Wizard IP

Security White Paper
August 2004

Issue 3

Abstract

This white paper discusses the security concerns connected with KVM-via-IP remote control products, and presents the purpose built security architecture of the Wizard IP product.

Table of Contents

Introduction

Traditional KVM switches enable KVM (Keyboard, Video monitor, Mouse) consoles to be switched between a group of computers thus avoiding the need to attach a keyboard, monitor and mouse to each computer and saving space, cost and power. KVM switches don't require any software to be loaded on the computers and consequently offer simple-to-use and robust computer management that continues to work even if the computers crash. The one major drawback of this type of technology is that the KVM consoles must have a direct cable connection to the KVM switch which limits their range to a few hundred metres.

Remote access software enables computers to be controlled from anywhere in the world using a dial-in, network or IP style connection. This type of software is available in many flavours but all the solutions share the same basic principles of operation. Software is loaded onto the "host" computer that intercepts the video, keyboard and mouse signals. This software communicates these signals to a second software program running on a remote "viewer" computer in a manner that enables the user of the "viewer" computer to view and control the "host" computer. These software remote control systems can't cope with "boot time" problems and don't work if the host computer crashes.
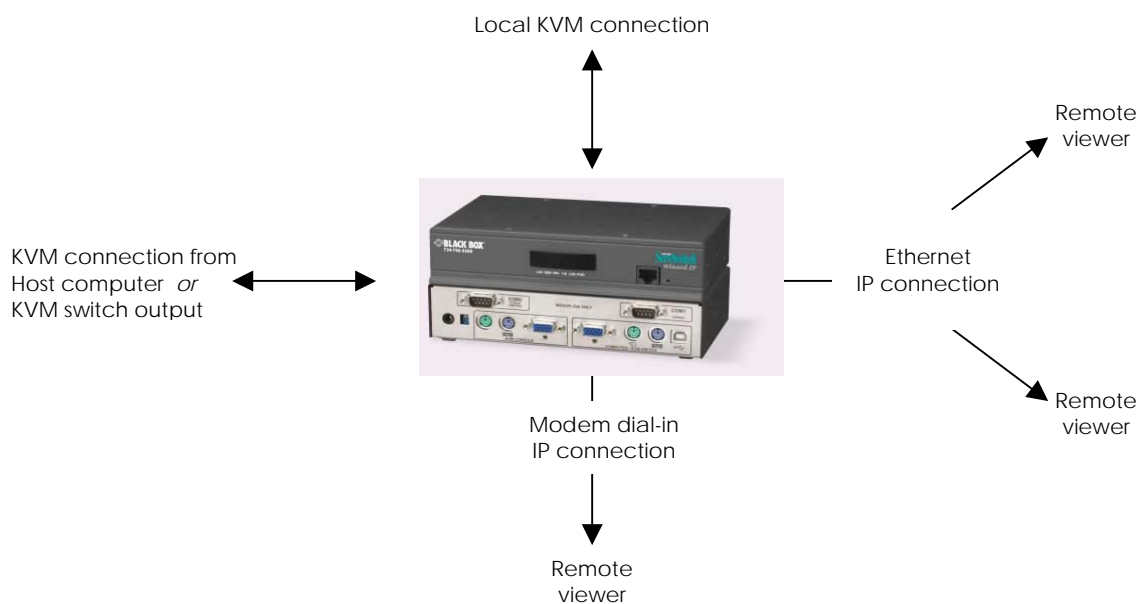
KVM-via-IP products are the result of combining the advantages of remote access software with the benefits of KVM technology. Like KVM switches, KVM-via-IP products don't require any software to be loaded on the host computers and instead interface directly with the keyboard, monitor and mouse connectors of the host computer or KVM switch. Circuitry within the KVM-via-IP appliance digitises the incoming video signal and processes it into digital data that is communicated to a viewer program running on a remote computer over a LAN, VPN or public internet.

The Wizard IP is an innovative KVM-via-IP product designed to address the demanding needs of the enterprise. The requirement for robust

security ranks highly, and this white paper explains the security architecture of the product.

Product overview

The Wizard IP product is a standalone unit, which can be easily configured to allow local, dial-in or remote IP connections to the target host or KVM switch. By using the local connection on the Wizard IP, users can have both local KVM console access and remote IP access to their servers. This mix of local and remote access is highly attractive to system administrators because it enables them to have direct local KVM access to computers in their server room whilst also enabling access from their office or from any remote location. The ability to simultaneously support IP network and dial-in modem connections offers system administrators the convenience of "in-band" access via the network and the security of reliable "out-of-band" access if the IP network is disrupted.

Local KVM connection

Remote viewer

KVM connection from Host computer *or* KVM switch output

Ethernet IP connection

Remote viewer

Modem dial-in IP connection

Remote viewer

The Wizard IP implements an enhanced VNC server embedded within its hardware. VNC is the world-wide de-facto standard for cross-platform software remote control and is the natural choice for KVM-via-IP products. VNC is currently installed and in use on many millions of computers in homes, small enterprises, government organisations, schools, university campuses and in most larger companies. An enhanced VNC viewer is supplied with the product, and can also be installed or directly run from the RealVNC web site [1]. In addition, a

Java viewer is embedded in the product, and can be run by connecting a web browser thus avoiding the need to install software on the remote viewing computer.

The need for security

Traditional KVM switches are inherently very secure, requiring physical access to the equipment. This can be controlled in the customary way with locks and keys. For users who have already gained physical access, a simple password system entirely local to the KVM switch is sufficient to provide a further level of secure access control to individual users and groups of users.

Access control is a much more worrying and difficult issue for products connecting to networks of any kind, from LAN, WAN to VPN and, of greatest concern, the public internet. Where the KVM-via-IP product is used to remotely access a privileged server console, such as a fileserver, a breach of security is potentially very damaging. For this reason, faith in the KVM-via-IP product's security is hugely important.

Security is often an after-thought, bolted on late in the development of a product. But security has a fundamental impact on the design and implementation of a complete system, and late consideration usually leads to flaws, loopholes and clumsy setup and configuration. Security for the Wizard IP product was considered from the outset, and a fully thought out and formally analysed security architecture was drawn up before any implementation and integration. Drawing on the expertise and advice of security experts within the Cambridge academic community, the Wizard IP meets the challenging requirements of internet connected products.

We now discuss the range of security measures included in the Wizard IP product which in combination allow it to be used with confidence across the most hostile of environments.

Access control

Identification
All access to the Wizard IP product, whether local, dial-in or internet, requires a valid user name and password. A privileged user "admin" has complete access to the configuration and management of the unit. The "admin" user can create other user names which are able to gain access to the host, but have only restricted capability to configure the unit. Each user profile has a number of capabilities which can be granted by the "admin" user, including the local and remote access rights . The table of user names and passwords are stored privately and securely on the unit itself, and are not duplicated or accessible externally. User names and passwords form the last line of defence for anyone who has gained physical or network access to the unit.

Passwords
For maximum security, it is important to choose strong passwords which are not easy to guess. When passwords are set, the unit will test for the cryptographic strength of the password and display a warning if the chosen password is considered weak. Similarly, a warning will be displayed if no password is set. The unit implements a strategy of temporarily locking out a user name if there have recently been repeated failed attempts to login. This scheme effectively prevents automated brute force attacks from discovering passwords by probing.

Logging
The Wizard IP product internally stores a comprehensive time stamped activity log. This allows the "admin" user to see a record of power on, reboot and firmware upgrade events. Access activity is shown in the form of successful or failed login attempts and includes the user name and the type of access (local, modem or remote). For remote access, the IP address of the remote computer is shown. In addition to providing information about normal operation, logs of this kind offer valuable diagnostics for detecting and analysing suspicious activity.

Private mode
A convenient feature of the Wizard IP product is the ability for any user to temporarily request exclusive access to the target host. Other users are locked out for the duration, and are presented with a warning

message. This feature is available both locally and remotely, and provides additional comfort when configuring secure systems or accessing sensitive information.

Screen lock
Further security is provided by a screen lock which will automatically come on after a period of local keyboard and mouse inactivity, preventing a screen which has been left unattended from being misused. This facility is implemented for local and remote connections.

Local access method

Physical access to any equipment provides an opportunity for misuse, and despite all other security measures internal to the product, facilities security is always a vulnerability. However, access to the local KVM connection is protected by user name and password in the same way as for a remote connection. In the local case, an on screen display provides the login dialog. For maximum security, the Wizard IP unit can be placed in a highly secure and restricted environment, with the local KVM connection being brought out to a less secure environment where the user name and password can provide strong access control.

Dial-in access method

By connecting an external modem, the Wizard IP product provides a remote access facility via a standard telephone line. Dial-in access provides an inherent first level of security because an attacker would need to know the telephone number to which the unit is connected in order to be able to attempt to connect. Unlike an IP network, probing the public telephone network is difficult to automate and costly. It is also widely accepted that the public telephone network, and a dial-in connection is very difficult to snoop or intercept. The unit incorporates a PPP server [2], allowing an IP connection to be made using a standard dial-in network configuration from a remote host. The enhanced VNC viewer can be run over the IP connection as described below, including the full range of encryption and authentication measures which are included.

IP network access method

The full utility of the Wizard IP product becomes apparent when it is connected to an IP network. Since IP networks are ubiquitous, the target host can potentially be controlled from anywhere in the world, and for convenience many users expect to be able to access KVM-via-IP products via an Internet connection. This requires a special level of care where security is concerned.

Other product approaches
Other KVM-via-IP products have implemented security schemes based around HTTPS [3], which is used primarily for secure web transactions. HTTPS was not specifically designed for use with KVM-via-IP products and consequently has some drawbacks. Each HTTPS site needs to be issued with an SSL [4] certificate from an authority such as Verisign [5] or Thawte [6], which has been signed by them using a private key. Web browsers are designed and built to trust these authorities, and can verify that any certificate presented to the browser by the HTTPS site is signed by such an authority. This is easily done using the authority's public key.

To use HTTPS effectively in a KVM-via-IP product, the owner of each unit would be required to obtain a certificate and configure that unit with the certificate. This represents a significant administrative and financial overhead, with a certificate typically costing in excess of $100 per annum. Furthermore, certificates are based on IP addresses or DNS names, and so a KVM-via-IP product would have to be previously configured to have an IP address or a DNS name which would remain static for the lifetime of the certificate. In effect, it is simply not feasible to obtain signed certificates in practical installations.

Instead, KVM-via-IP products which use HTTPS create their own self-signed SSL certificates. When a browser is connected to the unit, the certificate is shown to the user in a pop-up window, and the browser asks if this certificate is to be trusted or not. On the very first connection, this can be considered to be an acceptable policy. Indeed, secure remote login shells such as SSH [7] operate in the same manner. However, it is extremely difficult and in some cases impossible

to arrange for browsers to cache these certificates and so the pop-up window will occur every time the browser is connected to the unit.

This situation is open to "man in the middle" attacks, since it is left to the user to visually verify that a certificate has not changed between successive connections to the same unit. Experience shows that users do not take this degree of care, and will habitually accept the new certificate. This is worse than the situation with SSH, where the certificate is cached in the computer's file system, and the user will consider more carefully the situation where the certificate appears to have changed.

Wizard IP approach
For these reasons, the Wizard IP product does not rely on HTTPS for secure access, and avoids the corresponding certificate management issues. Furthermore, HTTPS and SSL implementations are bulky and complex, and contain many features which are not relevant to a remote access product. The product embodies the philosophy of SSH and some concepts from SSL. A custom design and implementation has enabled a very tightly focused integration, avoiding many of the security loopholes which have tended to plague the third party HTTPS and SSH implementations by virtue of their size and plethora of spurious additional functions. The security implementation has undergone rigorous testing and evaluation through large-scale deployment in a number of multinational companies.

First, public key authentication is carried out with 2048 bit RSA cryptography [8] (extendable to larger keys). This involves running a key generation algorithm to generate a pair of large primes. The key generation algorithm uses a number of entropy sources from the unit to ensure that the generated keys are truly random and cannot be predicted. Entropy sources include keystrokes and mouse movements, which the user is required to provide during the key generation phase. Then, encryption is carried out using the AES stream cipher [9] with a 128 bit key, which is generated and exchanged securely as a result of the authentication phase.

Wizard IP security specification

The notation $P_k\{m\}$ is used to indicate that a message **m** is to be encrypted with public key P_k. The notation $S_s\{m\}$ indicates that the message **m** is to be encrypted with the symmetric key S_s. The symbols **V** and **U** are used to refer to the viewer and unit in the protocol exchange. First, the unit sends its public key to the viewer. At this stage, the viewer compares the unit's IP address and public key against values stored in the local file system or registry cache in order to warn the user if it has changed since the previous access.

$$U \rightarrow V : P_U$$
$$V \rightarrow U : P_V$$

Then, randomly-generated strings or nonces **N** are generated, upon which to base the session key. Because these are encrypted with each party's public keys, only the holders of the corresponding private keys can obtain the nonces. This prevents an eavesdropper from intercepting them.

$$U \rightarrow V : P_V\{N_U\}$$
$$V \rightarrow U : P_U\{N_V\}$$

128 bit session keys are calculated based upon the two nonce values, using SHA-1 hashing [10].

$$S_{V2U} = H(N_V, N_U)$$
$$S_{U2V} = H(N_U, N_V)$$

Using the new session keys, the AES protocol is used to encrypt some well-known information (the Wizard IP uses a hash of the public keys) allowing both parties to verify that the other has correctly calculated the session keys.

$$U \rightarrow V : S_{U2V}\{H(P_U, P_V)\}$$
$$V \rightarrow U : S_{V2U}\{H(P_V, P_U)\}$$

Following this secure exchange of session keys, all subsequent message exchanges between unit and viewer are similarly AES encrypted using

a stream cipher mode to provide protection from in-depth analysis or replay attacks. The first such message exchange is the unit access control phase, involving a user name and password being transmitted from viewer to unit.

IP address filtering
The unit allows IP filtering of incoming packets. This allows the "admin" user to establish a pattern of IP addresses from which remote connections will be accepted. All other attempts to connect will be refused. This allows the unit to be configured to work only on a specific IP address range, such as a corporate LAN.   In another scenario, it allows access from specified external IP addresses, for example from a system administrator's home. This facility gives additional control and comfort when enabling access through the company firewall.

Java viewers
A Java viewer downloadable from the unit itself provides a convenient method of gaining access without installing any software on the remote computer. All browsers provide a safe execution environment for the Java program, which prevent it from accessing the local file system or registry. It is therefore impossible for a Java viewer to cache any certificates issued by any KVM-via-IP product. In the absence of authority signed certificates, Java viewers are potentially vulnerable to "man-in-the-middle" attacks. However, a human readable certificate fingerprint is presented to the user by the viewer at connection time. This gives the user an opportunity to visually check the certificate against a known value and so verify the server identity before continuing.

Firmware upgrade

It is recognised that the unit may occasionally require upgrading to introduce new functionality and performance enhancements.   Full firmware upgrade is supported either locally over the serial port, or optionally over the IP network connection. It is vital that only certified upgrades from a verifiable source are downloaded and installed, and the security architecture specifically addresses this problem through the use of public/private key digital signatures.

All firmware upgrades and accompanying digital signatures are distributed by Black Box. Firmware upgrades are binary, and do not require encryption. The signature is computed in two stages. First, a fingerprint of the binary is calculated using a public SHA-1 hash function. The fingerprint is then signed using RSA cryptography, using the *Wizard IP private key* known only to Black Box.

When a firmware upgrade and accompanying digital signature is downloaded, the Wizard IP product verifies the authenticity of the 2048 bit signature using RSA cryptography derived from the *Wizard IP public key*, installed at manufacture. The resulting fingerprint can be checked against the fingerprint of the downloaded binary calculated using the same SHA-1 hash function.

This method of signing firmware is extremely secure, since it is computationally infeasible for a malicious third-party to create a binary firmware upgrade with a matching RSA signature pair. The threat of having upgrade data spoofed is thus prevented.

Configuration and management

The Wizard IP product has an elegant and simple approach to unit configuration and management. Initial configuration, for example setting up IP network parameters, is carried out on the local KVM connection by attaching a monitor and keyboard. An on-screen-display presents a simple menu system to lead to user through the necessary steps. All other configuration is carried out over the IP connection itself.

Single remote connection
The key feature is to use a single connection from the remote computer to the Wizard IP product for both the remote control function AND for the configuration menus. This unique combination of interactive remote control and configuration menus overlaid in a single window on the remote computer screen provides a fully integrated and remarkably intuitive user-interface. Using a single software application, the VNC viewer, means that there are no other configuration tools to install and run separately and no cascades of disjointed and dissimilar windows. By contrast, other KVM/IP products have separate applications and connections for remote control and for configuration.

In addition to providing a completely consistent look and feel, the integrated approach simplifies the management of security by requiring only a single IP port to be open through the firewall. The security architecture described above make this single channel secure and safe. In a further significant simplification, the Wizard IP product is able to respond both as a web server or a VNC server on the same IP port, by auto-sensing the type of client connection. This allows the user to either connect with a web browser and download and run the Java viewer, or to connect with a native VNC viewer installed on the remote computer. Other KVM-via-IP products tend to have different ports for remote control protocol and for web server, and require more complicated configuration through firewall and routing equipment.

Deployment scenarios
It is anticipated that there will be a variety of deployment scenarios with different security requirements. On a completely trusted private network, security may not be a concern and the most basic user name and password scheme will suffice to control access to the Wizard IP. On larger or public networks, stronger security may be required and the remote access stream can be authenticated and encrypted to provide protection against a variety of attacks including snooping, brute force attacks and man-in-the-middle attacks. Correspondingly, the Wizard IP unit can be configured to require strong encryption or not, as appropriate for each deployment.

General security advice

If you make the Wizard IP accessible from the public Internet or from a modem, care should be taken to ensure that the maximum security available is activated. You are strongly advised to enable encryption and use a strong password. Security may be further improved by restricting client IP addresses, using a non-standard port number for access or limiting remote access to dial up connections only. Please refer to the "Networking Issues" section of the Wizard IP manual for more information.

Deployment advice
The security capabilities offered by the Wizard IP are only truly effective when they are correctly used. An open or weak password or unencrypted link can cause security loopholes and opportunities for potential intruders. For network links in general and direct Internet connections in particular, you should carefully consider and implement the following:

- Ensure that encryption is enabled on the Wizard IP.
- Ensure that you have selected secure passwords with at least 8 characters and a mixture of upper and lower case and numeric characters.
- Reserve the admin password for administration use only and use a non-admin user profile for day-to-day access.
- Use the latest Secure VNC viewer (this has more in-built security than is available with the Java viewer).
- Use non-standard port numbers.
- Restrict the range of IP addresses that are allowed to access the Wizard IP to only those that you will need to use.
- Do NOT Force VNC protocol 3.3.
- Add a further level of inherent security by restricting access only via modem or ISDN dialup.
- Ensure that the computer accessing the Wizard IP is clean of viruses and spyware and has up-to-date firewall and anti-virus software loaded that it is appropriately configured.

- Ensure that the computer accessing the Wizard IP has had all the latest operating system security patches and updates applied.
- Avoid accessing the Wizard IP from public computers.
- Ensure that passwords are updated or removed when no longer needed (e.g. when an employee leaves).

Additional security measures
- Use a KVM switch with On-Screen-Display driven security access and an auto-logout (after inactivity) feature to provide a second level of security. KVM switches such as the ServSwitch UNO, DUO or QUADRO are recommended.
- Place the Wizard IP behind a firewall and use port the numbers to route the VNC network traffic to an internal IP address.
- Review the activity log from time to time to check for unauthorized use.
- Lock your server consoles after they have been used.

References

1. http://www.realvnc.com, RealVNC website
2. http://www.ietf.org/rfc/rfc1332.txt, PPP protocol
3. http://www.ietf.org/rfc/rfc2616.txt , HTTP/HTTPS protocol
4. http://wp.netscape.com/eng/ssl3/draft302.txt, SSL protocol
5. http://www.verisign.com, trusted certificate authority
6. http://www.thawte.com, trusted certificate authority
7. http://www.ietf.org/internet-drafts/draft-ietf-secsh-architecture-15.txt, SSH protocol
8. http://www.faqs.org/rfcs/rfc2437.html, RSA cryptography specifications
9. http://csrc.nist.gov/CryptoToolkit/aes/rijndael/, AES specification
10. http://www.ietf.org/rfc/rfc3174.txt, SHA-1 specification