VNC® Connect security whitepaper

Version 1.4

Contents

Introduction

Customer security is of paramount importance to RealVNC®. As such, our security strategy is ingrained in all aspects of our VNC® Connect software. We have invested extensively in our security, and take great pride in our successful track record.

In order to explain our strategy in more detail, this document is divided into four key topics: security architecture, cloud infrastructure, client security, and development procedures. Each is guided by four simple, but powerful, principles:

- You do not have to trust RealVNC in order to trust our software and services.
- We do not record your sessions, and cannot decrypt session data now or in the future.
- Every session is treated as though it is made in a hostile environment.
- The owner of the remote computer ultimately decides who is able to connect.

The document details the measures we take to ensure VNC Connect remote access sessions are as secure as possible.

Terminology

Device access	A capability built into VNC Connect that enables attended or unattended access to computers you own or manage with VNC Connect installed. More information.
Instant support	A capability built into VNC Connect that enables attended access on demand to computers that do not, or cannot, have VNC Connect installed. More information.
VNC Viewer	A client application that enables you to control a remote computer. It runs on the computer or mobile device you want to control from. In this document, VNC Viewer is also used to refer to “the device on which VNC Viewer runs”
VNC Server	A client application that enables a remote computer to be controlled. If, as part of your VNC Connect subscription, you have: • Device access, then VNC Server (part of the VNC Connect download) must be installed and licensed on remote computers in advance. • Instant support, then VNC Server (in the form of a disposable app) is downloaded just-in-time to remote computers, and does not need to be installed or licensed. In this document, VNC Server is used to indicate the app in either of these ‘modes’, and in addition to “the computer on which VNC Server runs”.
Cloud connection	A remote access session that is brokered by RealVNC cloud services. Where possible, once brokered and secured, the session itself is handled peer-to-peer. If hand-off is not possible, RealVNC cloud services relay session data.
Direct connection	A remote access session that is conducted entirely peer-to-peer, with no communication via RealVNC cloud services at all. It is available only with an Enterprise subscription that includes device access.

Security architecture

Overview

At RealVNC, we make a fundamental security assumption that the connection between VNC Viewer and VNC Server may traverse a hostile environment, and we have built our entire security architecture with this in mind. As such, the security features and strategies described below apply equally to cloud and direct (TCP) connection methods.

When making a cloud connection, RealVNC cloud services only broker approved connections and act as a fallback transport mechanism for encrypted data. They explicitly **do not** enjoy a privileged security position. The ultimate responsibility for authorizing remote access lies solely with VNC Server.

When making a direct connection, VNC Viewer uses a direct TCP connection to VNC Server, performing no interaction with RealVNC cloud services at all. The clients are self-sufficient and do not need access to the Internet. Again, VNC Server is ultimately responsible for granting authorized remote access.

Remote Framebuffer Protocol (RFB)

VNC technology uses the Remote Framebuffer Protocol, an Internet Standard protocol originally created by RealVNC as the first remote desktop protocol. RealVNC continues to actively maintain this, and in June 2015 RFB version 5 was released, designed from the ground up to support cloud connectivity.

RFB 5 mandates the use of modern cipher suites and uses strong cryptography throughout. It is streamlined compared to TLS, making it much less prone to implementation vulnerabilities and misconfiguration. It offers very strong key exchange that is designed for cloud connectivity, by mixing in three sources of key material: the local client, the remote client and the cloud handshake. This puts the clients in full control of encryption keys, preventing tampering.

A detailed security analysis of RFB 5 can be found here.

Encryption

VNC Connect uses AES-GCM encryption to ensure the secrecy and integrity of data while in transit. All VNC Connect subscription types support 128-bit AES encryption. An Enterprise subscription provides an option to increase this to 256-bit AES. All encryption is end-to-end, ensuring no one can read the data in transit, including RealVNC.

Elliptic Curve Diffie-Hellman key exchange adds Perfect Forward Secrecy (PFS) on top of the RSA key exchange used for identity checking (refer to the section *Identity checking*, below). PFS provides a shared secret for each individual connection that can only be recovered while the connection is active, preventing leaked keys from being used to decrypt past or future connections.

Identity checking

The RealVNC identity-checking model allows VNC Viewer to know it is connecting to the correct computer, preventing impersonation. Each client is identified by an RSA key according to two different security models:

- For direct connections, a “Trust on First Use” (TFU) model is employed. In this case, the VNC Viewer user must manually approve each key the first time a connection is made to a new computer. VNC Viewer stores the keys and ensures that they have not changed on reconnection. This guarantees that no one has intercepted the connection.
- For cloud connections, RealVNC cloud services automatically verify identity, meaning the VNC Viewer user need not check the key manually. However, with device access, there is no need for VNC Viewer users to trust this automatic identity verification. Users can perform a manual identity check at connection-time, in order to guarantee our services have not intercepted the connection.

When performing manual identity checking, VNC Server’s identity is presented as an easily recognizable catchphrase. This makes it simple for users to notice changes to the VNC Server key, preventing impersonation. The catchphrase is derived from VNC Server’s RSA key and is a human-readable representation of the key’s fingerprint.

Cloud negotiation process

Cloud connectivity enables easy access to machines through NAT and firewalls. It does this by using an outbound connection to RealVNC cloud services from both VNC Viewer and VNC Server. These services broker the connection, enabling them to exchange IP addresses for peer-to-peer connectivity, and may also relay data in the event that peer-to-peer connectivity is not possible. Once the connection is made, the same RFB security is applied, regardless of the transport mechanism. The clients always assume the transport could be hostile, even if transported through our services. RealVNC has no ability to read or tamper with any connection.

By avoiding the use of inbound TCP or UDP packets, VNC Connect does not require any ports to be opened on your firewall. This prevents unauthenticated access to your network from outside.

Negotiation of peer-to-peer connectivity

When using peer-to-peer connectivity with cloud connections, the standard Interactive Connectivity Establishment procedure (ICE) is employed. This involves opening a UDP port on each client, performing IP address discovery using STUN, and then sending packets directly to the peer. UDP ports are only opened by VNC Server as needed when a connection is made, and are associated with a specific connection, reducing the attack surface to a minimum.

This operates at a lower level than RFB, so a separate security mechanism is used to sign every UDP packet, using a per-connection secret. This prevents attacks against the UDP port and interception of the connection at a lower level than the RFB data. In between the ICE and RFB layers, SCTP is used to add reliability to the data stream.

Independent cloud & VNC Server credentials

Device access

In order to control a remote computer you own or manage via the cloud, you must enter a series of unique authentication credentials:

- First, to discover a computer, you must have been invited to that computer's 'team'.
- Next, you must sign in to VNC Viewer using your RealVNC account credentials for that team.
- Once you have selected a computer, you must enter *its* authentication credentials. By default, VNC Server requests the details normally used to *log in* to that computer, though you can change the authentication scheme or increase the number of factors if you wish (see the section *Multi-factor authentication for VNC Server*, below). Access control lists configured on VNC Server (locally or via policy) determine who can gain remote access, and what actions they can take if access is granted.

Instant support

In order to control a remote computer on demand via the cloud, both you and the owner of that computer must co-operate to enter two sets of authentication credentials.

- First, you must have been invited to a remote access team for which you are explicitly named as a team technician.
- Next, you must sign in to VNC Viewer using your RealVNC account credentials for that team, and generate a unique 9-digit code for the session.
- To connect, you must give the 9-digit code to the computer owner out-of-band. Only when the computer owner enters the correct code can the session start.

These steps ensure that remote computers are protected by multiple authentication mechanisms. No single password controls remote access.

Cloud infrastructure

Overview

Our philosophy for the cloud is that no one security measure is paramount. In other words, our security is layered; if RealVNC cloud services were to be breached, or if a malicious third party were to gain access to your RealVNC account credentials, there is no way for that party to gain remote access to your computers.

RealVNC cloud services

VNC Connect initiates and maintains a connection via the cloud using our system of online services, which were designed in-house alongside our security team. These run on a security-hardened platform.

These services are protected by mandatory TLS, and all end points are suitably authenticated. All clients use TLS 1.2 when communicating with cloud services. We use rate-limiting and geographical distribution to defend against denial of service attacks. As our distributed architecture has no master nodes, our services are highly available. This ensures that service to clients is maintained during upgrades and failover. Data is replicated in real time to multiple data centers, and frequent database backups are kept on encrypted storage for recovery purposes.

Operations

Our technical operations team monitors RealVNC cloud services 24 hours a day, 365 days a year. These systems are regularly patched. Any critical vulnerabilities in upstream dependencies are assessed and patched outside of our regular patching schedule.

Access to service data is tightly controlled and granted on a case-by-case basis, with the approval of senior RealVNC management required. Every change made by the team is logged for audit purposes.

Servers containing sensitive data use host-based intrusion detection. If someone were to gain unauthorized access, automated alerts would be raised. Automated external port scanning is regularly performed on all Internet-facing servers. Our security team reviews the output of this regularly.

Public Key Infrastructure

Intra-service communication is secured using a closed Public Key Infrastructure (PKI). Industry best practice is used in the internal operation of this PKI, and best-in-class security devices (including hardware security modules and 256-bit AES encrypted hard drives) are used. By controlling the chain of trust end-to-end, we guarantee this is tightly controlled and not reliant on third party root certificate authorities.

Critically sensitive data is never stored in the cloud

VNC Server does not delegate authentication to the cloud. Instead, it performs its own authentication checks, meaning that any breach of data from the cloud cannot be used to gain access to computers. Note that, for device access, VNC Viewer always stores computer passwords for those users who choose to save them as a convenience locally, and never sends them to the cloud.

Similarly, payment information is not stored on the cloud. Instead, it is stored in a secure vault owned by a third-party payment provider. Their storage system complies with PCI DSS regulations.

Your RealVNC account credentials are stored securely, using bcrypt hashes with a random salt. If you choose to delete your RealVNC account, your details are completely removed from our servers.

RealVNC account management portal

Our online portal can be used to manage your RealVNC account, and control the users and computers in your team. Many of the security features in this section are administered using the portal.

Access to the portal itself is protected by mandatory TLS. Our website is graded A in the Qualys SSL Labs test.

We follow all best practices for secure web development, including using secure cookies and providing protection against content injection and cross-site scripting (XSS). To avoid session misuse, signed in users are automatically signed out after a period of inactivity.

Online role management

Online role management for your team is built into the portal. Four roles currently exist:

- **User**. Can sign in to VNC Viewer and remotely access computers. They cannot manage the team in any way.
- **Manager**. A User who can additionally invite people in to share remote access, add computers to the team (device access) or name technicians (instant support).

- **Administrator**. A Manager who can additionally add capacity, renew subscriptions, and manage payment methods.
- **Owner**. The owner can do everything, including changing the billing address and VAT number for all their teams.

Multi-factor authentication for your RealVNC account

By default, your RealVNC account is secured using email as a second factor. Each time you sign in online or in to VNC Viewer from a new device at a new location, you'll get an email requiring you to confirm the activity. The email records the time, location and type of device attempting to access your account. This ensures that people cannot sign in to your account even if they discover or guess your RealVNC account credentials (email address and password).

A device is subsequently remembered so you're not asked to confirm on that device again, nor on any other device at the now-trusted location, unless you explicitly choose to forget (see below).

You can further protect your RealVNC account by turning on 2-step verification on the **Security** page of the online portal. This means that each time you sign in online or in to VNC Viewer you are required to enter a TOTP token (an Internet standard used by Google Authenticator and similar apps) in addition to your account credentials. Effectively, TOTP replaces email as the second factor, and provides a higher level of security by requiring confirmation for every sign-in.

Mandatory multi-factor authentication for your team

If you have an Enterprise subscription, Managers, Administrators and Owners of teams can mandate 2-step verification for team members (including themselves). This means that every member of a team, each of whom has their own RealVNC account, must enable 2-step verification in order to participate in the team, and remote access is blocked until they comply. Every team member subsequently enters a TOTP token in addition to their account credentials each time they sign in to VNC Viewer.

Remote sign-out from remembered devices

On the **Security** page of the online portal, you can remotely sign out from (that is, forget) devices signed in to your RealVNC account. For devices signed in to VNC Viewer, this additionally removes any locally-stored VNC Server passwords, as well as cached data from your Address Book. This fail-safe ensures that if your hardware is misplaced or stolen, a malicious third party will still not be able to gain access to your RealVNC account.

Client security

Overview

VNC Connect consists of two apps: VNC Server and VNC Viewer. VNC Viewer is used to gain remote access to computers running VNC Server.

VNC Server client software is always responsible for securing access to the computer. VNC Server controls authentication and authorization of VNC Viewer and grants access. By contrast, some solutions use a gateway appliance or control mechanisms in the cloud to verify and grant access to a remote session. RealVNC never defers access control to an appliance or the cloud. Since VNC Server remains in control at all times, the overall attack surface is lowered.

Audit logging

Device access

VNC Server writes an audit entry to each platform's system log for every connection made. This collects a wide range of connection information and can be stored locally or on a Domain Controller. These logs can be used to inspect and audit individual connections and are extremely useful in supporting corporate compliance and regulatory governance requirements.

Instant support

RealVNC cloud services stores a record of every support session and makes it available on the **Sessions** page of the online portal. If you have an Enterprise subscription, you can drill down into an individual session online and examine a detailed activity log, consisting of chat transcripts, details of files transferred, elevation requests and reboot operations. Chat transcripts are encrypted-at-rest of RealVNC's servers.

Blacklisting (device access only)

VNC Server has per-IP blacklisting capabilities that prevent unauthenticated clients from making repeated authentication requests. On UNIX systems, the blacklisting capability is additionally applied per-user name as well as per-IP. Using a configurable exponential backoff, system administrators can define the blacklist threshold. Blacklisting is in place to primarily protect against brute force password attacks.

IP address filtering (device access only)

For direct connections (Enterprise subscriptions only), VNC Server can be configured to prevent connections from computers with particular IP addresses.

Manual identity checking (device access only)

Since all data connections are end-to-end encrypted, it is not possible for an actor within RealVNC to mount a passive attack on relayed data. However, any cloud service architecture which performs key negotiation on behalf of its clients may be able to mount an active attack by exchanging false keys. This attack would enable impersonation of a VNC Server computer. See also the section *Identity checking*, above.

To protect against an attack from within RealVNC when making a cloud connection, the identity used to protect end-to-end encryption is optionally presented to the user. This is displayed as a catchphrase in VNC Viewer that the user must

approve. Additionally, the clients may log the identities, allowing an administrator to verify that no active attack is being performed.

At RealVNC, we are transparent about our cloud security, and an actor within RealVNC cannot mount an attack against a client without leaving an auditable trace or alerting the user via VNC Viewer's identity verification dialog.

Gatekeeping (device access only)

If a local user (that is, VNC Server owner) is likely to be physically present while remote control sessions are in progress, VNC Server can be configured to query VNC Viewer users as they connect and prompt the local user to approve or reject each connection.

Multi-factor authentication for VNC Server (device access only)

VNC Server has a number of standard authentication schemes, offering either one or two factors of authentication. For Professional and Enterprise subscriptions, VNC Server uses system authentication by default, so connecting VNC Viewer users must enter the same Active Directory or system user name and password they normally use to *log on* to their desktop on the remote computer. This scheme can be changed to use:

- X.509 digital certificates stored on pluggable smartcards/authentication tokens, or in certificate stores on connecting devices, so connecting VNC Viewer users are transparently authenticated by something they own (a smartcard) and something they know (a smartcard PIN).
- System authentication augmented with RADIUS authentication, so connecting VNC Viewer users must first enter their system credentials, and then provide a TOTP code or other credential, or perform one or more authorization operations mandated by a RADIUS server (hosted by an identity management provider such as Duo or RSA SecurID).
- Single sign-on (Kerberos – Enterprise subscriptions only), so connecting VNC Viewer users are transparently authenticated by secure network services.
- Interactive system authentication on Linux and macOS, so connecting VNC Viewer users must enter an AD or system user name and then supply credentials, or perform authorization operations, mandated by PAM module(s).

In addition, you can combine the standard authentication schemes to create a custom scheme consisting of as many factors as you need.

Session permissions (device access only)

Once successfully authenticated to VNC Server, connected VNC Viewer users can be assigned session permissions on a per-user or per-group basis, to restrict access to remote control features while sessions are in progress.

For example, particular users or groups could be prevented from printing, transferring files, or copying and pasting text. Or entire sessions could be made view-only.

Idle timeout

By default, VNC Server terminates non-responsive connections after 1 hour. This timeout can be reduced if necessary.

Exclusive access (device access only)

By default, VNC Server permits any number of VNC Viewer users to connect concurrently. This can be configured to allow only one VNC Viewer user to connect at a time.

Screen blanking (device access only)

VNC Server can be configured to blank the screen of remote Windows 7 PCs while remote control sessions are in progress, to protect the privacy of operations being performed remotely. We're working on adding this capability to other operating systems and versions.

Policy settings

Microsoft Group Policy can be used to lock down both VNC Viewer and, for device access, VNC Server. This prevents modification of any options that have been set by corporate policy. On UNIX and macOS systems, policy configuration files are used to perform the same function. This ensures that employees are using VNC Connect in accordance with approved corporate policies. This capability is only available with an Enterprise subscription.

Secure credential storage (device access only)

In VNC Viewer there is an option to remember VNC Server passwords. These are stored locally, and never sent to the cloud. If VNC Viewer is installed on a Windows machine, these passwords are by default stored in the Windows Credential Vault. On macOS, they are stored in the Keychain. On UNIX, they are protected using file system permissions.

On all platforms, it is possible to set a VNC Viewer master password that is used to encrypt the individual VNC Server passwords. The encryption key is derived from the master password using PBKDF2 and the entries are individually encrypted using AES-GCM-128. This capability protects the secrecy of all remembered passwords.

Root certificate pinning

When establishing a connection through RealVNC cloud services, the clients check the TLS root (CA) certificate against a whitelist. This limits exposure to certificates issued by other certificate authorities in the OS trust store.

Signed binaries

On Windows, installers and installed binaries are signed using Authenticode, while Gatekeeper is used on macOS. We also use code-signing to ensure that the binary has not been modified in transit or at rest by malicious third parties. This helps to prevent the installation of unauthorized binaries.

iOS and Android store security

Our VNC Viewer mobile apps for iOS and Android are tested by Apple and Google, and signed to ensure authenticity. This prevents the installation of unauthorized or rogue applications.

Development procedures

Overview

Our dedicated security team has been constantly involved during development of VNC Connect, and remains actively involved in the decision-making process post-release.

Pre-development

We initially established a set of security and privacy requirements to which VNC Connect had to adhere. Our fundamental security principles – that you don't have to trust *us* in order to trust our software, that VNC Server is in charge of any connection, that we cannot decrypt your session data now or in the future, and that any active connection must be considered hostile at all times – were established during these early discussions.

Exhaustive security and privacy risk assessments were then carried out. New features such as cloud connectivity and online account management were seen as particularly high-risk, so threat modelling was used during the design phase.

Any hardware used for cloud connectivity is owned and operated solely by RealVNC, and stored in remote data centers that meet today's strict industry certification and audit requirements. Only nominated RealVNC staff have the capability to configure this hardware. This helps keep VNC Connect's attack surface to a minimum.

Development

Our security team are constantly analyzing our code, and continue to review new code as features are added. Code scanning tools, as well as manual static analysis, are used to ensure this code is kept to the highest possible security standards. Code reviews ensure that developers do not use functions or coding practices that are considered unsafe.

The code review process includes automated white-box fuzz testing, dynamic analysis using tools such as Valgrind and AddressSanitizer and a continuing attack surface review of VNC Connect.

Release/post-development

Our code is subject to a final security review before each new release. We then archive all pertinent data. This is essential in order for us to perform post-release servicing tasks.

Every aspect of VNC Connect has been designed with the highest level of security in mind. Despite this, it is incredibly important that any software vendor has an incident response plan. Because we understand that no security measure is unbeatable, we can and will release updates that protect our product from threats that emerge following its release.

This process is based on Microsoft's SDL Model. You can read more about this model at www.microsoft.com/sdl.

For over a decade, we have used CVE to archive any public-facing security vulnerabilities that we have fixed. We will continue to do so for VNC Connect, in order to remain as transparent as possible to our customers.

Summary

The security features and processes that protect VNC Connect are part of an in-depth strategy. This document has attempted to explain this strategy by separating it into four key categories.

We trust this has helped shed some light on our security and illustrated the integrity of our approach. However, given the inherent complexity of software security, we understand you may have specific enquiries. Please don't hesitate to contact us with your questions. We're only too happy to put you in touch with the appropriate member of our development team.

If you have any questions about the topics raised in this white paper, please contact us at **enquiries@realvnc.com** or visit **realvnc.com/contact-us.**

RealVNC's remote access and management software is used by hundreds of millions of people worldwide in every sector of industry, government and education. Our software helps organizations cut costs and improve the quality of supporting remote computers and applications. RealVNC is the original developer of VNC remote access software and supports an unrivalled mix of desktop and mobile platforms. Using our software SDKs, third-party technology companies also embed remote access technology direct into their products through OEM agreements.

www.realvnc.com