Interview guide and questionnaire for the research project

Unified Communication Architecture for Social Critical Environments

Introduction

The research overview and background for this interview is described in the *Participant Information and Consent Form* provided to the interviewee. This interview focuses on the requirements of an organisation/individual in the context of social critical environments with the need for Unified Communication (UC). The structure of the research is planned in multiple stages:

1. Work with multiple project participants to discover the specific functional, security and privacy needs with the help of interviews for the UC architecture.

2. After an analysis of the interviews, integrate mechanisms into a prototype architecture to address those needs based on the requirements gathered in the previous stage.

3. Analyse the UC, security, and privacy requirements defined in the previous steps and summarise the findings and conclusions with the help of the prototype and feedback from research participants.

This interview is organised in the following sections:

Scope and limits of the research project

The research prototype architecture should be limited by the following points to narrow down the scope of the research:

- Open source software should be the foundation for the prototype/architecture
- Browser based clients only should be used, no dedicated installable UC client software or specific hardware e. g. room system, special cameras, …
- The prototype architecture should provide the option for on premises or cloud operation
- No integration or interworking with other communication systems like PSTN (public switched telephone network). The architecture should be a closed system to address the security and privacy requirements.

Please review the high-level architecture drawing in the appendix before you start with the interview.

1 Overview

1.1 Please provide an overview of your organisation:

1.1.1 main focus
1.1.2 organisation structure
1.1.3 number of employees
1.1.4 legal status (e. g. NGO, …)
1.1.5 branch locations
1.1.6 geographic area of operation and focus area

1.2 What is your role in your organisation and the correlation to unified communication and the associated security/privacy requirements?

1.3 How many employees does your organisation have and where are the locations of the branch offices or individual contributors?

1.4 What's the estimated ratio between in person (internal/external) only meetings and meetings with participants joining from other locations via telephone, video, …?

1.5 How many participants (organisation internal/external) are typically in a meeting (size of meetings)?

1.6 In which countries are your internal and external meeting communication partners usually based?

1.7 Are the participants internal to your organisation or external (regular or ad-hoc)?

2 Current and future UC feature requirements

2.1 What kind of devices and software are used e. g. laptop with headset and software xyz, smartphone (iPhone, Android based, …) today and you want to use in the future?

2.2 What kind of technology does your organisation use today for (unified) communication e. g. video, audio, content sharing (screen sharing), … and are required in the future ?

List with priority:

2.3 How does your organisation invite/schedule such meetings e. g. Microsoft Outlook calendar invite, e-mail text, SMS…?

2.4 How should the scheduling/invite process look like in the future?

2.5 What are your current pain points around UC e.g. bandwidth requirements, voice quality, scheduling experience, missing video capabilities, lake of authentication….?

2.6 There are common invitation/scheduling methods within UC based on the examples below. Which of the following would be applicable for your organisation, if any?

2.6.1 Personal virtual meeting room (VMR)

A VMR is a per user pre-configured always available conference virtual meeting room. The user (owner) of the VMR can send out the dial-in instructions, for example via e-mail, in a format similar to https://www.milao.org/vmr.php?vmr=123456 and share an optional PIN with the invited party via a different communication channel e.g. telephone call, SMS, letter. The VMR number in this case is static and doesn't change. The PIN can be changed.

2.6.2 Ad-hoc meeting

The ad-hoc meeting is very similar to the personal VMR described above with the main difference that the architecture generates, every time a meeting is organised, a new random VMR number (one-time meeting) with a different optional PIN. These automatically generated dial-in instructions URL + PIN (optional) can be shared with the participants via e-mail or other communication channel.

2.6.3 Calendar based scheduled invite

With the calendar-based scheduling the inviting participant is using a web page to select date and time, meeting subject, and e-mail addresses of the participants. The system generates a meeting similar to the above described ad-hoc meeting and sends out the invite including the join instructions (URL + PIN optional) via email.

2.7 Instant Messaging (IM)

In addition to video and voice, instant messaging provides the capability for the participants to communicate in a separated area of the UC application to exchange text messages in a conference in real time.

2.8 Screen sharing

Screen sharing provides the ability for one of the participants to share the screen of his/her device with the other participants in the same conference. This is often used to share a presentation or other document. This feature doesn't provide remote control capabilities of the desktop or simultaneous collaboration on a document.

2.9 Other features?

3 Security requirements

The listed security requirements in this section are based on examples and focus on the STRIDE threats framework:

- (**S)**poofing
- (**T)**ampering
- (**R)**epudiation
- (**I)**nformation Disclosure
- (**D)**enial of Service
- (**E)**levation of privilege

The letters in brackets at the end of each question highlight the threat(s) with an example. This is not a complete list and should be used as a guideline to receive more examples/requirements for the architecture, which are maybe not considered by the author.

3.1 Is it required to authenticate the scheduler/inviter on the architecture or should they be anonymous (**S, R, E**)?

Example: Without scheduler authentication it can't be ensured the meeting invite comes from a specific person or a person with the authorization to setup a conference.

3.2 Is it required to authenticate the meeting participants during the join process (**S**, **R**)?

Example: Without participant authentication it can't be ensured the invited person is the person joining a specific meeting or is able to decline the attendance.

3.3 What kind of authentication is required e. g. username/password, digital certificate, distributed ID (DID), zero-knowledge authentication, PIN, etc. for the meeting participants and scheduler (**S, R, E**)?

Example: Depending on existing security policy an adequate authentication method should be defined, in case authentication is required. In case of PIN authentication, it needs to be ensured the URL and especially the PIN is communicated to the participants securely, most of the time via e-mail which can't be ensured all the times.

3.4 Is it feasible that every participant (internal/external) could be authenticated via digital certificates (PKI), which would require a proper certificate management in place for ALL participants (**S, R, E**)?

Example: Digital certificates are widely deployed, but come with the burden of enrolling, withdrawing, storing, and renewing them (certificate management) for internal and more complex for external individuals.

3.5 Is encryption of the scheduling, signalling, and media data required (**I, T**)?

Example: If the data is not encrypted the video and audio for example can be eavesdropped or modified by somebody between the communication participants (man in the middle attack).

3.6 How important is the availability of the system (**D**)?

Example: An attacker could overload the bandwidth capacity to the architecture and cause bad audio/video quality or even make the service unavailable. Would an outage of a certain period of time be accepted and what's the acceptable period?

3.7 Other security requirements?

4 Privacy requirements

The listed privacy requirements in this section are based on examples and focus on the LINDDUN framework:

- **(L)**inkability
- **(I)**dentifiability
- **N**on-(**re**)pudiation
- **(De)**tectability
- **(Di)**sclosure of information
- Content (**U)**nawareness
- Policy and consent **N**on-(**co**)mpliance

The letters in brackets at the end of each question highlights the privacy properties with an example. This is not a complete list and should be used as a guideline to receive more examples/requirements for the architecture, which are maybe not considered by the author.

4.1 What are the requirements for the trust between conference participants? Would a "Web-of-trust" approach be appropriate (**I, L, re**)?

Example: It is required for participants to meet at least once in person to exchange for example a password, PIN, or enrol a digital certificate.

4.2 Is it required to prevent the linkability of the participants of a meeting or successive meetings (**L**)?

Example: In a meeting with several participants it is possible to link the relation to each other by using the same invite information (e. g. https://www.milao.org/vmr.php?vmr=123456) for the meeting.

4.3 Should it be possible to identify the meeting participants inside the meeting and during the invite process/scheduling (**L, I**)?

Examples: The real name of the participant is shown in the video layout next to the person and can be associated and identified. The meeting invites are sent out via e-mail and the real name is used for the e-mail addresses. This is a threat to anonymity and pseudonymity.

4.4 What kind of information should be deleted after which period of time from the architecture (**L, I, re, Di, U, co**)?

Example: The architecture will store some privacy sensitive information to process meetings in various places e. g. log files, scheduling database. This information can be: IP addresses, e-mail addresses, participant names, scheduling times, meeting duration, scheduling information (who has been invited, subject, date and time of meeting), etc.

4.5 Should there be a central directory/address book for the scheduler to look up (recurring/internal) participants during the invite process? What kind of information should be stored e. g. e-mail address, telephone number, real name, pseudonym, … (**L, I, co**)?

Example: For the scheduler it would be easier to invite the participants, if their details are stored centrally and could be selected.

4.6 Is it required to scramble the voice of all or some of the participants of a meeting (**L, I**)?

Example: In a meeting the voice of a victim of torture needs to be modified (scrambled) to protect the individual.

4.7 Is it required to avoid the evidence that a participant attended a meeting (**re**)?

Example: It can be proven that a participant attended a specific meeting with a sensitive topic.

4.8 Is it required not to detect that a meeting happened (**De**)?

Example: It can be proven a video conference occurred based on the IP traffic patterns. A cloud-based operation of the architecture could be used to hide the location and origin of the architecture operator.

4.9 What is the role and required trust level of the administrator of the architecture (**L, I, re, De, Di**)?

Example: Administrators may have access to the architecture, log and configuration files, and scheduling information.

4.10 Should the participants' private information be protected so that it cannot be disclosed without the participants' awareness (**U**)?

Example: A conference participant could use his/her real name and is not aware this information is exposed. Pseudonyms could be enforced for participants instead of real names.

4.11 Is it required that all meeting participants to agree to a data processing agreement before they can join the meeting and what should be the content of the agreement **(U, co)?**

Example: As soon as a meeting participant tries to join the meeting there is an agreement page the user needs to agree to or the connection will not be established.

4.12 Other privacy requirements?

5 Appendix

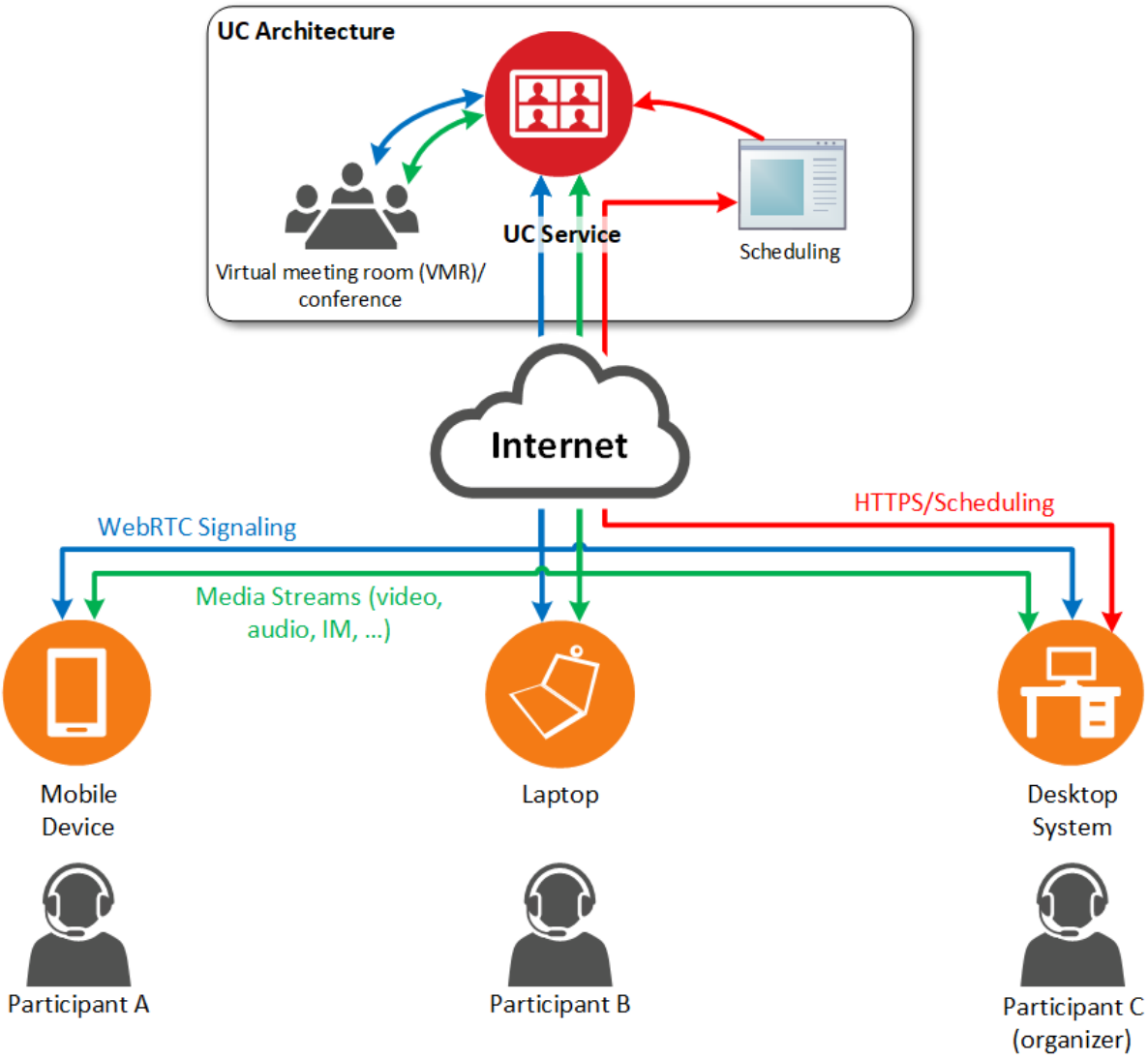

Figure 1 High Level Architecture Drawing