In a typical video conference all the participants involved should be properly identified and authenticated in some way or the other. This prevents unauthorized and unwanted people to be part of the conference. Present existing video conferencing systems however, have problems in this area, resulting in some risks. These risks relate precisely to the lack of facilities to properly identify and authenticate participants, making it possible for unwanted/unauthorised participants to join the conference or masquerade as another participant. In this paper a new approach is discussed that can mitigate these risks, by using facial recognition as a means of authentication.

**Authentication, Facial Recognition, Video Conferencing**

I. INTRODUCTION

A video conference is an interactive meeting between 2 or more locations facilitated by simultaneous two-way video and audio transmissions [1]. In the past these “interactive meetings” were mainly used for business meetings, where the participants were very far away from one another. Because of the expense of equipment and service of that time, this resource would only be used if the travel cost exceeded the price of use.

Video conferencing has come a long way from those expensive video conferencing solutions in the past. It has grown to be a cheap and efficient communication tool that is used by many people in the form of Skype [2], MSN messenger and Google Mail Video. As a result of this popularity, the technology has found its way into various environments such as enterprises and other businesses.

As the use of this technology grows in different enterprises and businesses, there will be a need to secure the access to the information that is conveyed during video conferences. The problem with this is that these businesses have employees with different positions and each of these positions have different levels of access to information.

Therefore, there needs to be some mechanism in place that controls who may enter a video conference, according to their access rights. This mechanism should fit over the current infrastructure and should not cause too much inconvenience to the user.

In this paper the infrastructure of a generic video conference will be analysed and potential problems will be pointed out. After this, a proposed solution will then be presented to solve these problems. Finally the paper is concluded with the approach that will be taken to implement this solution.

II. PROBLEMS IN VIDEO CONFERENCES

In an average video conference there are 4 types of components that perform different functions (shown below).

![Diagram of video conference components](image)

**Fig. 1. The components of a generic video conference with more than 2 participants.**

A. Users

These are all the participants in the video conference that contribute or interact, with other users and the facilitator. As seen in the diagram above there are multiple users that need to gain access to this video conference. If one of these users has been compromised, the whole video conference will be compromised. This could lead to information leaking out to an unauthorized third party.

As mentioned before, users typically have different access rights in a company. These access rights are there to prevent employees from seeing each other’s personal information and corporate information. For example, if executives are having a meeting about dismissing some of the staff in the company. You would need to only allow executives into the meeting and not any of the staff that they will be talking about. If it applies in normal situations why shouldn’t it apply to video conferences?

B. Facilitator

The facilitator is a user with more access than the average user. In some cases the users connects to the facilitator directly, instead of through a host making the facilitator also the host and mediator. Typically a facilitator has the ability to provide content to users and controls the direction in which the video conference is going. An example of this would be a lecturer in an e-class that provides the students (users) with notes.

The problem with this is that if a malicious user becomes a facilitator, that user has the ability to halt or delay the video
conference. This could potentially prevent very important meetings from taking place.

Another problem that arises, because of the above mentioned rights, is that if malware is provided in the content, malicious individuals can perform various activities. Some of these activities include, taking over the video conference and even using it to gain access to other conferences!

C. Mediator

The mediator performs the function of monitoring all of the participants in the video conference. It mainly deals with the technical details of a video conference, like setting up sessions and fixing disconnections. The mediator in some cases also performs some minor security.

The problem with this is that the mediator is not always present, because of various reasons such as resource shortages and expense of training. This component is also susceptible to some of the problems that occur for facilitators.

D. Host

This is the component that all of the above connects to, except in case of some peer-to-peer video conferencing systems. This component deals with various functions such as user authentication and administration.

The main problems that occur in this component happen, as a result of the host not being secure enough. These problems lead to incorrect authentication and a lot of the above mentioned problems. This is why the proposed solution (mentioned in the next section) focuses on this component.

III. PROPOSED SOLUTION

Facial recognition, a branch of computer vision [3], has grown to be a stable technology that is used in many applications [4, 5]. This technology has the added advantage of being non-invasive and convenient to the user. Another advantage is that by implementing it, there would be no significant change, to the way the current infrastructure works.

In the previous section, many of the problems mentioned can be attributed to the lack of identification, authentication and authorisation of the participants. So to address these problems, facial recognition is used to identify, authenticate and authorise the participants in the video conference.

For users to enter a video conference they would need to go through a secure authentication and authorisation process to avoid problems such as information loss, masquerading, intruders and unauthorised access. The same processes would also be applied to facilitators and mediators to prevent abuse of their permission rights.

To accommodate the various users that exist in a company, each user would have different access rights, in the facial template database. In a normal case, the user’s face will be checked against this database, when they are joining a video conference. This is done to make sure they may participate in the video conference. Thereafter there will be random tests, to check if the same user is attending the video conference and no one is masquerading as that specific user.

Another step in this proposed solution is to combine some of the mediator security aspects with the host. This allows for the mediator to be optional, but at the same time making sure that the video conference is always secure. This also makes it easier to manage threats, as most of the security is centralised at the host (or the facilitator in the case of peer-to-peer systems).

This introduction of security policies would greatly contribute to the reduction of existing security problems, giving confidence to businesses and enterprises.

IV. APPROACH

To implement this solution, a type of facial recognition algorithm [6] and an example platform (such as Skype) would need to be chosen. The software for the host would then need to be implemented with a matching biometric database. Once this is implemented, the processes of registration, identification, authentication and authorisation would be added to complete the solution. A more detailed approach and solution can be found in my master’s thesis [7].

REFERENCES


Dustin T. van der Haar completed his Bachelor of Science Degree in Information Technology in 2007 and obtained his Honours degree (Cum Laude) the following year in 2008. Dustin is currently busy with his Masters degree at the University of Johannesburg under Prof. Basie von Solms’s supervision.