Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
so as we move into the ‘new normal’ of the post-Covid-19 workplace. To be effective, deploying security solutions for endpoints must be easy and updates should be automatic.

“Endpoints need not continue to be the weakest point in the organisation cloud ecosystem. Organisations can implement measures to minimise the likelihood of a high-profile breach”

It is unlikely that one solution can cover all threats, so if standard anti-virus and EDR protection is already in-place, subsequent protections based on containerisation, anti-keylogging and anti-screen scraping, must be complementary and compatible. Finally, the importance of regulatory compliance must be taken into account. Security solutions should meet with PCI, PSD2, HIPAA and General Data Protection Regulation (GDPR) regulations. The fact that an organisation’s employees are working from home will be no defence if a GDPR breach occurs and it is facing a hefty financial penalty for want of endpoint security that is fit for purpose.

The technology exists to ensure that endpoints need not continue to be the weakest point in the organisation cloud ecosystem. Organisations can implement measures to minimise the likelihood of a high-profile breach. By securing the input of sensitive data and by wrapping security around the applications that handle sensitive data, organisations can add another layer, boosting the protection of endpoint devices. In today’s world with more and more data being handled outside of the protection of the corporate perimeter, with BYOD and working from home, emerging technologies can help with both compliance and the overall security posture.

About the author
Dave Waterson is CEO at SentryBay and an expert in endpoint and application security. His technical focus areas are anti-keylogging, anti-phishing, data security, secure browsing, IoT, mobile security, identity theft and cloud-based security. He was included among the top 10 tech thought leaders identified by AT Kearney at the World Economic Forum in Davos and is a winner of the Great British Entrepreneur of the Year Award for cyber security.

References
1. ‘Endpoint Security Trends Report 2019’. Absolute. Accessed Jul 2020. www.absolute.com/go/study/2019-endpoint-security-trends/.
2. ‘Endpoint Security Market 2019 – 2023’. The Radicati Group, Nov 2019. Accessed Jul 2020. www.radicati.com/wp/wp-content/uploads/2019/01/Endpoint_ Security_Market_2019-2023_Executive_Summary.pdf.
3. ‘The state of endpoint security risk: it’s skyrocketing’. Ponemon & Sullivan, 12 May 2020. Accessed Jul 2020. https://ponemonsullivanreport.com/2020/05/the-state-of-endpoint-security-risk-its-skyrocketing/.
4. Canter, Lily. ‘Coronavirus: Half of remote workers victims of cybercrime’. Yahoo Finance, 29 Apr 2020. Accessed Jul 2020. https://uk.finance.yahoo.com/news/coronavirus-half-of-remote-workers-victims-of-cybercrime-144200532.html.
5. ‘Global Threat Intelligence Report’. NTT Security, 2020. Accessed Jul 2020. www.nttsecurity.com/docs/librariesprovider3/resources/2019-gtir/2019_gtir_report_2019_uca_v2.pdf.
6. Bond, Robert. ‘SANS Institute – Less than 50% of cyber attacks detected by anti-virus software’. SecureOps, 8 Aug 2018. Accessed Jul 2020. https://secureops.com/security/anti-virus-ineffective/.
7. ‘What is a container?’. Docker. Accessed Jul 2020. www.docker.com/resources/what-container.
8. ‘Windows Defender Application Guard’. Microsoft, 28 Mar 2019. Accessed Jul 2020. https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/wd-app-guard-overview.

Zoombombing – the end-to-end fallacy
Ion-Alexandru Secara

Zoombombing, a trend in recent months, has quickly moved from online classroom pranks to organised disruption efforts, which the FBI has threatened to punish with jail time. “The FBI has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language.” the agency stated in a recent press release.1

As shelter-in-place and lockdown orders were enforced around the world, Zoom meetings replaced classrooms, offices, gaming lobbies and even concert halls. Throughout the month of March alone, over 200 million people used the conferencing platform, compared to the previous monthly maximum of 10 million.2

An investigation carried out by the New York Times in April has revealed that a considerable number of social media accounts, including Instagram accounts, Twitter accounts, message boards on Reddit and 4Chan, are
used by thousands of people to carry out Zoom disruption campaigns. The people in question create plans and share meeting passwords that they use to join public and private meetings.

Experts report that 500,000 Zoom accounts are usually being sold on the dark web and hacker forums. Some of those accounts have been broken into using information from older data breaches, known as credential-stuffing attacks. Many users use the same password (or a limited set of passwords) across all accounts that they use on the Internet. Therefore, once an account is compromised in one place, it is highly likely that there will be accounts made by the same user that can be accessed on other platforms, using the same set of credentials.

**Encryption claims**

While stuffing attacks contributed to a certain extent, an even more critical security issue led to many Zoom accounts being compromised. Zoom claims to use end-to-end encryption. This method is considered to be one of the most secure ways to communicate information online. It uses cryptographic keys to encrypt and decrypt data. Encryption and decryption happen at both ends of the connection, preventing anyone in the middle – including the platform itself – from accessing the information. Both the sender and the receiver have a private key, accessible only to each one of them, and a public key which is freely available. Each user’s public and private keys are mathematically related. Therefore, the sender uses the receiver’s public key to encrypt the message into ciphertext. Only the receiver can decrypt the message back to plain text, since no one else has the receiver’s private key.

But a blog post released by Zoom in April 2020 shows that the company’s end-to-end encryption architecture does not conform with the standard industry definition for this kind of encryption. Instead it describes the application of Transport Security Layer (TLS) encryption to the data transfer that happens between users and the Zoom servers, as seen in Figure 1.

Theoretically this allows the company to access data from its users, using server-side decryption. Moreover, some of the calls on the Zoom platform, and the keys for specific conferences, are actually routed through China. This was discovered in a study carried out by The Citizen Lab, which shows that a call between two users, one in Canada and the other in the US, was routed through a server located in Beijing.

Despite the fact that Zoom is headquartered in San Jose, the Zoom platform is developed by three companies based in China, which employ more than 700 people, as seen in the latest SEC filing from the company. Since a large portion of the engineers are located in China, Scott Stewart, VP of Stratfor’s Threat Lens, has previously stated that the company’s failure to use end-to-end encryption can allow an employee to be pressured by the Chinese authorities into accessing and sharing private meetings carried over the video conferencing platform.

This is a critical issue since it is not the first time Zoom has shared users’ information without their authorisation. An analysis carried out by Motherboard showed that user analytics, collected on Zoom’s iOS mobile application, are transferred to Facebook. A connection to the Facebook Graph API was cre-
ated whenever the app was accessed, as shown by network logs stored on iOS devices. While the transferring of data to Facebook was swiftly removed, Zoom could still be using server-side decryption to process and transfer user information to unauthorised third parties.

Architectural issues

An even larger issue that the video conferencing platform faces lies in the architecture that it uses. The transport protocol is a derivation of the Real-time Transport Protocol (RTP) standard. The derivation adds an extra custom encryption layer on top of the RTP standard. As published in a study by CitizenLab, a Zoom meeting is encrypted using a single AES-128 key, generated on the server side and shared with all the clients.

“AES-256 and end-to-end encryption, when used together in an appropriate manner, represent one of the most secure ways of encrypting and transferring data”

This key is encrypted in Electronic Code Book (ECB) mode, which is one of the simplest forms of encryption and is semantically insecure. Merely analysing ciphertext encrypted using ECB can reveal information about the original text. This is because ECB encrypts blocks of data of the same fixed byte size using the same exact key. Hence, if the information to be encrypted is not smaller than a single block of data – which is very rare since the block sizes used are commonly 64 or 128 bits – the ciphertext will have very similar patterns to the original data. In Zoom’s case, the main pieces of data to be communicated are the users’ video streams. Figure 2 clearly shows that the outline and patterns of the original image are easily observed in its ECB-encrypted version, compared to the same original image being encrypted using AES-128 in Cipher Block Chaining (CBC) mode.10

Using AES-128 in ECB mode is subpar to industry standards, as even Eric Yuan, the CEO of Zoom, has admitted.11 Many companies use AES-128 encryption in CBC mode. The main flaw of ECB is that each identical block of data will result in the same piece of cipher text. Therefore, CBC addresses this issue by making sure that the resulting cipher always changes. CBC initially creates an initialisation vector, a fixed-size random input, which is then passed through an XOR gate together with the first block of plain data. The result is then encrypted. The next block of plain data is then passed through the XOR gate together with the result from the previous block and the result is encrypted. This process continues until all the blocks of data are encrypted.12 The initialisation vector is also changed for every new message, making patterns even more difficult to find in the encrypted cipher. Decryption is relatively straightforward – the process above is done in reverse.

AES variants

There are three variations of AES encryption – AES-128, AES-192 and AES-256. The only difference between them is the number of encryption rounds. AES-128 uses 10 rounds, AES-192 uses 12 rounds and AES-256 uses 14 rounds.13 The more rounds of encryption that data goes through, the harder it becomes to break. A CIA report on cyber security strongly encouraged the use of AES-256 encryption, rather than AES-128, which seems to be the current industry standard.14

The CIA report mentions that AES-256 and end-to-end encryption, when used together in an appropriate manner, represent one of the most secure ways of encrypting and transferring data. The report also states that the encryption keys should not be left out in the open and readily available, but should be stored in a secure place that makes it hard for hackers to access.15 Those are all practices that Zoom does not implement.

“While Zoom has improved its security, we need end-to-end encryption to talk with our friends and loved ones without second-guessing everything we say, and worrying that someone else may be listening,” said Albert Fox Cahn, executive director of the Surveillance and Technology Oversight Project.16 “Encryption has always been indispensable to secure communication, but today it’s more crucial than ever.”

Still being used

Despite all these security threats and the FBI stating that hackers could exploit these weaknesses to “steal sensitive information, target individuals and businesses performing financial transactions, and engage in extortion”, Zoom is still used by millions of people, including high-ranking government officials. While Zoom can be used in browsers, a large portion of its user base downloads and uses the desktop application. This can pose a major security threat to the user’s computer and, as seen before, issues did happen with the Zoom desktop application around nine months ago.
The Zoom desktop application runs in the background on the user’s computer and listens to a specific port. Hence, when a user clicks to join a meeting in the browser, the desktop application is swiftly started – a request is sent to the port that the Zoom application listens on. When it receives the request, the application boots itself up. The issue, now fixed, was that the Zoom application accepted requests from any web or local source. This allowed hackers to create denial of service (DoS) attacks on a user’s computer by repeatedly sending requests to the port that the application is listening to. In turn, this would constantly boot up the application, stealing the user’s ‘focus’ and making the computer almost unusable, unless the Internet connection was lost.17

“Having an open port that can be used to download complete software to a user’s computer can allow hackers to silently download malware and viruses. This would most certainly compromise the user’s computer”

Another security threat was posed by the fact that the Zoom application could automatically re-download itself after the user uninstalled it. Having an application be able to download updates can be strictly controlled through policies and secure update channels, but having an open port that can be used to download complete software to a user’s computer can allow hackers to silently download malware and viruses. This would most certainly compromise the user’s computer.

Those issues were fixed several months ago – for people who have installed the patches and updates – but the possibility of new security vulnerabilities arising in the future is still there. Joseph Steinberg, a cyber security expert, has emphasised this by stating that: “If there are vulnerabilities, the [Zoom] app can jeopardise the security of data on the computer on which it is installed, or even potentially on other computers on the same network. Such vulnerabilities have been discovered – and more may exist.”18

Serious threats

The lack of use of security industry standards in Zoom’s video conferencing platform creates serious security threats to its users’ information and meeting confidentiality. However, there are signs that the company is trying to mitigate these issues and it has released a 90-day plan to address them.

To strengthen its security and privacy capabilities, Zoom has acquired Keybase, which developed a secure end-to-end messaging and file-sharing service.19 It appears that the company is moving towards the industry standard of end-to-end encryption. Developing an end-to-end encryption system would prevent server-side decryption threats, meaning that the chance of having the company itself access confidential user information is significantly reduced.

“Certain companies focus more on the functionality they provide to their users than they do on the appropriate security”

In a recent blog post, Zoom also announced that as part of its 90-day plan, it will start supporting AES-256 encryption in Galois Counter Mode (GCM). GCM has similar capabilities as CBC, described above, and in many ways they produce the same performance. However, the two encryption modes work differently internally. GCM creates a counter and then sends it through the block cipher. The output from the block cipher is then passed through an XOR gate, together with the plain text, to form ciphertext.20 This major security change has been implemented in Zoom 5.0 and will slowly be rolled out to the company’s entire user base. Using AES-256 GCM encryption would significantly increase Zoom’s security and would prevent cases, such as the example presented in Figure 1, from occurring.

This shows that Zoom is learning from its previous mistakes and security flaws and is actively taking steps to improve on them. While those steps will bring the videoconferencing platform up to date with industry standards, it clearly shows that certain companies focus more on the functionality they provide to their users than they do on the appropriate security. However, as working from home has made a large population of the world become massively dependent on the use of the Internet to carry out its day-to-day work activities, the security, integrity and confidentiality of information is becoming increasingly important.
Ion-Alexandru Secara is a former software engineer at Adobe, where he developed a monitoring tool for the Adobe API, and a former software engineer at Intuit, where he worked on creating secure endpoints and network channels for users that pay their taxes online. Due to his expertise in the field, Secara regularly speaks at API and network security conferences, while advising founders, from early-stage startups, on their approach to API and network security.

Resources
- StationX Cyber Security Blog, home page. Accessed Jul 2020. www.stationx.net/blog/.
- The Last Watchdog, home page. Accessed Jul 2020. www.lastwatchdog.com.
- Dark Reading, home page. Accessed Jul 2020. www.darkreading.com.

References
1. Setera, Kristen. ‘FBI warns of teleconferencing and online classroom hijacking during Covid-19 pandemic.’ FBI Boston, 30 Mar 2020. Accessed May 2020. www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.  
2. Miller, Maggie. ‘Zoom CEO says company reached 200 million daily users in March’. The Hill, Apr 2020. Accessed 2 Apr 2020. https://thehill.com/policy/cybersecurity/490794-zoom-ceo-says-company-reached-200-million-daily-users-in-march.  
3. Lorenz, Taylor; Alba, Davey. ‘Zoombombing becomes a dangerous organised effort’. The New York Times, 3 Apr 2020, Accessed Apr 2020. www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html.  
4. Hamilton, Isobel Asher. ‘Researchers found and bought more than 500,000 Zoom passwords on the dark web for less than a cent each’. Business Insider, 14 Apr 2020, Accessed Apr 2020. www.businessinsider.com/500000-zoom-accounts-sale-dark-web-2020-4.  
5. Gal, Oded. ‘The facts around Zoom and encryption for meetings/webinars’. Zoom Blog, 1 Apr 2020. Accessed Apr 2020. https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/.  
6. Marczak, Bill; Scott-Railton, John. ‘Move Fast and Roll Your Own Crypto’. The Citizen Lab, 3 Apr 2020. Accessed Apr 2020. https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidence-of-zoom-meetings/.  
7. ‘Form 10-K Zoom Video Communication, Inc’. United States Securities and Exchange Commission, 31 Jan 2020. Accessed Mar 2020. https://investors.zoom.us/static-files/09a01665-5f33-4007-8e90-de02219886aa.  
8. Babb, Carla. ‘US military, government workers still use Zoom despite FBI warning’. VOA News, 10 Apr 2020. Accessed May 2020. www.voanews.com/silicon-valley-technology/us-military-government-workers-still-use-zoom-despite-fbi-warning.  
9. Sarkar, Sharmishtha. ‘After backlash, Zoom ditches snooping Facebook code from iOS app’. Tech Radar, 29 Mar 2020. Accessed Mar 2020. www.techradar.com/news/after-backlash-zoom-ditches-snooping-facebook-code-from-ios-app.  
10. Ottenheimer, Davi. ‘Simple illustration of Zoom encryption failure’. Security Boulevard, 10 Apr 2020. Accessed Apr 2020. https://security-boulevard.com/2020/04/simple-illustration-of-zoom-encryption-failure/.  
11. Novet, Jordan. ‘Zoom CEO explains stance on encryption, says he wants to ‘work together’ with law enforcement’. CNBC, 3 Jun 2020. Accessed Jun 2020. www.cnbc.com/2020/06/03/zoom-ceo-eric-yuan-on-encryption-working-with-law-enforcement.html.  
12. de Mello, Flavio L; Xexeo, Jose AM. ‘Identifying encryption algorithms in ECB and CBC modes using computational intelligence’. Journal of Universal Computer Science, Jan 2018. Accessed Nov 2018. www.jucs.org/jucs_24_1/identifying-encryption Algorithms_in/jucs_24_01_0025_0042_demello.pdf.  
13. Crawford, Douglas. ‘How does AES encryption work?’. ProPrivacy, 4 Feb 2019. Accessed Jan 2020. https://proprivacy.com/guides/aes-encryption.  
14. ‘Use Cryptography Like The CIA’. Cryptosense, 24 Mar 2017. Accessed Aug 2019. https://cryptosense.com/blog/use-cryptography-like-the-cia/.  
15. Vallabhaneni, S Rao. ‘Wiley CIA Exam Review 2020, Part 2: Practice Of Internal Auditing’. Wiley Efficient Learning, Sep 2019. Accessed Feb 2020.  
16. ‘End to end encryption saves lives: it’s time for Zoom to lead the way in online public safety says civil society groups and security expert at press conference’. StopSpying, Apr 2020. Accessed May 2020.  
17. Leitschuh, Jonathan. ‘Zoom zero day: 4+ million webcams & maybe an RCE? Just get them to visit your website!’. Medium Infosec Writeups, 8 Jul 2019. Accessed Dec 2019. https://medium.com/bugbountywriters/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75e83feef5.  
18. Babb, Carla. ‘Pentagon Issues New Guidance on Zoom Use’. VOA News, 10 Apr 2020. Accessed Apr 2020. www.voanews.com/silicon-valley-technology/pentagon-issues-new-guidance-zoom-use.  
19. Yuan, Eric. ‘Zoom acquires Keybase and announces goal of developing the most broadly used enterprise end-to-end encryption offering’. Zoom Blog, 7 May 2020. Accessed May 2020. 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/.  
20. Rogaway, Phillip. ‘Evaluation of some blockcipher modes of operation’. Cryptography Research and Evaluation Committees for the Government of Japan, 10 Feb 2011. Accessed Jan 2020. https://web.cs.ucdavis.edu/~rogaway/papers/modes.pdf.