RevShield Software Suite Network Security Review

Summary
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 RevGuard. Please feel free to distribute this document to your customers in order to resolve possible security concerns.

RevGuard Network Activity
RevGuard performs two activities on the network:

- Sending Updates Out
- Creating Remote Sessions

Sending Updates
RevGuard sends a heartbeat to a remote software named RevWatch every five seconds. The software resides either on the internal network or in the cloud. The outbound heartbeat is in the form of an SSL SHA-256 Encrypted Webservice Call that goes through port 80 or a predefined custom port and contains the host name, any applicable alerts, and general system health.

Creating a Session and Types of Connections
A remote support connection can be initiated in two ways: Host-Mode session or an On-Demand session.

With a Host-Mode session, the client PC is preloaded with our Remote Support software and is constantly checking for a connection from a support agent PC. On-Demand sessions are very similar, but the system only sends the initial request when prompted by the network administrator of the client RevGuard system. The “RevWatch encryption and authentication” diagram below will help you to gain a more in-depth understanding of this data flow.

When establishing a session, RevGuard Remote Support 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-tunneling. Not even we, as the operators of the routing servers, can read the encrypted data traffic.

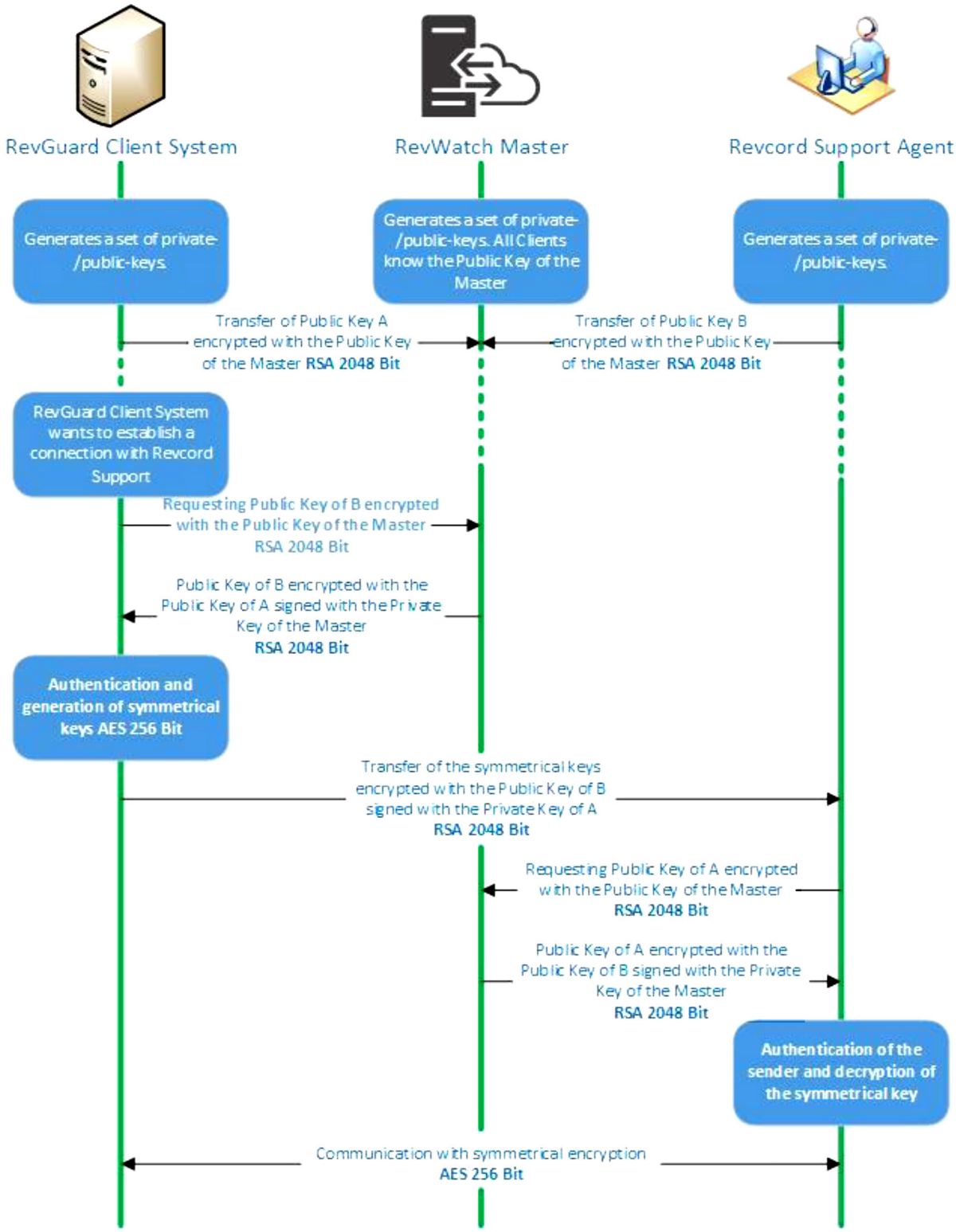
10190 Katy Freeway Suite #501
Houston, TX 77043
www.revcord.com

REVCORD
Revolutionizing Multimedia Recording

1-866-559-2188
Local 281-404-7040
Fax 281-404-5323

Version 2: 4-4-2016

Graphical Overview



10190 Katy Freeway Suite #501
Houston, TX 77043
www.revcord.com

REVCORD
Revolutionizing Multimedia Recording

1-866-559-2188
Local 281-404-7040
Fax 281-404-5323

Encryption and Authentication

RevGuard Remote Support 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 RevGuard Remote Support routing servers - cannot decipher the data stream.

Each RevGuard Remote Support 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.

Validation of RevGuard Remote Support IDs

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

Datacenter & Backbone

These two topics concern the availability as well as the security of RevGuard Remote Support. The central RevGuard Remote Support 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.

Brute-Force Protection

Prospective customers who inquire about the security of RevGuard Remote Support regularly ask about encryption. Understandably, the risk that a third party could monitor the connection or that the RevGuard Remote Support 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.

10190 Katy Freeway Suite #501
Houston, TX 77043
www.revcord.com

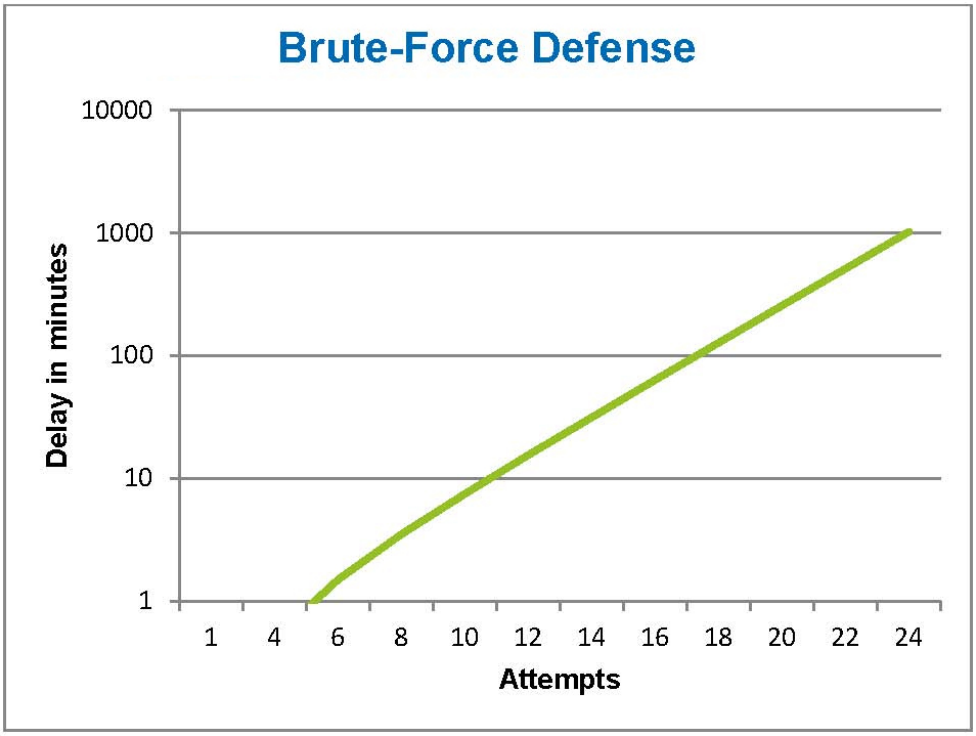
REVCORD
Revolutionizing Multimedia Recording

1-866-559-2188
Local 281-404-7040
Fax 281-404-5323

Version 2: 4-4-2016

As a defense against brute-force attacks, RevGuard Remote Support 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.

RevGuard Remote Support 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 RevGuard Remote Support -ID.



RevGuard Remote Support Account

RevGuard Remote Support accounts are hosted on dedicated 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 RevGuard Remote Support account, for example cloud storage login information, is stored AES/RSA 2048 bit encrypted.

Management Console

The RevWatch Management Console is a web-based platform for user management, connection reporting and managing Computers & Contacts. 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.

10190 Katy Freeway Suite #501
Houston, TX 77043
www.revcord.com

REVCORD
Revolutionizing Multimedia Recording

1-866-559-2188
Local 281-404-7040
Fax 281-404-5323

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.

Application Security in RevGuard Remote Support

Black & Whitelist
Particularly if RevGuard Remote Support is being used for maintaining unattended computers, 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 RevGuard Remote Support IDs and/or RevGuard Remote Support accounts are allowed to access a computer. 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 RevGuard Remote Support account and are therefore encrypted and stored using the same AES/RSA 2048 bit encryption security as described under the "RevGuard Remote Support 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 RevGuard Remote Support running `completely in the background. Even if the application is running as a Windows service in the background, RevGuard Remote Support is always visible by means of an icon in the system tray.

Password Protection
For spontaneous customer support, RevGuard Remote Support (RevGuard Remote Support On Demand) 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 RevGuard Remote Support 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 RevGuard Remote Support in Host Mode, 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 RevGuard Remote Support. 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.

10190 Katy Freeway Suite #501
Houston, TX 77043
www.revcord.com

REVCORD
Revolutionizing Multimedia Recording

1-866-559-2188
Local 281-404-7040
Fax 281-404-5323

Summary

Revcord has addressed one of the number issues facing logging recorders today…… secured monitoring and reporting.

For further questions or information, feel free to contact us at (US) +1 (866) 559-2188 or send an email to support@revcord.com.

10190 Katy Freeway Suite #501
Houston, TX 77043
www.revcord.com

REVCORD
Revolutionizing Multimedia Recording

1-866-559-2188
Local 281-404-7040
Fax 281-404-5323

Version 2: 4-4-2016