managing sustainable vulnerability disclosure and bug bounty programs.

Luta Security is helmed by cyber-security veteran Katie Moussouris. The Luta Security founder is best known for setting up bug bounty programs for Microsoft, Symantec, and the Pentagon.

Source: *Teleconferencing app Zoom announced today plans to revamp its bug bounty program as part of its long-term plan to improve the security of its service.*

<https://www.zdnet.com/article/zoom-to-revamp-bug-bounty-program-bring-in-more-security-experts/>

- Zoom has hired more team members in Security
- *Zoom Acquires Keybase and Announces Goal of Developing the Most Broadly Used Enterprise End-to-End Encryption Offering*
<https://blog.zoom.us/wordpress/2020/05/07/zoom-acquires-keybase-and-announces-goal-of-developing-the-most-broadly-used-enterprise-end-to-end-encryption-offering/>
- Better Team with focus, will improve Zoom security

My Conclusion on Zoom



Zoom video conferencing is great for teaching, use it myself.



Zoom video conferencing has had issues with encryption so maybe not for the most security critical meetings.

Is Zoom improving, definitely!

- BTW Are mobile phones secure, is calling through the telephone network secure, probably not
- No I dont own shares in Zoom.us

Questions?



Henrik Kramselund Jereminsen hkj@zencurity.com @kramse  

You are always welcome to send me questions later via email

Email: hk@zencurity.dk

Mobile: +45 2026 6000