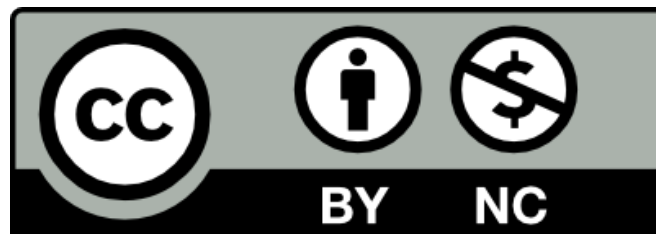


Zoom Security

Steven M. Bellovin

<https://www.cs.columbia.edu/~smb>



Zoom has had Security Problems

- Ability for a website to turn on a user's camera without permission
- Privilege escalation
- (Local) hijack of camera and mic
- Disclosure of hashed Windows password
- More

Zoom has had Privacy Problems

- Scraping Linked-In content
- Revealing email addresses
- Sending data to Facebook
- More

Zoombombing

- Outsiders can crash your meeting (or class)
- Outsiders can display nasty content, annoy folks with chats, scribble on slides, and more

Why?

- Is Zoom incompetent?
- Are they evil?
- Or are there deeper issues?

Security Issues

- Some (like the hashed password disclosure) look to be ordinary bugs
- They may need to step up their software quality control, but that's not unusual

Privacy Issues

- Zoom was aimed at enterprise communications, not personal interactions or classroom settings
- At work, it's *convenient* to have your coworkers listed as contacts
- At work, it's *convenient* to have a constant meeting ID

Most of the privacy issues (and Zoombombing) have arisen because Zoom is being used for different purposes than it was intended for. (Imagine employees Zoombombing the CEO meeting with the Board...)

But...

- Some of the problems, e.g., the ability for a website to turn on a camera without permission, suggest a cavalier attitude towards security
- Zoom viewed their change as “a legitimate solution to a poor user experience problem.”
- I worry that they don’t have a deep understanding of security and privacy

Improvement

- Zoom has been very forthright, acknowledging problems and providing quick patches
- They're going to do a thorough review, with outside experts
- What they really need: a CSO and a CPO with real power
- Will they hire such people and empower them?