M3UA

M3UA is a protocol for supporting the transport of any SS7 MTP3-User signalling (e.g., ISUP and SCCP messages) over IP using the services of the Stream Control Transmission Protocol. Also, provision is made for protocol elements that enable a seamless operation of the MTP3-User peers in the SS7 and IP domains. This protocol would be used between a Signalling Gateway (SG) and a Media Gateway Controller (MGC) or IP-resident Database, or between two IP- based 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.

**RFC4666**

Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) - User Adaptation Layer (M3UA)

# Inclusions

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

* Messages sent to the IPSP

# Exclusions

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

* SS7 MTP3-User Part messages (e.g., ISUP, SCCP, TUP, etc.)

# 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 | 1 day |
| Déjà vu Security | Deliverable | Schedule work |  |
| Déjà vu Security | Work | Build | 3 weeks |
| Déjà vu Security | Work | Test | 1 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 | 1 day |
| Build Pit | 15 days |
| Test Pit | 5 days |
| Acceptance Testing | 2 days |
| TOTAL HOURS | 23 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.

To capture packets on the Windows Loopback adapter, the RawCap[[1]](#footnote-1) tool can be used.

If the protocol captures are not possible, the raw binary data is also acceptable. If provided in this manor, each message will be in a separate file. Each sequence of messages that would normally be considered a single capture will be considered a GROUP. In each group a SEQuence of messages will be sent between two parties (FROM, TO). Additionally each message sent will have some MESSAGE TYPE, or description. The MESSAGE TYPE defined in the RFC should be used.

*GROUP\_SEQ\_FROM\_TO\_MESSAGE\_TYPE.bin*

GROUP – Which capture set this belongs to

SEQ – Sequence number of message

FROM – Who sent the message

TO – Who message was sent to

MESSAGE\_TYPE – Message type/description

Examples:

01\_01\_CLIENT\_SERVER\_ASP\_Up.bin

01\_02\_SERVER\_CLIENT\_ASP\_Up\_Ack.bin

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

1. http://www.netresec.com/?page=RawCap [↑](#footnote-ref-1)