Security Considerations When Using Kaveman

Peter D. Gray
Digital V6 Inc.

December 10, 2001

1 Introduction

This white-paper discusses a number of security considerations that must be made when deploying Kaveman on a network. The purpose of this document is to help the user to decide on the security model to use with Kaveman and have a better understanding of the security features of this product.

2 Terminology

Controlled Computer (Server) This will refer the computer to which the Kaveman's VGA, keyboard and mouse connections are attached. The server is the machine which is in need of remote administration. We will assume in this document that the server is located in a secure environment, such as a locked server cabinet. In most cases, the Kaveman will be physically located only a few inches away from the server itself. For this reason, we will also assume the Kaveman is in a secure environment.

Client machine This refers to the remote computer that is connecting to the Kaveman over the network. Normally, the client machine is using Netscape or some other HTML browser to do this. The client machine may also use VNC client software to communicate with the Kaveman. VNC, a free download, is a remote display system which allows anyone to view a computing 'desktop' environment from anywhere on the Internet and from a wide variety of machine architectures.

Production network This is the network over which real traffic travels. This is the network that an IT person is charged with keeping running, that the bulk of the company's in-band traffic flows across and that is probably the main LAN/WAN.

Maintenance network This is a backup, or spare, network that is established solely for out-of-band and maintenance access to servers, routers and infrastructure.

3 Security Modes and Features

3.1 Baseline features

The following security features are always in effect and provide an excellent default level of security for the Kaveman.

- All software on the Kaveman is immutable—it cannot be changed by anyone. Unlike a PC, the firmware which enforces the Kaveman security model cannot be changed by the end user. Therefore, it is not possible to install a trojan horse or virus on the Kaveman.

- Like most operating systems, when the Kaveman receives more than three failed password attempts within a short time frame, it will force all following attempts to proceed very slowly. This feature defeats any attempts to automate guessing of passwords because it is impractically slow to check many wrong passwords. See also "Turtle mode" below.

- The Kaveman makes remote administration easy. However, signing in to remotely administer the controlled computer over IP does not automatically give the user complete access to the server. Like any passer-by, if the server's console is locked or logged-out, the user must provide a user name and password to access the machine. Similarly, to access sensitive data, the user would need a special administration password. If the user logs off of the server *every time* after using the Kaveman, another layer of security that the attackers must circumvent is created.

- All web traffic to and from the Kaveman can be encrypted using 128-bit SSL. Just like an online bank account, all connections to the Kaveman can be made over HTTPS protocol. This mechanism is supported by most modern web browsers

and is relatively transparent to the user. (To verify the connection is secure, check for the closed padlock icon in the corner of the web browser.) This low-level encryption is sufficient to prevent eavesdropping, inserting commands into the data-stream or other tampering with the data in transit. It is also this encryption that protects Kaveman passwords from traveling over the network in the clear.

The video data is not encrypted in the current product. However, the keyboard and mouse commands are encrypted when Kaveman's Java viewer is used. The standard VNC protocol does not support encryption of any kind. Both of these protocols are binary in nature, so custom software would be required in order to peice together the video image from any successfully evesdropped data [1].

If the company is concerned with eavesdroppers, networks can be further secured with an external VPN-type product.

3.2 Easy mode

In "Easy mode", all network traffic is encrypted, but simple passwords are used for authentication. This is the default mode of operation and offers more than enough security when the Kaveman is being controlled over a private network or from behind a firewall. It is possible to disable the passwords in this mode.

3.3 Certificate mode

In this enhanced mode, the user must configure the Kaveman with one or more digital certificates that uniquely identify the Kaveman and the client machine. A client machine without the required certificate file will not be able to communicate with the Kaveman. In this sense, digital certificates are acting as improved passwords. The amount of encryption applied to the data stream is not affected by the use of certificates.

[1] Digital V6 is considering a future product that would encorporate encryption on the video as well. Please talk to our sales department for more information.

3.4 Stealth mode

In stealth mode, a Digital V6 exclusive feature, the Kaveman deliberately violates certain TCP/IP protocol standards in order to conceal its presence on the network. For example, it will not respond to any ICMP PING requests. A TCP/IP connection request (or UDP packet) to any unused port will go unanswered and will not solicit the normal "connection refused" response. The goal is to make the Kaveman invisible to a "port scan" attack, by acting as if it was not there. For optimum security, the web server port number should be changed from the default as well (user configurable). Operation of the Kaveman, by legitimate users who know both the IP address and web server port number, will be as normal. However, outsiders who might be searching for the Kaveman will not be able to detect it on the network unless they correctly guess both the IP address and port number.

3.5 Turtle mode

This optional mode enables the Kaveman to shutdown when it feels that its security may be under attack. For example, if more than five password failures are detected in a certain time frame, the Kaveman will shutdown and disconnect itself from the network. The only way to recover operation of the Kaveman is to login from the local control port (the keyboard connected to the 'thru' connector) and give the appropriate reset command. Remote access to the Kaveman is completely locked out. The operation of the attached server is not affected. Clearly, turtle mode opens the Kaveman to denial-of-service attacks which could be rather annoying to legitimate users. Therefore, this mode is not enabled by default. There is an optional Turtle timeout duration (in hours) that by default is set to 24 hours.

3.6 Monitor-only application

In some applications, the main desire is to monitor the screen of remote servers. In this case, it may be possible to leave the keyboard and mouse disconnected from the Kaveman. Since only the VGA video is connected, it is not possible to do anything more than monitor the screen remotely. To reboot, or change the server's configuration, a local keyboard, mouse and video screen would have to be used.

Clearly, some benefits of the Kaveman would be lost in this configuration.

4 Deployment Models

There are a number of different ways to add Kaveman to an existing network or design a network for use with the Kaveman. Which approach applies, depends on the intended use for Kaveman.

Whenever the number of points from which an attacker can communicate with the Kaveman is reduced, the more secure the server becomes.

4.1 Shared nternal network

In this model, the Kaveman is connected to the same LAN as the server machine. This setup may be appropriate for servers on a LAN within a single building. The weakness of this approach is the lack of an "out of band" path to the Kaveman. However, if the server is not associated with network routing or control, there is no reason to think the network would be down if the server crashes. Traffic to and from the Kaveman travels over the production network. Any machine on the production network could, with appropriate passwords and digital certificates, connect to the Kaveman and control it.

Because this is an internal network, it is behind one or more firewalls. The network has many machines connected to it, but all of these machines are under the user's administrative control and it is safe to assume that only legitimate users are accessing this network. Most office LAN's with many client machines and a few file servers are modeled like this. The network is private, and it is assumed that any potential intruders are outside this network. Naturally, important data is protected with passwords, audit and control network access, but it is safe to assume the servers are not under daily attack from experts.

The default security model ("Relaxed security") should be sufficient in a network configured like this.

4.2 Separate Maintenance LAN

In this approach, there is a separate network reserved for accessing the Kaveman. The production network never carries traffic from or to the Kaveman. There is a performance advantage to this approach as the video information from the Kaveman does not need to compete with the production network's normal traffic. The biggest advantage, however, is the security provided. By controlling access physically to the maintenance network, gives the IT person absolute and reliable control over this limited network. Unlike the production network, this net does not need to be wired into every corner of the facility, so it might be quite inexpensive to add a maintenance network to the building. A small maintenance network might extend only through the server room and the IT person's office.

The additional security gain from putting the Kaveman on a separate network is small, since all network traffic is encrypted. The best reason to use a maintenance LAN is to allow out-of-band access to the server, particularly when the production network is down.

4.3 Public Internet

In many applications involving server co-location, there will be no opportunity to use a maintenance network. Both the server and the Kaveman must be on the same network segment, and both will be connected to the public Internet. If a firewall is used, then some protection can be added to defend the Kaveman from outside attacks. However, in general, it is in this scenario where the native security on the Kaveman becomes most important.

We recommend that the IT person enables stealth mode, turtle mode and, if possible, use digital certificates when using the Kaveman on the public Internet.

4.4 Other variations

4.4.1 Internet with VPN

The IT person can create a virtual maintenance LAN by using a VPN (Virtual Private Network) product. The VPN would create a private network over the public Internet, or internal production network. There is no special support on the Kaveman for VPNs, since this approach is best implemented outside of it. The company will require a hardware-based virtual private network solution. The Kaveman does not currently support any software VPN scheme.

4.4.2 Firewalls

It is possible to protect a Kaveman by putting it behind a firewall (perhaps a dedicated firewall) and restricting access based on source IP address. By doing this, the IT person will be able to restrict access to the Kaveman to a limited number of IP addresses or subnets. Some people will say that this is vulnerable to source-routing IP address spoofing, but such attacks are rare and very difficult to implement.

In general it is possible to use turtle mode and stealth mode to achieve similar results to a firewall, but an external firewall may offer more advanced monitoring and detection than is possible on the Kaveman itself.

5 Conclusion

The Kaveman was originally designed to be used on the Internet. As a result, it has many security features and operation modes that allow it to be safely and confidently deploy it in any network situation.