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.
Facing up to security and privacy in online meetings

Reinhardt Botha, Nelson Mandela University and Steven Furnell, Nelson Mandela University and University of Nottingham

One of the most noticeable effects of the Covid-19 pandemic from the technology perspective has been the significant uptake of online meeting platforms, which many have suddenly found to be a necessary alternative to face-to-face meetings in all manner of contexts. From relatively casual meetings that may have taken place among co-workers in the office, through to the staging of full conference events, online platforms have essentially come to the rescue when in-person gatherings were no longer an option.

Of course, in parallel with essentially being forced to use the tools out of necessity, many have also found that they introduce an element of previously untapped flexibility, enabling and encouraging contact that may not previously have happened (which is not to say that the option was not there before – the technology would have enabled it, but relatively few were taking advantage of it).

At the same time, the rapid transition to home working left many organisations unprepared from a security perspective, with the use of online meetings representing one of the most notable consequences of working from home.1 With a significant number of people becoming first-time users as a result of the pandemic, it arguably caught a user population that was largely unprepared, unguided and unaware of what good security looked like.

Additionally, with home working, they may have had no easy option to turn to for support.

Security challenges

This article spotlights the security and privacy challenges from a number of perspectives. While the infrastructure may present its own challenges to security and privacy, this paper does not consider that. The first order of business here is discussing security and privacy from the perspective imposed by the multitude of online meeting platforms that exist. Thereafter the paper moves to operational concerns, looking at security and privacy along the lifetime of the meetings: first the scheduling of the meeting, then the actual meeting, followed by post-meeting activities. Figure 1 depicts various areas in which security and privacy concerns will come into play (noting that the discussion of the infrastructure layer is out of scope for the discussion in this article).

Before proceeding it is worth noting that the increased adoption and use of such tools during the pandemic has led to a rather dynamic environment in terms of new versions and updates, and the technology has arguably evolved somewhat on the fly during the pandemic in response to demand for new features and fixes. As such, while this paper is commenting on the situation at the time of writing, there is a good chance that various aspects will have changed by the point of publication and beyond. Notably, however, given that the sampling period is around a year into the global pandemic, these are still the best features that users will have had during the majority of the home working period.

Multi-platform environment

One of the first challenges in terms of considering the security of online meetings is the sheer range of different platforms available. Among the most prominent exam-
ples are Zoom, Microsoft Teams, Cisco Webex, Google Meet and Adobe Connect. However, numerous other options exist (eg, a summary from TechFunnel catalogues a further 22 examples alongside those already listed), and their utility can vary depending upon whether the aim is to support casual discussion, team-based collaboration or speaker-to-audience events. For this article we will assume the generic context of a group meeting, which simply seeks to provide a virtual alternative for the sort of pre-pandemic meeting that would typically have taken place face-to-face in a meeting room.

“With a significant number of people becoming first-time users as a result of the pandemic, it arguably caught a user population that was largely unprepared, unguided and unaware of what good security looked like”

Even if their organisation has settled on a particular platform, many users will have encountered various others as a result of dealings with other people or organisations that have made different choices. For example, in addition to using the five listed above, the authors’ experience during the Covid-19 period also included using BigBlueButton, BlueJeans, GotoMeeting, Google Meet and Skype for Business. As such, users may have found themselves installing and configuring a multitude of different tools – often at short notice – when realising that they needed to download an additional client or plug-in in order to join an imminent meeting.

The latter aspect is of particular note, especially in cases where updates were needed due to security vulnerabilities having been discovered in the earlier versions. As a widely recognised example, we can consider the case of Zoom. Having initially been heralded as the salvation for home workers, Zoom unfortunately acquired a bad name for security early on in the pandemic, as a result of lack of end-to-end encryption, concerns over data privacy and other vulnerabilities (perhaps the most notable of which was so-called ‘Zoom bombing’, where uninvited participants were able to enter and disrupt meetings). This subsequently resulted in an order from the US Federal Trade Commission, ordering Zoom to avoid misrepresentation of the data it collects from users and how it is protected, as well as to “establish and implement, and thereafter maintain, a comprehensive information security program”.

Perhaps unsurprisingly, the negative coverage has somewhat stigmatised Zoom in terms of security and consequently affected many people’s willingness to use it. However, it is by no means alone in having had vulnerabilities, and there were also a number of reports relating to other platforms. This is illustrated in Figure 2, which depicts the number of entries relating to different platforms within the Common Vulnerabilities and Exposures (CVE) database of publicly known cyber security vulnerabilities (see cve.mitre.org).

Considerations before meetings

Having considered the underlying platforms, the discussion now highlights

![Figure 2: 2020 CVE entries for online meeting platforms.](image)
further points that may arise during individual meetings. We start at pre-meeting configuration, then look at the measures during the meeting and conclude with observations from an after-meeting perspective.

“Various security and privacy-relevant options can be rather hidden away. Indeed, various features will not be encountered in normal day-to-day use, unless the user knows to go looking for them.”

A fairly immediate observation that can be made in relation to setting up meetings is that various security and privacy-relevant options can be rather hidden away. Indeed, various features will not be encountered in normal day-to-day use, unless the user knows to go looking for them. This highlights the fact that features not only need to be available – they also need to be suitably visible and accessible.

For example, in Teams, options are accessed by a link to set the options at the bottom of the message (see Figure 3). Since the link is part of the message, further confusion could be spread since the link is available to everybody, although only the organiser can make changes.

As a more substantial example, we can look at the security options available for scheduling a meeting in Zoom, comparing those presented directly within the application (Figure 4) and the further web-based options available if the user follows a link to change settings (Figure 5). The web portal clearly offers a range of further options that could be useful, and which users may wish to configure on a per-meeting basis (particularly around the points that relate to controlling/limiting access). However, the fact that they are in this interface rather than the main one reduces the likelihood of them being seen and remembered. In fact, some users may never see them, as without clicking the link to go looking there is no indication of what further options are there to be found.

**Controlled access**

Controlling access to meetings is critical. The use of passwords adds a perceived layer of security to the meeting. However, it should be noted that in Zoom, for example, passwords are per meeting and not per user. As such, it provides no proof of identity but only adds an extra hurdle. If these ‘passwords’ are advertised through bulk emails or social media, it adds no security or privacy to the meeting.

“While two-factor authentication provides assurances to participants regarding their account being used by an unauthorised party, for meeting organisers it adds no additional proof as profile details can be easily spoofed.”

Zoom has encountered negative coverage as a result of unauthorised users entering unprotected meetings when the pandemic forced online meetings to become the norm. Zoom introduced the option to protect accounts with two-factor authentication. However, it should be noted that while two-factor authentication provides assurances to participants regarding their account being used by an unauthorised party, for meeting organisers it adds no additional proof as profile details can be easily spoofed.

When the above is considered in the context of organisations, a bigger burden of proof can be required. For example, Teams could restrict meetings to the internal organisation, thus requiring users to authenticate to the domain. Similarly, in Zoom, users can choose to require that a user is signed into Zoom with a specified domain, or even require authentication to an external single sign on (SSO) provider.
Since this may not always be plausible to implement, there are other mechanisms to support security and privacy efforts in relation to controlling access to meetings:

**Lobbies or waiting rooms** can require the user to be approved and let in by the host. Within MS Teams, this can be bypassed for people that are part of the organisation and thus already authenticated within the organisation, removing an additional burden on the administrator. Users from outside the organisation are then authenticated based on information displayed from their current authentication to Teams. Zoom also provides a waiting room that can be customised. In small meetings, administrators could clear the waiting room quickly as participants may be known or quickly confirmed. However, in large meetings, this can add a considerable overhead to the administrator who needs to ‘authenticate’ a user with minimal proof (e.g., based on a user’s screen name). However, if someone has been admitted to the meeting in error, or a certain portion of discussion needs to remain confidential from certain participants, then they can also be placed back into the waiting room. However, this option is not fully available on the fly, as the waiting room facility typically needs to be enabled by the host when setting up the meeting.

**Country-level locks** can be used in Zoom to limit the attendees to a specific country. This may assist in the administrative burden if the administrator can be confident that meeting participants are only from certain countries. However, this requirement may conflict with other security and privacy mechanisms used by participants. Most notably, VPNs may make it appear that a user is in a different country than they really are. The corollary to this is that attackers can make it look like they are in a country when they are not.

**Join before host** options may lead to people joining the meeting before determining whether they belong there. If the participants are not aware of who belongs in the meeting, it could cause privacy and confidentiality concerns. While this may not be relevant in public meetings, in private business meetings, this could be problematic. In both cases, unwanted participants could be disruptive.

**Auto-mute on entry** options serve to prevent interruptions of that nature and prevent people joining the meeting late from being unintentionally disruptive.

**Pre-meeting configuration**

There are also further pre-meeting configuration options that can have an impact upon the privacy of the subsequent meeting content. Again, using Zoom’s settings as a point of reference, two relevant examples are as follows:

- Meeting convenors also have the option to auto-record the meeting from the start. While this is indeed convenient for the organiser, who may need the recording to create minutes...
of the meeting, auto-recording takes away the opportunity to warn and receive consent from participants for recording verbally. Recording of meetings creates potential concern throughout the meeting’s lifecycle and is further discussed below in the in-meeting and post-meeting contexts.

- While both public and private chat channels are generally available within the meeting platforms, organisations might wish to give more consideration as to whether they allow it. Aside from the distraction of the side-line conversations that can arise, the chat represents data generated by the meeting. Thus, an artefact that could be saved and become privacy-relevant is created. These settings need to be configured before the meeting takes place. Another interesting aspect to consider is the interaction between features. In Zoom, for example, users who are recording the meeting also save any private chats that they participated in as part of the meeting transcript.

All of this serves to show that the configuration options available to convenors during meeting setup provide some control over the resulting security and privacy aspects of a meeting. However, other attendees do not have any control at this stage, including the visibility of the meeting configuration. For example, privacy-sensitive participants cannot determine whether meeting recordings will be allowed before the recording. With this in mind, the next section proceeds to examine the options that convenors and attendees have once meetings have started.

Considerations during meetings

Once meetings are underway, it is fair to say that attendees have limited control over things. Unless prevented by the host’s prior settings, they can elect whether to be visible on camera and whether to participate via microphone or chat. However, there are a couple of notable aspects in which they may have some further decisions or considerations to be faced.

Virtual backgrounds or background blur: This allows participants the option to have some privacy of their surroundings when on camera, which can be particularly relevant for home working if they do not wish to give others a view into their domestic environment. Support for this aspect is still quite varied between platforms. For example, Zoom had offered the option for custom backgrounds from the outset of the pandemic, whereas Teams initially supported only background blurring or a few pre-set images but was offering fully custom backgrounds by June 2020. Meanwhile, Adobe Connect does not offer any background privacy features, and Google Meet only supports them if the user is accessing the meeting via the Google Chrome browser (and has suitable hardware to support the use of the video effect).

“While you give consent to be recorded (albeit without an option to opt-out and still be part of the meeting), the basic message says nothing about the distribution/use of the recording”

Recording the meeting: Various platforms allow for the recording of meetings. What is potentially problematic is the control given to the participants. As an example, we can consider the recording of meetings in Microsoft Teams. While participants are told that the meeting is being recorded, they are offered no warning or option to opt out before it starts. Teams tries to remind the host to exercise courtesy by telling the participants that are being recorded (see Figure 6a), but ultimately there is nothing that requires participants to have received any consent confirmation. Meanwhile, what the other participants get to see is presented in Figure 6b, and the message presented to them seems rather disingenuous. It is clear that the recipient is not getting a complete opportunity to opt out (eg, if he was already in vision at the time the host started to record, then even if he disables his camera at this point, he will be visible for a brief portion of the final recording).

Considerations after meetings

The main issue after meetings tends to arise if the session has been recorded, as this introduces issues around the storage and distribution of recordings and/or associated text transcripts. Distributing recordings of meetings: Some platforms, for example MS Teams, do not allow sharing of the recording outside of organisational boundaries, which leads to downloads and distribution through other channels. While you give consent to be recorded (albeit without an option to opt-out and still be part of the meeting), the basic message says nothing about the distribution/use of the recording. To reflect on the implications of this, think of a time when online meetings were not as pervasive. People might have felt very comfortable with the meeting secretary making a recording for use in the compilation of minutes, but not for other purposes. Those recordings were generally voice-only and access to them was strictly controlled. People might assume the same about the recording of online meetings, but this may not reflect what is happening. First, a video recording differs significantly in privacy terms from a voice recording. It represents the person’s likeness, and if background blurring is not used, the person’s surroundings. Second, the recordings are often available to all participants of the meeting. While this may not seem like a problem, it would allow for easy distribution, possibly resulting...
in confidentiality and privacy concerns. The problem lies in the lack of control by the participant who was recorded.

**Automatic transcripts:** The ability of platforms to create automatic transcriptions of recorded meetings introduces another artefact that must be managed securely. As with the recordings themselves, the transcript puts people more ‘on the record’ throughout a meeting than they might previously have been. Casual or even indelicate comments (that may have been overlooked or omitted from formal minutes) are no longer ephemeral. Thus, the transcripts need to be considered as having at least the same level of sensitivity as minutes from a meeting.

**Variations and complications**

Another dimension to the challenge is that some of the platforms can be used via web browsers or locally installed applications, and the features and control available to users can vary as a result (eg, in Adobe Connect, screen sharing and offline recording are not available to users via the browser and can only be done using the desktop application).

“There is a lack of security by design, alongside an apparent lack of consideration or prioritisation of security and privacy aspects in the user interface and experience”

Additionally, while the discussion has looked at desktop versions, there are further variations to be found in the mobile apps. As observed in prior work over a decade ago, desktop and mobile contexts can often differ in the security options that they offer. Figure 7 illustrates elements of the desktop and mobile interfaces for Zoom, from macOS and iOS versions respectively, and (aside from the layout) the range of key options is ostensibly the same. However, there is a notable difference insofar as opening the option in the desktop version offers the user a pop-up window with a link to their ‘Default settings’ (from which the various other security and privacy-related meeting settings are available).

The Zoom app usefully reports that it has synchronised settings from the web portal, but offers no link to get to them. Similarly, there is no option to reach them from within any of the other settings within the app, whereas the desktop version provides a link as part of the General settings. This is arguably significant when this interface is the only route to accessing some of the security-related settings (eg, the option to require a passcode for participants joining by phone). While mobile users could login separately via a web interface in their browser, this clearly breaks the user experience (and they need to know/remember that such settings are there in the first place – having the link as part of the app interface flags it for possible exploration, which is especially useful if users are looking around to answer the question ‘is there a way to do XYZ?’).

**Conclusions**

There is no denying that online meeting platforms have been a lifeline for many activities during the pandemic. As such, it may even feel unpleasant to be negative about them. Moreover, the discussion may ultimately seem to be suggesting a catalogue of criticisms and finding faults without offering any solutions. However, part of the point is that a solution should not need to be found in the first place – various of the issues highlight further examples showing that there is a lack of security by design, alongside an apparent lack of consideration or prioritisation of security and privacy aspects in the user interface and experience. Many of the issues are likely to be resolved over time as the tools evolve, but it would be nice to imagine that we will one day reach a point where such gradual nudging towards effective security is no longer needed because it will be there from the outset.

**About the authors**

Reinhardt Botha is a professor of information technology and director of the Centre for Research in Information and Cyber Security (CRICS) at Nelson Mandela University, South Africa. His research interests include information security and privacy, security management and access control. He has authored around 100 papers in refereed international journals and conference proceedings.

Steven Furnell is a professor of cybersecurity at the University of Nottingham. He is also an honorary professor with Nelson Mandela University and an adjunct professor with Edith Cowan University in Western
Security misconfigurations and how to prevent them

Sergio Loureiro, SecludIT

Security misconfigurations present serious trouble when security settings are not properly defined and implemented and default values are retained. Usually, this means the configuration settings do not comply with industry security standards such as the Center for Internet Security (CIS) benchmarks, OWASP Top 10 etc, which are critical to ensuring smooth business continuity, security maintenance and a reduction in business risk.1,2

Misconfiguration normally happens when a system or database administrator, or a developer, does not properly configure the security framework of an application, website, desktop or server. This leads to avenues for exploitation from opportunistic hackers.

For a seasoned cyber criminal, misconfigurations are often seen as an easy target, as it can be simple to detect misconfigured web servers, cloud instances and applications, which then become exploitable. This can cause significant harm and lead to catastrophic data leakage issues for enterprises. Examples include the 2019 Teletext exposure of 530,000 data files, which was caused by an insecurely configured Amazon Web Service (AWS) web server.3

Unfortunately, once a system falls victim to a vulnerability or lack of security safeguarding, your sensitive data is at risk of being stolen or altered. Often, the biggest problem that organisations face is that these flaws are not identified or addressed early enough in accordance with security hygiene best practice. This is becoming a widespread security challenge, with misconfiguration accounting for 82% of overall security vulnerabilities and we’ve been seeing high-profile stories around this topic in the industry press for a number of years.4 These include the exposure of 750,000 birth certificate applications in the US on an AWS storage bucket in 2019, and another misconfigured cloud storage bucket exposing hundreds of thousands of mobile phone bills for AT&T, Verizon and T-Mobile subscribers due to human error and misconfiguration.5,6

As the previously mentioned examples show, many enterprises are migrating...