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 as part of the target group, the soft facts in the section "The Company / the Software" will help you get a picture.

The Company / the Software

About us

The 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 are exclusively developing and selling secure systems for web-based collaboration. Within a short span of time, a fast start and a rapid growth have led to more than 200 million installations of the TeamViewer software and to users in more than 200 countries around the globe. The software is available in more than 30 languages.

Our Understanding of Security

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

It is obvious that such a mighty 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 the access to your computer safe and to protect our very own interest: Millions of users worldwide only trust a secure solution and only a secure solution secures our long-term success as a business.

Quality Management

From our understanding, security management is unthinkable without an established quality management. The TeamViewer GmbH is one of the few providers on the market practicing a 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 qualities.

Security-related inspection

TeamViewer underwent security-related inspections by the German companies FIDUCIA IT AG and GAD eG (they are the largest IT services provider in the cooperative financial system in Germany with data processing centers for more than 1200 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 banks, other financial institutions, health care and governments) are successfully using TeamViewer.

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

TeamViewer Sessions

Creation of a Session and Types of Connections

When establishing a session, TeamViewer determines the optimal type of connection. After the handshake through our master servers, in 70% of the cases a direct connection via UDP or TCP is established (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!

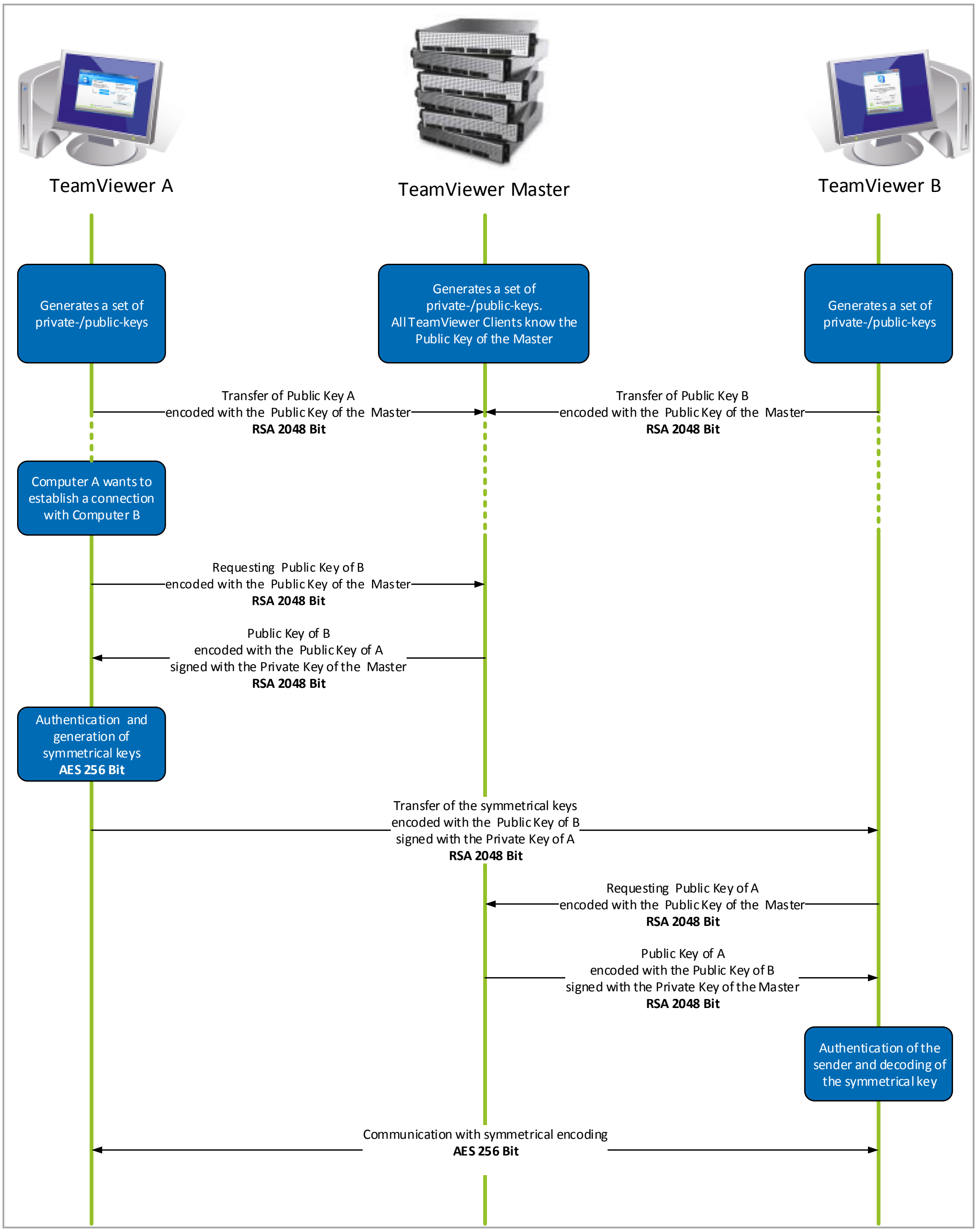
As later described in the paragraph "Encryption and Authentication" even we as the operators of the routing servers cannot read the encrypted data traffic.

Encryption and Authentication

TeamViewer works with a complete encryption based on RSA public/private key exchange and AES (256 Bit) session encoding. This technology is used in a comparable form for https/SSL and can be considered completely safe by today's standards. As the private key never leaves the client computer, it is ensured by this procedure 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 from the masters and check its signature respectively. 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 A
TeamViewer Master
TeamViewer B
Generates a set of private-/public-keys
Generates a set of private-/public-keys. All TeamViewer Clients know the Public Key of the Master
Generates a set of private-/public-keys
Transfer of Public Key A encoded with the Public Key of the Master RSA 2048 Bit
Transfer of Public Key B encoded with the Public Key of the Master RSA 2048 Bit
Computer A wants to establish a connection with Computer B
Requesting Public Key of B encoded with the Public Key of the Master RSA 2048 Bit
Public Key of B encoded with the Public Key of A signed with the Private Key of the Master RSA 2048 Bit
Authentication and generation of symmetrical keys AES 256 Bit
Transfer of the symmetrical keys encoded with the Public Key of B signed with the Private Key of A RSA 2048 Bit
Requesting Public Key of A encoded with the Public Key of the Master RSA 2048 Bit
Public Key of A encoded with the Public Key of B signed with the Private Key of the Master RSA 2048 Bit
Authentication of the sender and decoding of the symmetrical key
Communication with symmetrical encoding AES 256 Bit

TeamViewer encryption and authentication

Validation of TeamViewer IDs

The TeamViewer IDs are based on various hardware and software characteristics and are automatically generated by TeamViewer. The TeamViewer servers check the validity of the ID 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 gain insight into the connection or that the TeamViewer access data is being tapped is feared the most. However, in reality, very primitive attacks are the most dangerous ones.

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

As a defense against brute force attacks, TeamViewer exponentially increases the latency between the connection attempts. For 24 attempts it already takes 17 hours. The latency is only reset after successfully entering the correct password.

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

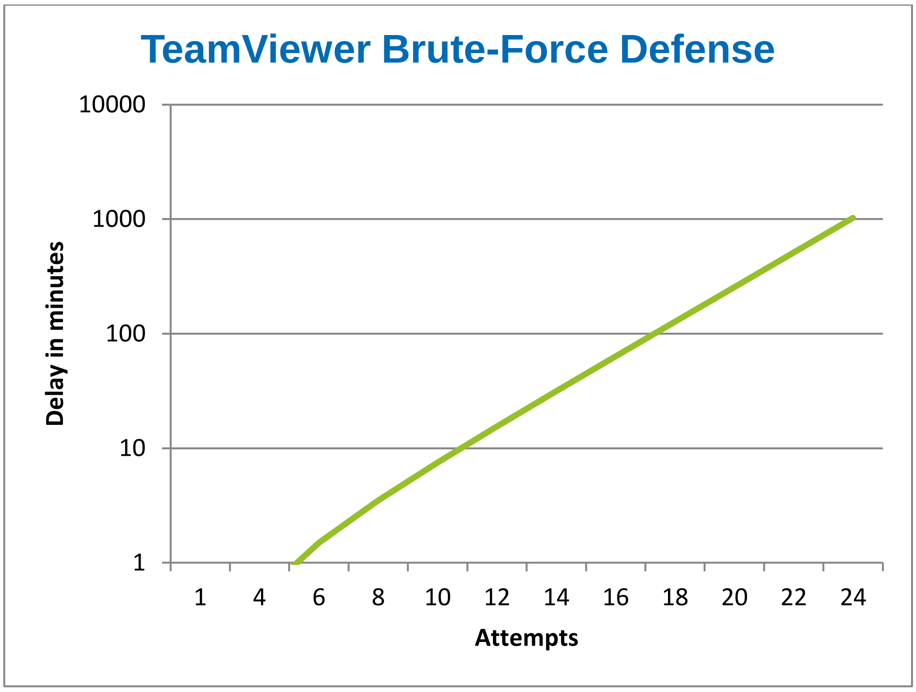


Chart: Time elapsed after n connection attempts during a brute force attack

Code Signing

As an additional security feature, all of our software is signed via VeriSign Code Signing. Due to this, the publisher of the software can always be reliably identified. If the software has been changed afterwards, the digital signature becomes automatically invalid.
Even the customizable TeamViewer modules are being signed dynamically during its generation.

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 connection and redundant power supply. Exclusively brand-name hardware is being used.

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 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 being used. An eavesdropper 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 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 and HIPPA compliant data centers. Any data transfer is transmitted 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 modules.

Application Security in TeamViewer

Black- & Whitelist

Especially if TeamViewer is 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 interesting.

With the whitelist function you can explicitly indicate which TeamViewer IDs and/or TeamViewer accounts are allowed to access this computer, with the blacklist function you can block certain TeamViewer IDs and TeamViewer accounts.

No Stealth Mode

There is no function which enables you to have TeamViewer running completely in the background. Even if the application runs as a Windows service in the background, TeamViewer is always made visible by 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 the access to this computer.

Access control incoming and outgoing

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 the functionality to the actually needed functions 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.

In combination with access control through white listing TeamViewer allows you to get HIPAA and PCI ready.

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 your emails to support@teamviewer.com.

Contact

TeamViewer GmbH
Kuhnbergstr. 16
D-73037 Göppingen
Germany
service@teamviewer.com

General Manager: Holger Felgner
Registration: Ulm HRB 534075