VRI Direct Security Whitepaper

VRI Direct's prime directive is always to provide a secure, trusted environment over which our users can confidently communicate with each other without concern that their conversations will be eavesdropped, their personal information stolen, or their activities monitored by unauthorized individuals. We accomplish this directive through many different best-practice security policies, procedures, and implementations.

User Password Storage

User passwords are salted and then encrypted using National Institute of Standards and Technology (NIST)-approved PBKDF2 key derivation algorithm and SHA512 hashing algorithm. The key derivation algorithm applies the hashing algorithm a minimum of 10,000 times. Pseudo-random, 256-bit salt values are unique to each user password and are regenerated each time a password is created or updated. The resulting derived key length is 64 bytes.

The end result is a securely encrypted, one-way hashed password that cannot be retrieved back into its original form. The practical implication of our password encryption strategy is that nobody can open the database and read the passwords, nor is there a key available to decrypt those password. A user who does not know his or her password must create a new one.

Network Communications

The VRI Direct platform uses encrypted Web traffic and realtime communications traffic. Both traffic types are detailed below.

Web Traffic

All Web traffic is communicated over HTTPS ports secured with standard 256-bit Secure Sockets Layer (SSL) encryption. The SSL certificates used to verify VRI Direct's identity are issued from globally trusted Certificate Authorities (CA), currently RapidSSL, GlobalSign and DigiCert High Assurance CA-3.

We use HTTP Strict Transport Security (HSTS) policy and HTTP security headers (X-XSS-Protection, X-Frame-Options) in combination with server-side settings to help guard against cross-site and cross-frame scripting attacks, and to guarantee that our content originates strictly from HTTPS ports.

These two approaches help prevent hackers from intercepting the traffic and reading the details in the stream. Secure sites such as Google Gmail, Facebook, banking institutions, and many others follow these same strategies.

Realtime Communications

The VRI Direct platform's distributed Realtime Communications Service (RCS) provides secure, encrypted conference call features and manages audio, video and text chat communications across all call participants. RCS security comprises two parts: connection authentication, used to ensure that all parties wishing to connect to the service are authenticated and trusted; and communication security, providing strong encryption and secure transmission of media communications to prevent eavesdropping.

RCS Connection Authentication

The connection between VRI Direct clients and the RCS is authenticated using a shared secret key signing

process. The RCS service and the VRI Direct platform share a private key used by the platform to sign connection requests made by VRI Direct clients. Each client who successfully logs into VRI Direct is assigned a user identifier (UID) within the VRI Direct platform. When a client requests an RCS connection, the VRI Direct platform prepares a connection request by signing the request with the shared secret, then salting the request and creating a SHA-256 signature used to guarantee the connection request. This is then passed to the client, who must then send the signed request to the RCS. The RCS verifies that the signed client request matches the request sent by the VRI Direct platform before authorizing the connection.

RCS Communication Security

Signalling

The RCS transmits all signalling messages over a TLS/TCP data channel using TLS 1.2 encryption. The data itself is encrypted using DHE-RSA-AES256-GCM-SHA384 cyphersuite with 256-bit key encryption. Perfect forward secrecy is achieved in key exchange using Ephemeral Diffie-Hellman. All message authentication is done simultaneously with encryption, producing SHA384 output. SSL version 2 and 3 are explicitly forbidden.

Media Streaming

All media streams are protected using the Secure Realtime Transport Protocol (SRTP). DTLS-SRTP is used to establish encryption keys. Certificates for DTLS are generated by the client and the media streamer; these fingerprints are then exchanged over the secure TLS/TCP signalling channel, where DTLS then uses the certificates to generate the keys used to encrypt the data. These keys are not persisted anywhere. From there, SRTP is used to encrypt and authenticate data packets streamed between all trusted parties; this encryption employs AES CM mode with 128-bit keys for the RTP packet encryption and HMAC SHA1 for the packet authentication and integrity.

The main practical implication of both our RCS connection and RCS communication security approaches is that our system is safe from outside users trying to intercept VRI calls not intended for them.