SSH File Transfer Protocol

The SSH File Transfer Protocol provides secure file transfer functionality over any reliable data stream. It is the standard file transfer protocol for use with the SSH2 protocol.

# 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.

**SSH File Transfer Protocol, Draft 02, October 2001**

SSH File Transfer Protocol[[1]](#footnote-1)

# Inclusions

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

* All messages included in version 3, draft 2 of the protocol
* The pit will test an SSH FTP server only

# Exclusions

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

* Messages send from server to client
* All other portions of the SSH protocol including, but not limited to:
  + SSH Authentication Protocol
  + SSH Transport Layer Protocol
  + SSH Connection Protocol

# 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 | 4 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 | 2 day |
| Build Pit | 20 days |
| Test Pit | 5 days |
| Acceptance Testing | 2 days |
| TOTAL HOURS | 28 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

1. This version of the protocol has been selected as the basis for restarting the draft process. It’s unclear as to the support of other versions of the protocol, the most current of which is version 6. [↑](#footnote-ref-1)