Protecting the security of you video calls

(English translation of an invited Afrikaans article by Prof Basie von Solms, published on 6 May 2020 on the LitNet website at

https://www.litnet.co.za/beskerm-die-sekerheid-van-jou-video-oproepe/)

The present Covid-19 pandemic has forced all of us to very quickly find new ways to perform normal tasks because the old ways were not possible anymore. Some of these normal tasks which were impacted are of course those related to physical person to person communication like meetings, conferences, lectures and other situations where we used to meet in a physical room or lecture hall.

The logical solution to this new problem was to use available technology making use of online Internet based video calls, which had been available long before the virus appeared and for which several products are available. The technology was well known and had been widely used, but mostly on an ad hoc basis. Today everybody is basically exclusively using this technology for online meetings, conferences, lectures and many more.

Of course we can be very happy that such technologies are available for immediate use to maintain productivity and knowledge transfer. Unfortunately, the sudden use and acceptance of these video communication technologies, have caused serious problems., specifically related to privacy, confidentiality and security. The reason for this is because many of these video technologies are very user friendly and easy to use, people grabbed the opportunities and started using the technology in a helter-skelter way. The technology has therefore been used by many users not having the knowledge, experience and insight into the relevant risks, specifically about securing their communications. This resulted in cyber criminals disrupting and hijacking such communications.

Many published papers have in the recent past reported that video communication using the Zoom product was disrupted and hijacked in this way. Such attacks actually got a name and are called Zoom bombing. Typically, the cyber hijacker will join a video conference and then make unacceptable comments and inject unacceptable images to all screens. Of course this totally disrupts any event.

Although there may be certain inherent vulnerabilities in the Zoom product, many of these type of cyber-attacks could have been prevented if the host of the meeting had been knowledgeable about the available security, confidentiality and protection settings of the product. If such settings have been activated before and during an online discussion, it would have prevented many such attacks.

It is not the purpose of this article to discuss such settings in Zoom in detail – there are many good articles available which provide lots of detail how to maintain the integrity of an online conference. Any search engine will retrieve many such articles. For example, the article *'Do's and Don'ts of videoconferencing security'* at https://www.computerworld.com/article/3535924/do-s-and-don-ts-of-videoconferencing-security.html gives a lot of good hints on making Zoom more secure.

However, it is very important to investigate the general risks involved with the use of such products.

Let us start by investigating a few of the direct consequences of practicing bad video conference preparation and hygiene.

During such online conference the whole discussion can be recorded. There are several reports where complete discussions were later located somewhere on the Internet – somebody copied the recording in an unauthorised way. Just imagine if this was a discussion where a company Board discussed sensitive information of the company, like the annual budget or their competitor strategies. It could also have been a sensitive discussion between a doctor and a patient. It is therefore essential that the video product used has the technical functionality to secure the discussion and prevent interception. Another risk is that your competitor may get access to your sensitive video meeting, but remain quiet and 'invisible' to obtain your sensitive information – literally an electronic fly on the wall!

Furthermore, it must be remembered that in such a video call, all participants can potentially get indirect access to the other participants' devices (computers, laptops, tablets, mobile phones). Potentially this can allow a cyber-criminal to load malware on your device which can cause massive problems for you. Basically such a cyber-criminal can then take over your phone's camera and switch it on and off as he desires. Access to your personal information is also possible which can result in all your online login information to online services can be stolen. Therefore, over and above the fact that the host of the meeting must follow good procedures and practices, every participant must also ensure that his or her device has the necessary security protection installed on the individual device.

AS mentioned above, it is not necessary the specific video product which is the culprit in the story, but very often it is the users of the product which use the product without realizing the risks. They use the basic generic vanilla version, which can cause many of the problems mentioned above. Most of these video products have security settings which are powerful enough to prevent many of these type of attacks - of course if these setting are properly implemented and the prescribed procedures and guidelines are followed.

The basic rules for the use of any computer device or product used to access Cyberspace, is

- You must realize and understand that you are responsible for your own security and safety – do not accept the device or product is secure and safe by definition – you must be knowledgeable about how to secure the product before you use it!
- You must realize that no device or product used to access Cyberspace can ever be made 100% secure and safe – there will always be risks!

Of course this is a massive challenge for lectures, teachers and others who do not always have the technical knowledge to protect their environment, and have no clue about the security status of the devices of their learners. The same hold for every institution venturing into Cyberspace.

Therefore, it will help a lot if a school, company or relevant institution, provide a user friendly Manual or Guideline about the specific products which are used and to provide such Manuals and Guidelines to hosts and participants – do not just hope everything will work fine – take responsibility!