Is Zoom doomed?

SHAHRIAR RAHMAN

Corona pandemic has battered all economic activities globally. The crisis that triggered a worldwide economic meltdown has been a reason for the stagnation of everyday lives in more than 180 countries of the world. In an unprecedented turn of events, people are now resorting to conducting any and every non-essential work from home. This has given the rise to remote workforce interaction tools including video conferencing service. Zoom, a videoconferencing app, is probably that has made the most out of this crisis. Its popularity has skyrocketed in just a few months resulting in doubling its stock price. But its new-found popularity was marred recently as the service came under scrutiny for security and privacy issues.

Several incidences of 'Zoom-bombing', as many IT researchers coined it, has been reported globally where attackers hijacked the video=feed of their target. According to The Intercept, Zoom doesn't have any end-to-end encryption in their call conferencing system as they claimed before which might live the user's PC in a vulnerable state. Moreover, the researcher found that the videoconferencing app never mentioned to their users that it clandestinely installed webservers on Apple devices. To make things even worse, Zoom failed to remove these web-servers even after the end-user uninstalled the app.

Interestingly, according to researches carried out by the University of Toronto, Zoom has three subsidiaries in China from where it sometimes issues its encryption keys even if the participants are from the west. Generally, the server closest to participants is the one that issues the encryption key, so it is certainly baffling why Zoom issued encryption keys from servers halfway across the world when it had more servers nearby. These revelations have prompted the FBI to issue a warning of possible privacy and security breach if a user is opting for Zoom when they are working from home during the Corona Crisis. Apple, SpaceX, NASA and several other organisations have already issued ban on using Zoom from their work PC or any other work-related activities.

WHAT'S THE PROBLEM?

So, what are those exploits? From an analysis done by Citizen Lab, there are three exploits that are worth mentioning:

Firstly, the encryption key conundrum. Whenever a call is initiated, the device running the call will fetch for an encryption key. Each of the participants actually shares the same key to encrypt their incoming and outgoing data. These keys are generated and managed by servers known as the 'Key management system'. Zoom has 73 of these servers globally including 5 in China. Usually, a near-by server generates the key of the origination of the call. But there are some instances, where the key was generated from Chinese servers even though the participants were not from China. So, what's wrong with the key generated from a Chinese server? Well, due to the stringent Chinese internet laws, any server in China needs to share every encryption code generated within China needs to be shared with the government rendering that Zoom calls virtually insecure.

Secondly, the AES issue. Advanced Encryption Standard or AES is an encryption standard that is used everywhere to create encryption. Zoom right now uses 128-bit encryption. Don't get me wrong, 128-bit is still pretty secure. It would take a hacker ages even with a supercomputer. But it's not the best encryption out there. Most services now use 256-bit encryption is exponentially harder to crack. Even NSA recommends using 256-bit encryption for sensitive services. Sadly, despite claiming it uses 256-bit encryption, Zoom in reality uses 128-bit encryption.

Lastly, the usage of legacy Electronic Code Book (ECB). ECB is the algorithm that encrypts and decrypts the AES in zoom which has been discarded by most services because of its flaws. During the input, ECB retains the pattern of the message which gives out some details of the packaged data. It's sort of like if you leave a heavy object on a soft carpet. Even after removing the object from the carpet, one can easily assume the size of the object that was kept. This is exactly what happens in case of ECB. It leaves a ghostly shadow of the input data revealing sensitive information to hackers.

WHAT'S ZOOM DOING ABOUT THESE?

In the wake of these allegations, Zoom's Chief Executive Officer Eric Yuan and Chief Product Officer Oded Gal issued a public apology on social media for having fallen short on the security and privacy concerns and misleading everyone about having full-proof end to end security. They even pleaded for 90 days of time to fix all these issues and delivery a full-proof product.

WHAT CAN WE DO NOW?

For the time being, the sensible thing to do is avoid Zoom. There are tonnes of alternative available in the market that you can use for free. So far, Google Hangout and Skype Meet Now is probably the most popular alternative. Google is making its premium features available for now, so you certainly can make the most out of it. If you are into opensource stuff, then you can give 'Jitsi Meet' a try. Cisco Webex and FaceTime are also worth trying. For informal and limited use, you can try Facebook Messenger or WhatsApp web.