TeamViewer

GIVE YOUR DESKTOP WINGS

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.

In case 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 yourself.

The Company / the Software

About us

The TeamViewer GmbH is based in the south German city of Göppingen (near Stuttgart) and was founded in 2005. We are exclusively dealing with developing and selling secure systems for web-based collaboration. A fast start and a rapid growth have led to several million installations of the TeamViewer software and to users in more than 50 countries around the globe within a short span of time. The software is currently available in 14 languages.

The TeamViewer GmbH is privately owned and has been profitable since its foundation.

Our Understanding of Security

TeamViewer is used a million times around the world for giving spontaneous support over the internet or for accessing unattended computers (e.g. remote support for servers). Depending on the configuration of TeamViewer that means that the remote computer can be controlled as if you were sitting right in front of it. Is the user who is logged on to a remote computer a Windows or Mac administrator, he/she 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 our other development goals - in order to make the access to your computer safe and also to save our very own interest: Millions of users worldwide will 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 is following 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 a security-related inspection by the German 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 the present moment (September / 2008) TeamViewer is in use on more than 15,000,000 computers. International top corporations from all kinds of industries (including such highly sensitive sectors as banks and other financial institutions) 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 similar security and availability requirements before they have - 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.

Creation and Operation of a TeamViewer Session

Creation of a Session and Types of Connections.

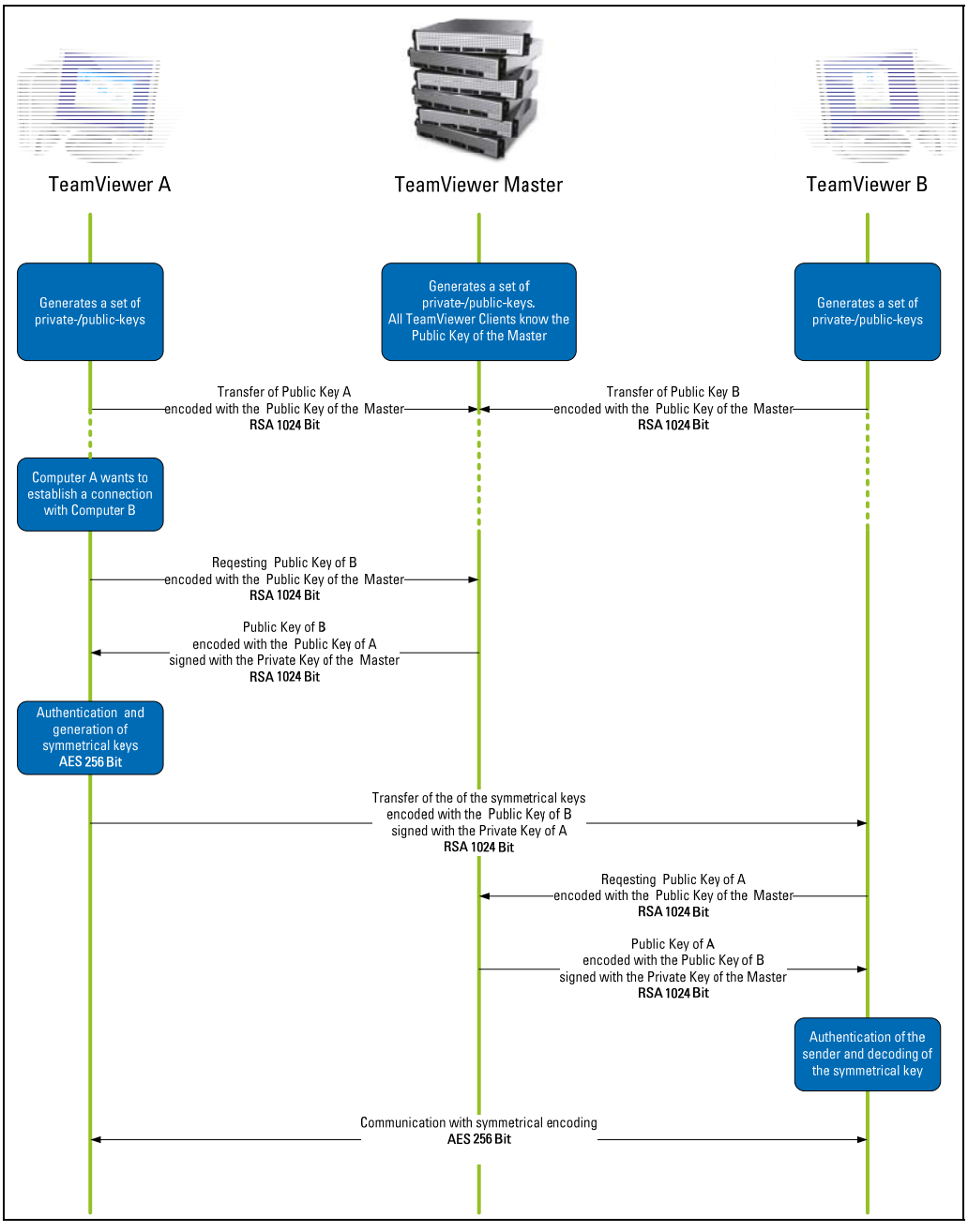
When creating a session, TeamViewer determines the optimal type of connection. After the handshake through our master server, in 70% of the cases a direct connection via UDP or TCP is established (even behind standard gateways, NATs and firewalls). The rest of the connections are routed through our highly 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 either.

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 clients has already implemented the public key of the master cluster and can thus encrypt messages for the master server and check the signature of the master, 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.



TeamViewer encryption and authentication

Validation of TeamViewer IDs

The TeamViewer IDs are automatically generated by TeamViewer itself based on hardware characteristics. The TeamViewer servers check the validity of the ID before every connection so that is not possible to generate and use fake IDs.

Protection from Brute Force Attacks

If prospective customers inquire about the security of TeamViewer, they 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. In reality it is very often very primitive attacks that are the most dangerous ones.

In the context of computer security brute force attacks are often attempts to guess a password which is protecting a protected resource by trial and error. With the growing computing power of standard computers the time needed for guessing even longer password has been increasingly reduced.

As a defence 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.

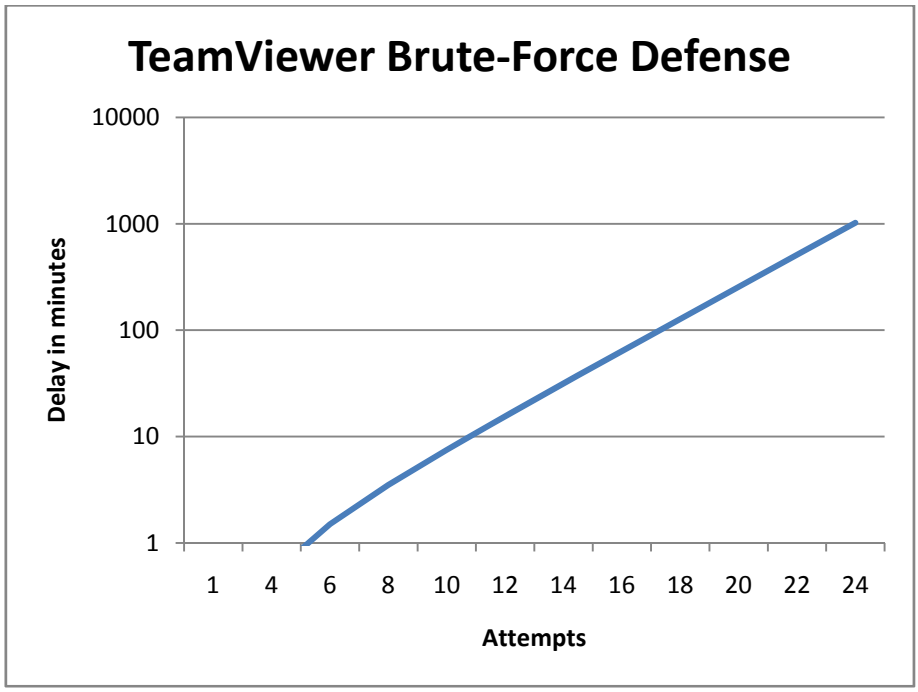


Chart: Time elapsed after n connection attempts during a brute force attack

Code Signing

As an additional security feature all our software is signed via VeriSign Code Signing. Due to this the publisher of the software can always be reliably identified. Has the software been changed afterwards the digital signature becomes automatically invalid.
Even the customisable QuickSupport module is being signed dynamically during its generation.

Datacenter & Backbone

These two topics concern the availability as well as the security. The central TeamViewer server is located in a highly modern data centre with multi-redundant carrier connection and redundant power supply. Exclusively brand-name hardware (Cisco, Foundry, Juniper) is being used.

The access to the data centre is only possible after a thorough identity check through a single entrance gate. CCTV, incursion detection, 24/7 surveillance and on-site security personnel protect our servers against attacks from within.

Application Security in TeamViewer

Black- & Whitelist

Especially if TeamViewer is used for maintaining unattended computers (i.e. TeamViewer is installed as a Windows service) it can be interesting - in addition to all other security mechanisms - to restrict access to this computers to a number of specific clients.

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

No Stealth Mode

There is no function which 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 through 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 deliberately 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 his/her password you can connect to the customer's computer by entering the ID and password. After a reboot on the customer's side a new session password will be generated so that you can only reach your customer's computers if you are explicitly 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. So for instance you may configure your remote support or presentation 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.

Further Questions?

If you have any further questions we are always looking forward to your calls 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

Executive: Dr. Tilo Rossmanith
Trade register: Ulm HRB 534075