ZOOM's ENCRYPTION CONCERNS AND NEED FOR A STRONG LEGAL FRAMEWORK IN INDIA

Harsh Bajpai, Ph.D Candidate, Durham Law School

With the outbreak of coronavirus, video conferencing services have seen a record spike, and platforms such as Zoom, Signal, Microsoft Teams and others are scaling new heights in terms of its userbase. Amidst this, the Ministry of Home Affairs' Cyber Coordination Centre issued an advisory on April 15, 2020, stating that Zoom is not a 'safe platform'. The advisory explicitly rejects the usage of Zoom for government offices/officials for official purposes and lays out specific precautionary measures and guidelines for the usage of the application by private individuals. The advisory points out that there exists a vulnerability/'error' while handling the webcam and microphone on the systems. The attacker can carry out Denial of Service attacks (DoS) by restricting users through passwords and access grant or listen to the content of the meetings. This 'error' or vulnerability is lack of encryption standards, especially in the case of video-based meetings.

According to an April 2020 White Paper[1] by Zoom on its security guide, "Zoom can encrypt all presentation content at the application layer using the Advanced Encryption Standard (AES) 256-bit-algorithm."It further states that AES 256 encryption uses Transport Layer Security (TLS) encryption standard. In-meeting chat messages, shared files and meeting transcripts can be optionally saved to Zoom's cloud servers, where they are stored and encrypted as well. ***However, a security researcher named Jonathan Leitschuh[2] and Citizenlab[3] of the University of Toronto not only found out ambiguities in the Zoom's meaning of the word encryption but also that transfer of encryption keys happens on Chinese servers.*** For better understanding of the level of vulnerability, we should examine the difference between TLS and end-to-end encryption. The encryption that zoom uses to protect meetings is TLS, which is similar to the one that web servers' uses to secure HTTPS [Hypertext Transfer Protocol Secure] websites. For e.g.: the connection between one's web browser and this article is encrypted with TLS standard. This is different from end-to-end encryption. In TLS standard, though, a third party cannot access the Zoom meeting, but Zoom itself can. The mechanism is entirely different in case of WhatsApp which is end-to-end encrypted and thereby cannot have any access to video, audio or textual content shared on its platform. However, since the content shared on Zoom is transferred across Zoom cloud servers, and in order to provide high-resolution video-streaming during video calls, the personal data of the users remains visible on Zoom's endpoints. Thus, Zoom has the technical ability to spy on private video meetings and could be

[1]Zoom Video Communications Pvt. Ltd. – Zoom Security Guide, Retrieved from https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf

[2]Leitschuh, J. (2019, September 25). Zoom Zero Day: 4 Million Webcams & maybe an RCE? Just get them to visit your website! Retrieved from https://medium.com/bugbountywriteup/zoom-zero-day-4-millionwebcams-maybe-an-rce-just-get-them-to-visit-yourwebsite-ac75c83f4ef5

[3]Kenyon M. (2020). Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) on Quick Look at Zoom's Privacy. Retrieved from citizenlab.ca/2020/04/تحرك-بسرعة-واستخدم-تشفيرك-الخاص-نظرة-س/

compelled someday by law enforcement agencies to hand over recordings in response to legal requests.

Now the question which remains unanswered is where are these Zoom cloud servers located. Although Zoom is headquartered in the United States, the application has been developed by three companies based in China, all known as Ruanshi Software and only two of which are owned by Zoom. In a hurry to provide video-conferencing services, Zoom deployed server capacity only in few countries, starting with China. As a result, when numbers spiked, several calls were routed through China, as well as, encryption keys were issued via servers in China. The primary reason is that, as another Zoom document claim that AES-256 encryption is used in Electronic Codebook (ECB) mode. ECB mode is regarded as bad because the input data and the encrypted data is almost similar, which makes it prone to malicious actors. The 2013 Adobe password database leak is a prominent example of ECB mode. Modes other than ECB like GCM, EAX, OCB or SIV result in pseudo-randomness and add an extra layer of misuse resistance, rendering the application secure.

Weak security protocols provide a gold mine for Zoom bombers, phisher men and spies to enter into the video-meetings and collect signals (SIGINT) and human intelligence (HUMINT). Routing through China which does not have data privacy laws of its own, Zoom can be used as a tool to suppress freedom of speech and expression and right to privacy. Zoom has been asked[4] to disclose a transparency report as to the number of government requests for user data; it receives country-wise and compliance rates. However, now Zoom has come with a new version, Zoom5.0[5] with AES 256-bit GCM encryption; and, system-wide enablement to GCM encryption was done on May 30, 2020. Further, to counter routing through Chinese servers, Zoom has established two data centers in India. Hosts can select data center regions at the scheduling level for meetings and webinars. The particular data center will be showcased in the Info icon in the upper left of Zoom Window.

India has primarily been unhindered of crypto wars, however, after the recent attack of Pegasus Malware, our country requires considerable attention to the legal framework around encryption policy. Concerns around foreign compromise of telecommunication infrastructure are not endemic to India. The Internet Engineering Task Force (IETF) debated on updating TLS 1.2, which is a widely used protocol that powers most online encryption, came with a more robust version of TLS 1.3. A similar stance was taken by the Ministry of Electronics and Information Technology (MeitY) in its concept note titled[6] 'TLS 1.3 Implementation (Effects on Encryption

[4]Oribhabor I. &Micek P., Access Now Letter to Zoom (March 18, 2020), "Zoom's Policies Affecting Digital Rights", Retrieved from https://www.accessnow.org/cms/assets/uploads/2020/03/Letter-to-Zoom-.pdf.

[5] Seth H., "Zoom officially rolls out Zoom 5.0 to users", Hindu Business Line, April 30, 2020, Retrieved from https://www.thehindubusinessline.com/info-tech/zoom-officially-rolls-out-zoom-50-to-users/article31469704.ece#

[6]Rathi A. et.al., "Regulating the Internet: The Government of India & Standards Development at the IETF", November 29, 2018, Centre for Internet and Society, India, Retrieved from https://cis-india.org/internet-governance/files/regulating-the-internet

and Decryption) - Impact on Indian enterprises' - which is a welcoming move. Further harmonization of an international legal encryption standard with the national policy would serve as a major boost in strengthening encryption laws. The move such as by MeitY ensures that it is harder for foreign intelligence agencies or other attackers to decrypt Indian internet traffic, and thereby strengthening national security.