Real-time Transport Protocol

Real-time transport protocol, including RTP, RTCP and SRTP. The Real-time Transport Protocol (RTP) defines a standardized packet format for delivering audio and video over IP networks. RTP is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications, television services and web-based push-to-talk features.

RTP is used in conjunction with the RTP Control Protocol (RTCP). While RTP carries the media streams (e.g., audio and video), RTCP is used to monitor transmission statistics and quality of service (QoS) and aids synchronization of multiple streams. RTP is one of the technical foundations of Voice over IP and in this context is often used in conjunction with a signaling protocol such as the Session Initiation Protocol (SIP) which assists in setting up connections across the network.

The Secure Real-time Transport Protocol (or SRTP) defines a profile of RTP (Real-time Transport Protocol), intended to provide encryption, message authentication and integrity, and replay protection to the RTP data in both unicast and multicast applications.

# Specifications

The following specifications are included in the scope of work. The inclusions and exclusions sections provide more detailed lists of specific features that will be included or excluded from the project scope.

**RFC3550**

RTP: A Transport Protocol for Real-Time Applications

**RFC3551**

RTP Profile for Audio and Video Conferences with Minimal Control

**RFC2833**

RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals

**RFC4867**

RTP Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs

**RFC3952**

Real-time Transport Protocol (RTP) Payload Format for internet Low Bit Rate Codec (iLBC) Speech

**RFC3711**

The Secure Real-time Transport Protocol (SRTP)

**ITU-T T.38**

Procedures for real-time Group 3 facsimile communication over IP networks

**3GPP TS 26.101**

Mandatory speech codec speech processing functions; Adaptive Multi-Rate (AMR) speech codec frame structure

**3GPP TS 26.201**

Speech codec speech processing functions; Adaptive Multi-Rate - Wideband (AMR-WB) speech codec; Frame structure

**3GPP TS 26.114**

IP Multimedia Subsystem (IMS); Multimedia telephony; Media handling and interaction

**GSMA IR.92**

IMS Profile for Voice and SMS

## Specifications not Directly Used

The following specifications were provided by Huawei, but do not directly apply to the features required by the fuzzer. They will not be used to build the fuzzer outside of an understanding of the data sets required to gain coverage of these areas.

**RFC3951**

Internet Low Bit Rate Codec (iLBC)

**ITU-T G.711**

Pulse code modulation (PCM) of voice frequencies

**ITU-T G.729**

Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)

**ITU-T G.722**

7 kHz audio-coding within 64 kbit/s

**ITU-T G.723.1**

Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s

**3GPP TS 26.071**

Mandatory speech CODEC speech processing functions; AMR speech Codec; General description

**3GPP TS 26.090**

Mandatory Speech Codec speech processing functions; Adaptive Multi-Rate (AMR) speech codec; Transcoding functions

**3GPP TS 26.091**

Mandatory Speech Codec speech processing functions; Adaptive Multi-Rate (AMR) speech codec; Error concealment of lost frames

**3GPP TS 26.092**

Mandatory speech codec speech processing functions; Adaptive Multi-Rate (AMR) speech codec; Comfort noise aspects

**3GPP TS 26.094**

Mandatory speech codec speech processing functions; Adaptive Multi-Rate (AMR) speech codec; Voice Activity Detector (VAD)

**3GPP TS 26.171**

Speech codec speech processing functions; Adaptive Multi-Rate - Wideband (AMR-WB) speech codec; General description

**3GPP TS 26.190**

Speech codec speech processing functions; Adaptive Multi-Rate - Wideband (AMR-WB) speech codec; Transcoding functions

**3GPP TS 26.191**

Speech codec speech processing functions; Adaptive Multi-Rate - Wideband (AMR-WB) speech codec; Error concealment of erroneous or lost frames

**3GPP TS 26.192**

Speech codec speech processing functions; Adaptive Multi-Rate - Wideband (AMR-WB) speech codec; Comfort noise aspects

**3GPP TS 26.194**

Speech codec speech processing functions; Adaptive Multi-Rate - Wideband (AMR-WB) speech codec; Voice Activity Detector (VAD)

# Inclusions

The following items will be included in the scope of work:

* RTP
* RTCP
* SRTP
* Profiles defined in specifications that operate over RTP, RTCP and SRTP

# Exclusions

The following items will not be included in the scope of work:

* Any feature not directly exposed over RTP, RTCP and SRTP.
* Specification referenced, but not directly included in the list of specifications in this document.

# Schedule

|  |  |  |  |
| --- | --- | --- | --- |
| Who | Type | What | When |
| Déjà vu Security | Deliverable | Scope document |  |
| Huawei | Deliverable | Approve scope document |  |
| Huawei | Deliverable | Protocol captures |  |
| Huawei | Deliverable | Test environment |  |
| Déjà vu Security | Work | Verify test environment and protocol captures | 2 day |
| Déjà vu Security | Deliverable | Schedule work |  |
| Déjà vu Security | Work | Build | 9 weeks |
| Déjà vu Security | Work | Test | 2 week |
| Déjà vu Security | Deliverable | Pit, user guide |  |
| Huawei | Deliverable | Accept deliverable | 1 week |

## Hours Breakdown

|  |  |
| --- | --- |
| Work Item | Hours |
| Verify test environment and protocol captures | 2 day |
| Build Pit | 45 days |
| Test Pit | 10 days |
| Acceptance Testing | 3 days |
| TOTAL HOURS | 60 days |

# Deliverables

The following sections provide a detailed description of each major deliverable.

## Protocol Captures (Huawei)

Huawei will provide protocol captures in the PCAP format suitable for loading into Wireshark. The protocol captures must include examples of each protocol feature to be fuzzed. This includes all items in the inclusions section of this document. Multiple captures can be provided showing different features.

The protocol captures must be provided prior to work starting.

## Test Environment (Huawei)

Huawei will provide a work test environment for validation of the fuzzing definition. If the protocol is supported, Huawei will provide a configuration for the Deja vu Security's lab containing two Huawei AR series routers.

This environment must be provided prior to work starting.

## Pit, User guide (Déjà vu Security)

Work delivery will be in the form of a ZIP archive containing the following:

* Pit files
  + XML file(s)
  + Configuration file(s)
* Custom extensions
  + Source code
  + Binaries (when applicable)
* PDF User guide document
  + Lists RFCs
  + Inclusions/exclusions
  + Example configuration/usage based on test environment provided
  + Descriptions of all parameters
  + Descriptions of all pits (when more than one is delivered)
  + Description of any custom extensions