TeamViewer Security Information

Target Group

This document is aimed at professional network administrators. The information in this document is of a rather technical nature and very detailed. Based on this information, IT professionals can get a detailed picture of the software security before deploying TeamViewer. Please feel free to distribute this document to your customers in order to resolve possible security concerns.

If you do not consider yourself to be part of the target group, the soft facts in the section "The Company / the Software" will still help you get a picture.

The Company / the Software

About us

TeamViewer GmbH was founded in 2005 and is based in the south of Germany, in the city of Göppingen (near Stuttgart), with subsidiaries in Australia and the U.S. We exclusively develop and sell secure systems for web-based collaboration. Within a short span of time, a fast start and rapid growth have led to more than 200 million installations of the TeamViewer software by users in more than 200 countries around the globe. The software is available in more than 30 languages.

Software development takes place exclusively in Germany.

Our Understanding of Security

TeamViewer has been used millions of times around the world for providing spontaneous support over the internet, accessing unattended computers (e.g. remote support for servers) and for hosting online meetings. Depending on the configuration, TeamViewer can be used to remotely control another computer as if one were sitting right in front of it. If the user who is logged on to a remote computer is a Windows, Mac or Linux administrator, this person will be granted administrator rights on that computer as well.

It is clear that such powerful functionality over the potentially unsafe internet has to be protected against attacks in various ways. As a matter of fact, the topic of security dominates all of our development goals, both to make access to your computer safe and to protect our own interests: millions of users worldwide only trust a secure solution, and only a secure solution assures our long-term success as a business.

Quality Management

From our understanding, security management is unthinkable without an established quality management system. TeamViewer GmbH is one of the few providers on the market that practices certified quality management in accordance with ISO 9001. Our quality management follows internationally recognized standards. We have our QM system reviewed by external audits on an annual basis.

External Expert Assessment

Our software, TeamViewer, has been awarded a five-star quality seal (maximum value) by the Federal Association of IT Experts and Reviewers (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.). The independent reviewers of the BISG e.V. inspect products of qualified producers for their quality, security and service characteristics.

Security-related inspection

TeamViewer has undergone a security-related inspection by FIDUCIA IT AG (an operator of data processing centers for around 800 German banks) and has been approved for use at bank workstations.

References

At present, TeamViewer is in use on more than 200,000,000 computers. International top corporations from all kinds of industries (including such highly sensitive sectors as banking, finance, healthcare and government) are successfully using TeamViewer.

We invite you to have a look at our references on the internet in order to gain a first impression of the acceptance of our solution. Surely you will agree that presumably most of the companies had similar security and availability requirements before they - after an intensive examination - finally decided on TeamViewer. To form your own impression though, please find some technical details in the following paragraphs.

TeamViewer Sessions

Creating a Session and Types of Connections

When establishing a session, TeamViewer determines the optimal type of connection. After the handshake through our master servers, a direct connection via UDP or TCP is established in 70% of all cases (even behind standard gateways, NATs and firewalls). The rest of the connections are routed through our highly redundant router network via TCP or http-tunnelling. You do not have to open any ports in order to work with TeamViewer!

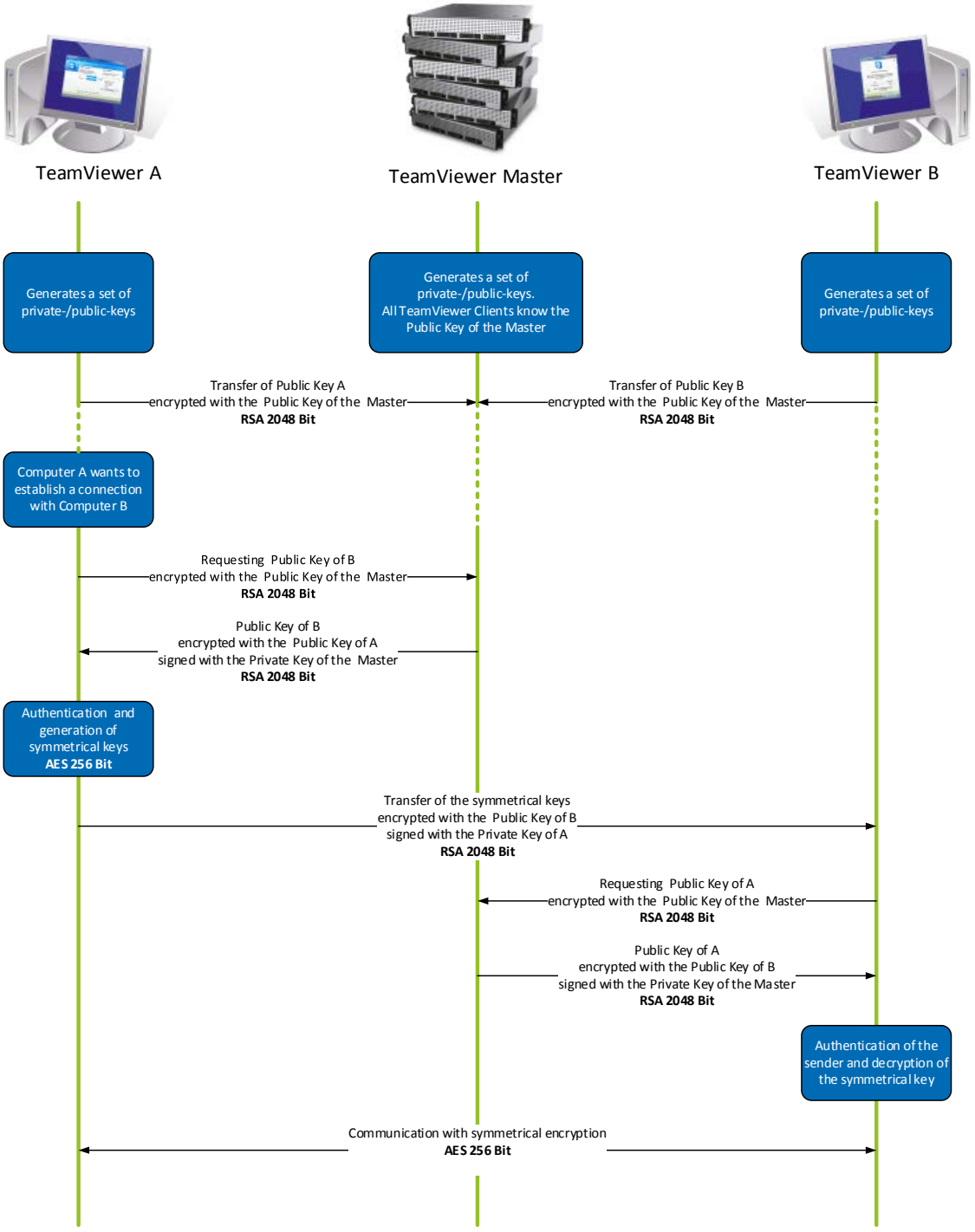
As later described in the paragraph "Encryption and Authentication," not even we, as the operators of the routing servers, can read the encrypted data traffic.

Encryption and Authentication

TeamViewer Traffic is secured using RSA public/private key exchange and AES (256 bit) session encryption. This technology is used in a comparable form for https/SSL and is considered completely safe by today's standards. As the private key never leaves the client computer, this procedure ensures that interconnected computers - including the TeamViewer routing servers - cannot decipher the data stream.

Each TeamViewer client has already implemented the public key of the master cluster and can thus encrypt messages to the master cluster and check messages signed by it. The PKI (Public Key Infrastructure) effectively prevents "man-in-the-middle-attacks." Despite the encryption, the password is never sent directly, but only through a challenge-response procedure, and is only saved on the local computer.

During authentication, the password is never transferred directly because the Secure Remote Password (SRP) protocol is used. Only a password verifier is stored on the local computer.



TeamViewer encryption and authentication

Validation of TeamViewer IDs

TeamViewer IDs are based on various hardware and software characteristics and are automatically generated by TeamViewer. The TeamViewer servers check the validity of these IDs before every connection.

Brute-Force Protection

Prospective customers who inquire about the security of TeamViewer regularly ask about encryption. Understandably, the risk that a third party could monitor the connection or that the TeamViewer access data is being tapped is feared most. However, the reality is that rather primitive attacks are often the most dangerous ones.

In the context of computer security, a brute-force attack is a trial-and-error-method to guess a password that is protecting a resource. With the growing computing power of standard computers, the time needed for guessing long passwords has been increasingly reduced.

As a defense against brute-force attacks, TeamViewer exponentially increases the latency between connection attempts. It thus takes as many as 17 hours for 24 attempts. The latency is only reset after successfully entering the correct password.

TeamViewer not only has a mechanism in place to protect its customers from attacks from one specific computer but also from multiple computers, known as botnet attacks, that are trying to access one particular TeamViewer-ID.

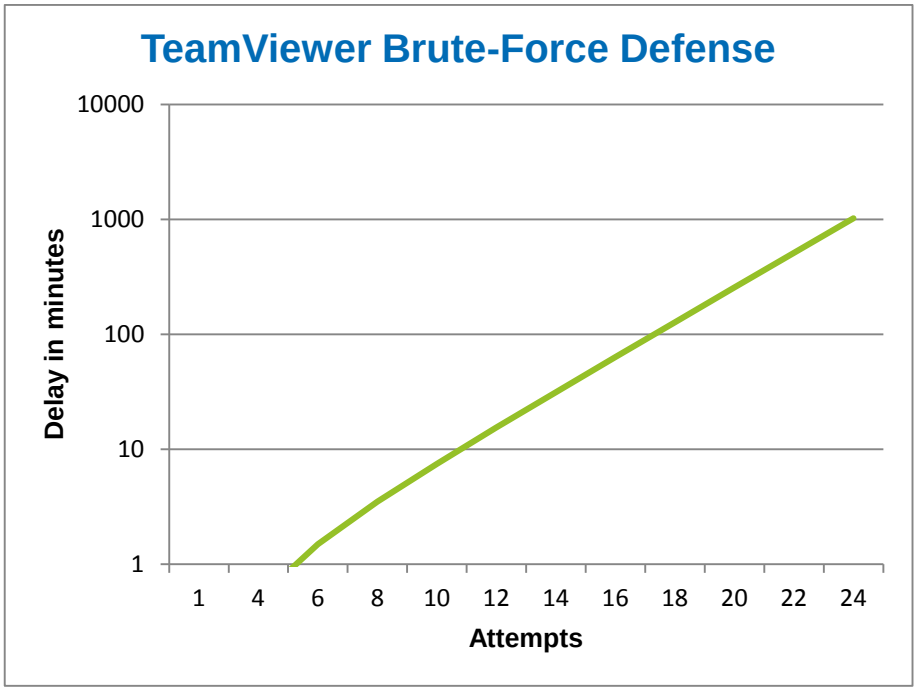


Chart: Time elapsed after n connection attempts during a brute force attack

Code Signing

As an additional security feature, all of our software is signed via VeriSign Code Signing. In this manner, the publisher of the software is always readily identifiable. If the software has been changed afterwards, the digital signature automatically becomes invalid.

Datacenter & Backbone

These two topics concern the availability as well as the security of TeamViewer. The central TeamViewer servers are located within the European Union in ISO 27001-certified data centers with multi-redundant carrier connections and redundant power supplies. Brand-name hardware is used exclusively.

Personal access control, video camera surveillance, motion detectors, 24x7 monitoring and on-site security personnel ensure access to the data center is only granted to authorized persons and guarantee the best possible security for hardware and data. There is also a detailed identification check at the single point-of-entry to the data center.

TeamViewer Account

TeamViewer accounts are hosted on dedicated TeamViewer servers. For information on access control, please refer to Datacenter & Backbone above. For authorization and password encryption, Secure Remote Password protocol (SRP), an augmented password-authenticated key agreement (PAKE) protocol, is used. An infiltrator or man in the middle cannot obtain enough information to be able to brute-force guess a password. This means that strong security can even be obtained using weak passwords. Sensitive data within the TeamViewer account, for example cloud storage login information, is stored AES/RSA 2048 bit encrypted.

Management Console

The TeamViewer Management Console is a web-based platform for user management, connection reporting and managing Computers & Contacts. It is hosted in ISO-27001 certified, HIPAA compliant data centers. All data transfer is through a secure channel using SSL (Secure Sockets Layer) encryption, the standard for secure Internet network connections. Sensitive data is furthermore stored AES/RSA 2048 bit encrypted. For authorization and password encryption, Secure Remote Password protocol (SRP) is used. SRP is a well-established, robust, secure password-based authentication and key exchange method using 2048 bit modulus.

Policy-Based Settings

From within the TeamViewer Management Console, users are able to define, distribute, and enforce setting policies for the TeamViewer software installations on devices that belong specifically to them. Setting policies are digitally signed by the account that generated them. This ensures that the only account permitted to assign a policy to a device is the account to which the device belongs.

Application Security in TeamViewer

Black- & Whitelist

Particularly if TeamViewer is being used for maintaining unattended computers (i.e. TeamViewer is installed as a Windows service), the additional security option to restrict access to these computers to a number of specific clients can be of interest.

With the whitelist function you can explicitly indicate which TeamViewer IDs and/or TeamViewer accounts are allowed to access a computer. With the blacklist function, you can block certain TeamViewer IDs and TeamViewer accounts. A central whitelist is available as part of the “policy-based settings” described above under “Management Console.”

Chat and Video Encryption

Chat histories are associated with your TeamViewer account and are therefore encrypted and stored using the same AES/RSA 2048 bit encryption security as described under the “TeamViewer Account” heading. All chat messages and video traffic are end-to-end encrypted using AES (256 bit) session encryption.

No Stealth Mode

There is no function that enables you to have TeamViewer running completely in the background. Even if the application is running as a Windows service in the background, TeamViewer is always visible by means of an icon in the system tray.

After establishing a connection there is always a small control panel visible above the system tray. Therefore, TeamViewer is intentionally unsuitable for covertly monitoring computers or employees.

Password Protection

For spontaneous customer support, TeamViewer (TeamViewer QuickSupport) generates a session password (one-time password). If your customer tells you their password, you can connect to their computer by entering their ID and password. After a restart of TeamViewer on the customer's side, a new session password will be generated so that you can only connect to your customer's computers if you are invited to do so.

When deploying TeamViewer for unattended remote support (e.g. of servers), you set an individual, fixed password, which secures access to the computer.

Incoming and Outgoing Access Control

You can individually configure the connection modes of TeamViewer. For instance, you can configure your remote support or meeting computer in a way that no incoming connections are possible.

Limiting functionality to those features actually needed always means limiting possible weak points for potential attacks.

Two Factor Authentication

TeamViewer assists companies with their HIPAA and PCI compliance requirements. Two-factor authentication adds an additional security layer to protect TeamViewer accounts from unauthorized access.

In addition to both username and password, the user must enter a code in order to authenticate. This code is generated via the time-based one-time password (TOTP) algorithm. Therefore the code is only valid for a short period of time.

Through two-factor authentication and limiting access by means of whitelisting, TeamViewer assists in meeting all necessary criteria for HIPAA and PCI certification.

Further Questions?

For further questions or information, feel free to contact us at (US) +1 (800) 951 4573 and (UK) +44 (0) 2080 997 265 or send an email to support@teamviewer.com.

Contact

TeamViewer GmbH
Jahnstr. 30
D-73037 Göppingen
Germany
service@teamviewer.com