

ScreenView Protocol

Josh Brown

July 25, 2022

Abstract

ScreenView is a suite of cryptographical and application level networking protocols culminating in a zero configuration end to end encrypted remote screen viewing and controlling software. ScreenView aims to replace TeamViewer, RDP, and VNC for many use cases while being more performant and more secure. ScreenView requires little set up and is just as easy or easier to set up than other solutions. ScreenView defines four different layers of protocols, each encapsulating all the layers below it. Cryptography for communication between peers and the server is based upon TLS 1.3 and Wireguard. End-to-end cryptography used for ALL communication between peers is based upon TLS-SRP. ScreenView end-to-end cryptography prevents man-in-the-middle attacks even if the intermediary server is compromised, unlike TeamViewer. Screen data is sent over UDP to achieve superior performance than TCP based solutions such as VNC. All UDP packets must be authenticated with keys established over TCP before a response is made by the server preventing amplification attacks. A congestion control mechanism is used to handle low bandwidth and poor networking conditions. Finally, ScreenView supports advanced use cases including file transfer, multiple displays, sharing specific windows, shared whiteboards, and clipboard transfer.

Contents

1	Definitions	4
1.1	Cryptographical Definitions	4
2	Introduction	5
2.1	Application Layers	5
3	Server Encryption Layer (SEL)	5
3.1	TCP	5
3.2	UDP	6
3.2.1	Transport Data Key Derivation	6
3.2.2	Transport Data Messages	6
4	ScreenView Server Communication (SVSC) Protocol	7
4.1	Definitions	7
4.2	Handshake	7
4.2.1	ProtocolVersion	7
4.3	Leasing	7
4.3.1	LeaseRequest	8
4.3.2	LeaseResponse	8
4.3.3	LeaseExtensionRequest	8
4.3.4	LeaseExtensionResponse	9
4.3.5	ID Generation	9
4.3.6	Rate Limits	9
4.3.7	Cookie Value	10
4.4	Sessions	10
4.4.1	EstablishSessionRequest	10
4.4.2	EstablishSessionResponse	10
4.4.3	EstablishSessionNotification	11
4.4.4	SessionEnd	11
4.4.5	SessionEndNotification	11
4.4.6	SessionDataSend - TCP/UDP	12
4.4.7	SessionDataReceive - TCP/UDP	12
4.5	Keepalive - TCP/UDP	12
5	Weak Pre Shared Key, Key Authentication (WPSKKA) Protocol	13
5.1	Handshake	13
5.1.1	KeyExchange	13
5.1.2	AuthScheme	13
5.1.3	TryAuth	14
5.1.4	AuthMessage	14
5.1.5	AuthResult	14
5.2	Transport Data Key Derivation	14
5.3	Subsequent Messages: Transport Data Messages	15
5.3.1	TCP	15

5.3.2	UDP	15
5.4	SRP Dynamic/SRP Static	16
5.4.1	HostHello	16
5.4.2	ClientResponse	16
5.4.3	HostVerify	17
5.5	Public Key (3)	17
6	Remote Visual Display (RVD) Protocol	17
6.1	Definitions	17
6.2	Handshake	18
6.2.1	ProtocolVersion - TCP	18
6.2.2	Unreliable Authentication - UDP	18
6.2.3	HandshakeComplete - TCP	19
6.3	Control messages	19
6.3.1	PermissionsUpdate - TCP	19
6.3.2	DisplayShare - TCP	20
6.3.3	DisplayShareAck - TCP	20
6.3.4	DisplayUnshare - TCP	20
6.3.5	MouseLocation - TCP/UDP	21
6.3.6	MouseHidden - TCP/UDP	21
6.4	Input	21
6.4.1	MouseInput - TCP/UDP	21
6.4.2	KeyInput - TCP/UDP	22
6.5	Clipboard	22
6.5.1	ClipboardRequest - TCP	22
6.5.2	ClipboardNotification- TCP	23
6.6	FrameData - UDP	24

1 Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#).

1.1 Cryptographical Definitions

Based on [Wireguard](#):

ϵ represents an empty zero-length bitstring

DH(PRIVATE KEY, PUBLIC KEY) Curve25519 point multiplication of private key and public key, returning 32 bytes of output.

DH-GENERATE() Generates a random Curve25519 private key and derives its corresponding public key, returning a pair of 32 bytes values, (private, public).

AEAD(KEY, COUNTER, PLAIN TEXT, AUTH TEXT) ChaCha20Poly1305 AEAD, as specified in [RFC7539](#), with its nonce being composed of 32 bits of zeros followed by the 64-bit little-endian value of counter.

HASH(INPUT) BLAKE3(input), returning 32 bytes of output.

HMAC(KEY, INPUT) Hmac-BLAKE3(key, input), the ordinary BLAKE3 hash function used in an HMAC construction, returning 32 bytes of output.

KDF_n(KEY, INPUT) returns an n-tuple of 32 byte values from [HKDF](#) with Hash function.

2 Introduction

This section describes the high level overview of ScreenView. Terms used in this section are defined in other sections.

2.1 Application Layers

The table belows is an abstract diagram of the different layers of ScreenView. Each layer encapsulates all the below layers.

Transport Layer
Server Encryption Layer
Server Communication Layer
E2EE (Peer ↔ Peer) Encryption Layer
Host ↔ Client Communication Layer

The Transport Layer is the OSI Transport Layer level protocol for networking (TCP or UDP). The [Server Encryption Layer](#) provides security between the Server and a Peer. [The Server Communication Layer](#) facilities communication between Peers and the Server. The [E2EE \(Peer ↔ Peer\) Encryption Layer](#) provides end-to-end encryption between a Peer and another Peer. The [Host ↔ Client Communication Layer](#) facilities communication between a Peer and another Peer.

3 Server Encryption Layer (SEL)

SEL provides security for communication between Peers and the Server. TCP and UDP have different security methods. UDP encryption depends on secrets established in the SVSC protocol and therefore can only be begin after TCP encryption is already established.

3.1 TCP

The TCP SEL is TLS 1.3 as defined in [RFC8446](#). TLS v1.3 MUST be used. Previous versions of TLS MUST NOT be used.

The Client initiates a TLS connection with the Server in accordance with [RFC8446](#). All subsequent SEL TCP communications occurs over TLS:

Peer ↔ Server		
Bytes	Name	Value
2	data-length	
1	type	1
<i>data-length-1</i>	data	

3.2 UDP

UDP encryption and authentication rely on the *session-id*, *peer-id* and *peer-key* values established in a session (described in 4.4). The Server (nor the Peer) MUST NOT process or reply to any messages that don't pass authentication. This prevents an amplification attack.

3.2.1 Transport Data Key Derivation

The Server and Peer derive keys.

$G := \text{session-id}$

$H := \text{peer-id}$

$J := \text{peer-key}$

$(SU_{peer}^{send} = SU_{serv}^{recv}, SU_{peer}^{recv} = SU_{serv}^{send}) := \text{KDF}_2(\text{HASH}(G || H || J), \epsilon)$

$NU_{peer}^{send} = NU_{serv}^{recv} = NU_{peer}^{recv} = NU_{serv}^{send} := 0$

3.2.2 Transport Data Messages

Peer \rightarrow Server		
Bytes	Name	Value
2	data-length	
1	type	2
16	<i>peer-id</i>	
8	counter	
remaining bytes	data	

Server \rightarrow Peer		
Bytes	Name	Value
2	data-length	
1	type	3
8	counter	
remaining bytes	data	

$\text{data} := \text{AEAD}(SU_m^{send}, NU_m^{send}, P, \epsilon)$

$\text{counter} := NU_m^{send}$

$NU_m^{send} := NU_m^{send} + 1$

Where P is the payload to be transported

NU_m is an 64 bit counter that MUST NOT wrap. After a transport message is sent, if NU_m equals $(2^{64} - 1)$ the TCP connection MUST be dropped. Subsequent UDP messages MUST NOT be sent.

4 ScreenView Server Communication (SVSC) Protocol

The SVSC protocol is the Server Communication Layer protocol used for Peers to interact with the relay server, Server. Peers can lease an ID as well as begin a session with another Peer. Once a session is established, Peers can forward messages to another Peer. Unless otherwise noted, all messages **MUST** occur over TCP.

All SVSC messages' first byte contain a number to indicate the message type.

4.1 Definitions

- Peer - denotes a client in classical server/client environment
- Server - The intermediary server used for routing and proxying data between two Peers

4.2 Handshake

4.2.1 ProtocolVersion

Handshaking begins with the Server sending the Peer a ProtocolVersion message. This lets the server know the version supported by the Host. the ProtocolVersion message consists of 12 bytes interpreted as a string of ASCII characters in the format "SVSC xxx.yyy" where xxx and yyy are the major and minor version numbers, padded with zeros.

Server → Peer		
Bytes	Name	Value
1	type	0
11	version	"SVSC 001.000"

The Peer replies either 0 to indicate the version is not acceptable and that the handshake has failed or 1 if the version is acceptable to the Peer and the handshake as succeeded. If 0 is sent, all communication **MUST** cease and the TCP connection **MUST** be terminated.

Peer → Server		
Bytes	Name	Value
1	type	1
1	ok	0 or 1

4.3 Leasing

A lease is a temporary assignment of an ID to a Peer. The ID format and generation is discussed in [4.3.5](#). A maximum of 1 ID can be leased per TCP connection. ID generation **MUST** be rate limited to prevent ID exhaustion. Rate limiting rules are out of scope for this protocol, however some suggestions are listed in [4.3.6](#).

4.3.1 LeaseRequest

A *LeaseRequest* message requests a lease of an ID.

Peer → Server		
Bytes	Name	Value
1	type	2
1	has-cookie	0 or 1
Below only if <i>has-cookie</i> is 1		
24	cookie	

If a Peer would like to request an ID it had previously been issued after expiration, it may include the cookie value it received in the LeaseResponse. There is no guarantee that the Peer will receive the same ID or that the Server will even consider the cookie value.

4.3.2 LeaseResponse

A LeaseResponse message is a response to a LeaseRequest. If has-cookie is 1, a Server MAY consider the cookie value in LeaseRequest or completely ignore it.

Server → Peer		
Bytes	Name	Value
1	type	3
1	accepted	0 or 1
Below only if <i>accepted</i> is 1		
4	id	
24	cookie	
8	expiration	

expiration is a 64 bit Unix timestamp representing the expiry of lease. Disconnection of a Peer (e.g, the TCP connection is dropped) does not end a lease.

cookie a 128 bit value. The generation of this value is discussed in 4.2 .7.

Consideration of the cookie value MUST have no effect on the the value of accepted. That is, if the request is for a specific ID (implied by the presence of a cookie value and a has-cookie value equal to 1 in the LeaseRequest) and the ID requested is not available, the Server SHOULD respond with a different available ID and an accepted value of 1 (assuming an ID is available). accepted MUST only be 0 if no IDs are left, for rate limiting reasons, or some other reasons unrelated to the cookie value.

4.3.3 LeaseExtensionRequest

A LeaseExtensionRequest message is used to extend a lease. Before a lease has expired, the Peer can request a lease extension. The Server can accept or deny this request. The Peer SHOULD send this message no earlier than as soon as 50 percent of the lease duration has expired.

Peer → Server		
Bytes	Name	Value
1	type	4
24	cookie	

4.3.4 LeaseExtensionResponse

A LeaseExtensionResponse message is a response to a LeaseExtensionRequest.

Server → Peer		
Bytes	Name	Value
1	type	5
1	extended	0 or 1
Below only if <i>extended</i> is 1		
8	new-expiration	

new-expiration is a 64 bit Unix timestamp representing the expiry of lease.

4.3.5 ID Generation

An ID is a 26 to 33 bit decimal number. This comes out to about up to 8 to 10 decimal digits, respectively. The Server may scale the keyspace depending on current usage. For optimal user experience while maintaining efficiency, the Server **MUST** only use keyspaces between 26 bits and 33 bits for ID generation. ID generation must also be uniformly random. All active IDs must be stored on the server. New IDs **MUST** be unique. ID generation **MAY** occur using the below algorithm:

Let S represents a set of all active IDs, B be a number of bits between 26 and 33, and $generate(x)$ be a functions that returns a x uniformly random bits.

Algorithm 1 ID generation

```

id
repeat
     $id \leftarrow generate(B)$ 
until  $id \notin S$ 
 $S \leftarrow S \cup \{id\}$ 
return  $id$ 

```

4.3.6 Rate Limits

To prevent ID exhaustion, rate limits **SHOULD** be in place. TCP is used for LeaseRequests so IP addresses can not be spoofed. However, using proxy services such as Tor, simple IP based rate limits are likely not entirely sufficient. Servers **MAY** want to block all known proxy IP addresses.

4.3.7 Cookie Value

A *cookie* value is a 128 bit value used for authentication in LeaseExtensionRequest and LeaseRequest messages. Specific generation of a cookie is out of scope, however care must be taken to ensure it is not predictable or exploitable. This value MAY be simply a random 24 byte key, HMAC-SHA1(*id*, *key*) || *id*, or something else entirely.

4.4 Sessions

A session is a connection between two Peers. At least one Peer must have an ID. A Peer can have a maximum of one session at any time. Immediately after receiving a EstablishSessionResponse message with a status of 0 or a EstablishSessionNotification message a Peer MUST establish UDP connection by sending a Keepalive message as defined in 4.5. Failure to do so MAY result in dropped SessionData* packets.

4.4.1 EstablishSessionRequest

An EstablishSessionRequest message is a Peer request to establish a session with another Peer.

Client → Server			
Bytes	Name	Value	Description
1	type	6	
4	lease-id		The ID of the Peer to establish this connection with

4.4.2 EstablishSessionResponse

An EstablishSessionResponse message is a response to EstablishSessionRequest.

Server → Client			
Bytes	Name	Value	Description
1	type	7	
4	lease-id		the ID of the Peer attempted to connect to
1	status	0-5	described below
Below only if <i>status</i> is 0			
16	session-id		described below
16	peer-id		described below
16	peer-key		described below

status can have the following values:

Value	Description
0	session establishment was successful
1	ID not found
2	Peer is offline
3	Peer is busy
4	You are busy
5	Other error

A Peer may be considered offline if, for example, an unexpired ID has been assigned to them and then the TCP connection is dropped.

session-id is a 128 bit random value used for session identification

peer-id is a 128 bit random value used to authentication a Peer for a given session. A Peer's peer-key MUST never be revealed to anyone but the Peer it belongs to (and the Server that generated it) for security reasons.

4.4.3 EstablishSessionNotification

A EstablishSessionNotification notifies a Peer that a session has been established with them.

Server → Host			
Bytes	Name	Value	Description
1	type	8	
16	session-id		described in 4.4.2
16	peer-id		described in 4.4.2
16	peer-key		described in 4.4.2

peer-id and peer-key are the id and key of the Peer being notified NOT the id and key of the Peer they are connecting to.

4.4.4 SessionEnd

A SessionEnd message is used to terminate a session. Once a Server receives a SessionEnd message, the Server MUST immediately stop forwarding messages and send a SessionEndNotification to the other Peer. The Peer must ignore any SessionDataPacket message received after this.

Peer → Server			
Bytes	Name	Value	Description
1	type	9	

4.4.5 SessionEndNotification

A SessionEndNotification notifies a Peer that a session has ended. If a Peer sends a SessionEnd message, the Server MUST send a SessionEndNotification message

to a Peer. The Peer must ignore any SessionDataPacket message received after this

Server → Peer			
Bytes	Name	Value	Description
1	type	10	

4.4.6 SessionDataSend - TCP/UDP

A SessionDataSend is a message from a Peer intended to be forwarded to the Peer on the other side of the session. If a connection is not available (e.g. UDP was dropped or never established) for SessionDataReceive message to be sent to the other Peer, the SessionDataSend message is silently dropped.

Peer → Server			
Bytes	Name	Value	Description
1	type	11	
remaining-bytes	data		data to be forwarded

4.4.7 SessionDataReceive - TCP/UDP

A SessionDataReceive is a message being forwarded to a Peer from the Peer on the other side of the session. The Server SHOULD forward the message along the same transport as it was received.

Server → Peer			
Bytes	Name	Value	Description
1	type	12	
remaning-bytes	data		data to be forwarded

4.5 Keepalive - TCP/UDP

For each transport (TCP and UDP), if no message has been sent in KeepaliveTimeout a Server sends a keepalive message over the respective transport. The Peer MUST respond with another Keepalive message.

For TCP, if a KeepaliveTimeout response is not received by the Server in double KeepaliveTimeout seconds the TCP connection is considered dropped.

For UDP, if a KeepaliveTimeout response is not received by the Server in half KeepaliveTimeout seconds another Keepalive message is sent. If a response is not received in an additional half KeepaliveTimeout seconds, the UDP connection is considered dropped.

Server ↔ Peer		
Bytes	Name	Value
1	type	13

5 Weak Pre Shared Key, Key Authentication (WPSKKA) Protocol

The WPSKKA protocol is the E2EE Encryption layer protocol used to communicate between Peers. All WPSKKA messages' first byte contain a number to indicate the message type.

5.1 Handshake

The handshake begins with a key exchange. The Host sends its ephemeral public key in a KeyExchange message. The Client replies with its ephemeral public key KeyExchange message. Then the Host offers to the Client a list of available authentication schemes. The goal of WPSKKA is to authenticate the Peers' ephemeral keys through one of those schemes.

5.1.1 KeyExchange

The Host and Client exchange their ephemeral public keys.

Host ↔ Client		
Bytes	Name	Value
1	type	1
32	public-key	

5.1.2 AuthScheme

Once the Host receives the Client's public key, it sends the Client a list of authentication schemes it supports.

Host → Client		
Bytes	Name	Value
1	type	2
1	num-auth-schemes	
num-auth-schemes	auth-schemes	

num-auth-schemes is the number of auth schemes. auth-schemes contains 1 byte per auth-scheme to indicate which authentication scheme is available. Authentication schemes are defined below.

Authentication Schemes	
Number	Name
0	None
1	SRP Dynamic
2	SRP Static
3	Public key

5.1.3 TryAuth

The TryAuth messages indicates a Client would to attempt authentication with a particular auth scheme.

Client → Host		
Bytes	Name	Value
1	type	3
1	auth-scheme-number	

auth-scheme-number is the authentication scheme the Client would like to attempt. If the Host does not support the auth-scheme-number sent by the Client, the Host MUST send a failed AuthResult message.

5.1.4 AuthMessage

Messages used in the authentication scheme are encapsulated in this message.

Host ↔ Client		
Bytes	Name	Value
2	length	
1	type	4
length-1	auth-message	

5.1.5 AuthResult

The AuthResult message indicates the result of the authentication attempt. A successful authentication result MUST only be sent once.

Host → Client		
Bytes	Name	Value
2	length	2
1	type	5
1	ok	0 or 1

ok indicates whether the authentication method was successful (1) or failed (0). If the authentication method failed, the Client MAY attempt another authentication scheme or try the same one again by sending a TryAuth message.

5.2 Transport Data Key Derivation

$$C_{host} = \text{DH}(E_{client}^{pub}, E_{host}^{priv})$$

$$C_{client} = \text{DH}(E_{host}^{pub}, E_{client}^{priv})$$

$$(ST_{host}^{send} = ST_{client}^{recv}, ST_{host}^{recv} = ST_{client}^{send}, SU_{host}^{send} = SU_{client}^{recv}, SU_{host}^{recv} = SU_{client}^{send}) := \text{KDF}_4(C_{host} = C_{client}, \epsilon)$$

$$NT_{host}^{send} = NT_{client}^{recv} = NT_{host}^{recv} = NT_{client}^{send} = NU_{host}^{send} = NU_{client}^{recv} = NU_{host}^{recv} = NU_{client}^{send} := 0$$

ST keys and NT nonces are used for TCP. SU keys and TU nonces are using for UDP.

5.3 Subsequent Messages: Transport Data Messages

Transport Data Messages MUST NOT be sent until authentication is complete.

5.3.1 TCP

Host ↔ Client		
Bytes	Name	Value
2	data-length	
1	type	6
remaining bytes	data	

$$\text{data} := \text{AEAD}(ST_m^{\text{send}}, NT_m^{\text{send}}, P, \epsilon)$$

$$\text{counter} := NT_m^{\text{send}}$$

$$NT_m^{\text{send}} := NT_m^{\text{send}} + 1$$

Where P is the payload to be transported.

NT_m is an 64 bit counter that MUST NOT wrap. After a transport message is sent, if NT_m equals $(2^{64} - 1)$ the UDP and TCP connection MUST be dropped. Subsequent messages MUST NOT be sent.

5.3.2 UDP

Host ↔ Client		
Bytes	Name	Value
2	data-length	
1	type	7
8	counter	
remaining bytes	data	

$$\text{data} := \text{AEAD}(SU_m^{\text{send}}, NU_m^{\text{send}}, P, \epsilon)$$

$$\text{counter} := NU_m^{\text{send}}$$

$$NU_m^{\text{send}} := NU_m^{\text{send}} + 1$$

Where P is the payload to be transported.

NU_m is an 64 bit counter that MUST NOT wrap. After a transport message is sent, if NU_m equals $(2^{64} - 1)$ the UDP and TCP connection MUST be dropped. Subsequent messages MUST NOT be sent.

5.4 SRP Dynamic/SRP Static

SRP relies on SRP as defined in [RFC5054](#) to establish a shared key used to authenticate the ephemeral public keys via a MAC.

The Host will serve as the SRP server, the Client will serve as the SRP client. The password will be created and stored by the Host. This password can be randomly generated (Dynamic) or chosen by the Host (Static). The Host may serve both Dynamic and Static SRP authentication methods. The Client will select which type to use in the TryAuth message.

5.4.1 HostHello

The Host sends a HostHello message to the Client.

Host → Client		
Bytes	Name	Value
1	type	1
16	username	
16	salt	
256	srp-B	

$I := RAND(128)$

$s := RAND(128)$

$B := SRP-B()$

username := I

salt := s

srp-B := B

5.4.2 ClientResponse

Client → Host		
Bytes	Name	Value
1	type	2
256	srp-A	
32	mac	

srp-A := SRP-A()

$L_{client} = L_{host} := SRP-PREMASTER()$

mac := HMAC(KDF₁(L_{client}), public-key)

public-key is the Client's public key

The Host validates the MAC. If the MAC is incorrect a failed MUST be AuthResult is sent.

5.4.3 HostVerify

Host \rightarrow Client		
Bytes	Name	Value
1	type	3
32	mac	

$$\text{mac} := \text{HMAC}(\text{KDF}_1(L_{\text{host}}), \text{public-key})$$

public-key is the Host's public key

After the HostVerify is sent, the Host MUST send a successful AuthResult.

5.5 Public Key (3)

WIP

6 Remote Visual Display (RVD) Protocol

The RVD protocol is used to communicate messages regarding mouse input, keyboard input, frame data, and clipboard data between the Host and the Client.

All messages MUST occur over the transport listed.

All RVD messages' first byte contain a number to indicate the message type.

6.1 Definitions

- Host - A peer with an ID that wants to share their screen to the Client
- Client - A peer that wants to view and maybe control the Host's screen
- Display - A rectangular visual region that is shared by a Host to a Client. May or may not be Controllable.
- Controllable - A Display that accepts keyboard and mouse input from the Client.

6.2 Handshake

6.2.1 ProtocolVersion - TCP

Handshaking begins by the Client sending the Host a ProtocolVersion message. This lets the Host know the version supported by the Host.

The ProtocolVersion message consists of 11 bytes interpreted as a string of ASCII characters in the format "RVD xxx.yyy" where xxx and yyy are the major and minor version numbers, padded with zeros.

Client → Host		
Bytes	Name	Value
1	type	0
11	version	"RVD 001.000"

The Host replies back either 0 to indicate the version is not acceptable and that the handshake has failed or 1 if the version is acceptable to the Client and the handshake has succeeded. If 0 is sent, all communication MUST cease and an error SHOULD be displayed to user. A SessionEnd message should be sent by the Host.

Host → Client		
Bytes	Name	Value
1	type	1
1	ok	0 or 1

6.2.2 Unreliable Authentication - UDP

To prevent UDP amplification attacks, the Host and Client MUST each authenticate each others addresses before sending unreliable messages.

For simplicity and better abstraction, even if an unreliable transport is not being used for the transport or a signal server is used, this section of the protocol MUST be performed.

If unreliable transport is not used, this MUST be performed over the reliable transport.

UnreliableAuthInitial

Client → Host		
Bytes	Name	Value
1	type	2
16	challenge	
16	zero	0

challenge is a random 128 bit value

zero is 128 bits padding with the value 0

UnreliableAuthInter

Host → Client		
Bytes	Name	Value
1	type	3
16	response	
16	challenge	0

response is the 128 bit value received from the Client in the UnreliableAuthInitial message

challenge is a random 128 bit value

UnreliableAuthFinal

Client → Host		
Bytes	Name	Value
1	type	4
16	response	

response is the 128 bit value received from the Host in the UnreliableAuthInitial message

6.2.3 HandshakeComplete - TCP

Finally, the Host sends a HandshakeComplete message to indicate it is ready to receive messages.

Host → Client		
Bytes	Name	Value
1	type	5

6.3 Control messages

Control messages are messages that instruct the Client about changes regarding the Host.

6.3.1 PermissionsUpdate - TCP

The PermissionsUpdate message is sent by the Host to the Client to indicate the permissions. The default permissions are all false.

Host → Client		
Bytes	Name	Value
1	type	6
1	permissions	see below

The bits of permission are defined below in little endian:

Bit	Name
0	clipboard-read
1	clipboard-write
2-7	reserved

6.3.2 DisplayShare - TCP

A DisplayShare message informs the Client about a Display the Host would like to share.

For each DisplayShare sent, an additional DisplayShare with the same display-id MUST NOT be sent until a DisplayUnshare message is sent for that display-id. The Client MUST respond with a DisplayShareAck message with the same display-id. The Host MUST NOT send FrameUpdates for the Display until the Host has received a DisplayShareAck message with the display-id. If the Host does not receive a DisplayShareAck message within 5 seconds, the Host MUST send a DisplayUnshare message for the display-id and consider the Display unshared. The Host MAY try to share again.

If the Host receives a DisplayShareAck message with a display-id that it does not recognize, it MUST ignore it. If the Client receives a DisplayUnshare message with a display-id that it does not recognize, it MUST ignore it.

Host → Client		
Bytes	Name	Value
1	type	7
1	display-id	0-255
1	access	see below
2	name-length	0-255
name-length	name	

The access bits are defined below in little endian:

Bit	Name
0	controllable
1-7	reserved

6.3.3 DisplayShareAck - TCP

The DisplayShareAck message is sent in reply after receiving a DisplayShare message. It indicates to the Host, that the Client is ready to receive FrameData.

Client → Host		
Bytes	Name	Value
1	type	8
1	display-id	0-255

6.3.4 DisplayUnshare - TCP

The DisplayUnshare message is sent by the Host to the Client to indicate that the Display is no longer shared. The Host MUST NOT send FrameUpdates for a Display with this display-id until a new Display with this id has been reshared via the DisplayShare message.

Host → Client		
Bytes	Name	Value
1	type	9
1	display-id	0-255

6.3.5 MouseLocation - TCP/UDP

The *MouseLocation* message send information about where the mouse is currently on the screen. The Host sends this information periodically throughout the session. The Host SHOULD send a *MouseLocation* update when mouse input is received from the Host's system or in reply when it receives a *MouseInput*.

Each shared Display has its own pointer. Each pointer has a visibility state of visible or hidden. Visible pointers are drawn by the Client while hidden pointers are not. Displays begin with a hidden pointer. When a *MouseLocation* message is received, the pointer for the Display (specified by the display-id field) is made visible. When a *MouseHidden* message is received, the pointer for the Display is made hidden.

Host → Client			
Bytes	Name	Value	Description
1	type	10	
1	display-id	0-255	
2	x-location		x coordinate of the mouse
2	y-location		y coordinate of the mouse

6.3.6 MouseHidden - TCP/UDP

Host → Client			
Bytes	Name	Value	Description
1	type	11	
1	display-id	0-255	

6.4 Input

Input messages (including *MouseLocation*) may be sent over TCP or UDP. TCP is preferred in most situations. However, in situations where speed is prioritized over the guarantees TCP provides (such as gaming), UDP can be used.

6.4.1 MouseInput - TCP/UDP

Client → Host

Bytes	Name	Value	Description
1	type	12	
1	display-id	0-255	
2	x-position		x coordinate of the mouse
2	y-position		y coordinate of the mouse
1	button-mask-delta		described below
1	button-mask-state		described below

Indicates either pointer movement or a pointer button press or release. The pointer is now at (x-position, y-position), and the current state of buttons 1 to 8 are represented by bits 0 to 7 of button-mask respectively, 0 meaning up, 1 meaning down (pressed).

On a conventional mouse, buttons 1, 2 and 3 correspond to the left, middle and right buttons on the mouse. On a wheel mouse, each step of the wheel is represented by a press and release of a certain button. Button 4 means up, button 5 means down, button 6 means left and button 7 means right.

button-mask-delta indicates which mouse buttons have state updates (1 indicates a state update). button-mask-state have the actual up or down state. Only state updates for buttons indicated by button-mask-delta should be considered.

6.4.2 KeyInput - TCP/UDP

The *KeyInput* event sends key presses or releases.

Client → Host			
Bytes	Name	Value	Description
1	type	13	
1	down-flag	0 or 1	indicates whether the key is now pressed or released
4	key		"keysym"

Details can be found at the [RFB Spec](#)

6.5 Clipboard

6.5.1 ClipboardRequest - TCP

Used to check if a clipboard type exists on the Host.

Client → Host		
Bytes	Name	Value
1	type	14
1	clipboard-type	
Below only if clipboard-type's first bit is 1		
1	type-name-length	
type-name-length	type-name	

clipboard-type first bit (MSB) indicates whether this request is for a default type (0) or a custom type (1). clipboard-type's second bit (second MSB) indicates whether this request is a exists request (0) or a content request(1). An exists request is for checking whether the type exists but does not return content. A content request returns content if it exists. The remaining bits indicate the default type if the request is for a default type. Otherwise they MUST be 0.

clipboard-type's remaining bits referring to the following default types:

Value	Description
0	text
1	text
2	rtf
3	html
4	file-pointer

6.5.2 ClipboardNotification- TCP

Notifies a Peer of a clipboard update. The receiving Peer should update their clipboard.

Host ↔ Client		
Bytes	Name	Value
1	type	15
1	clipboard-type	
Below only if clipboard-type's first bit is 1		
1	type-name-length	
type-name-length	type-name	
Below always		
1	type-exists	0 or 1
Below only if clipboard-type's second bit is 1 and type-exists is 1		
3	content-length	
<i>content-length</i>	data	zlib'ed raw data

type-exists indicates whether the clipboard type specified exists on sending Peer. If the notification is a response to a request type-exists can be 0 to indicate that type was not found, or 1 to indicate that type was found. If the notification is not a response type-exists SHOULD be 1. type-exists can be 1 and content-length can be 0 if for example the clipboard text type exists, but is currently empty.

clipboard-type, type-name-length, and type-name MUST match a request if the notification is in response. If clipboard-readable is 0 and a Host receives a ClipboardRequest, it MUST be ignored. If no Display is Controllable or clipboard-readable is 0 and a Host receives a ClipboardNotification, it MUST be ignored.

content-length - the length of the content (maximum 2^{24} bytes or 16MB)

6.6 FrameData - UDP

The *FrameData* message contains a single RTP-VP9 or RTCP packet

Host → Client		
Bytes	Name	Value
1	type	16
1	display-id	0-255
2	size	
<i>size</i>	data	