CS TimeClock

Networking Specification

Document Date: June 2009
Document Status: Version 1.02
Program Status: Implemented in CS TimeClocks version 1.15 and later.

Contents

Introduction

The CS TimeClocks are networkable. They talk to each other, and to other computers. This approach adds considerable benefits to the system, but it also comes with additional risks.

This document discusses the reasons for the connections, and their risks. It contains information useful to both support staff, and end user customers. It also contains the technical information necessary for network administrators to ensure that the network functionality is possible.

You do not need to turn on all the functionality offered by the clock. Thus this document provides the necessary information to deciding which options you wish to make use of. The document has been broken down to explain connections used on the LAN and connections used on the WAN.

There is understandable concern when adding networking devices to any LAN or WAN. It is most important to determine the risks in doing so, and understanding the implications of those risks. However understanding the risks also empowers users to make decisions based on fact rather than paranoia. Networking can be a safe activity, and understanding the scope of the networking ensures that it remains a safe activity.

Primary Security Concerns

The clock cannot catch a virus

The CS Time Clock uses an uncommon processor which is not the same processor chip found in every day PC's. Viruses designed for one processor cannot be used on another processor.

The CS Time Clock uses an industry standard, robust, non-Windows-based, operating system. A virus written for one operating system cannot run on another operating system. Virtually all the viruses in the world are written for Windows because Windows is the most common system.

The clock cannot be "hacked"

In an ideal configuration the clock will be open to the internet, able to provide data to the necessary programs and to enable support teams to assist with any problems on site. It should be noted that access through these methods is extremely limited, they expose the data for interrogation, but they do not allow new programs to be placed on the clock.

The clock is capable of updating its own firmware from a repository on the internet. The method used uses industry standard techniques to avoid any malicious data from being included. This update is done over a secure connection – similar to the one used by your bank when doing internet banking.

The clock is not an appealing target

Because it uses a non-Intel processor, and a non-Windows operating system, any attack on the clock would need to be very specifically designed as an attack on the clock itself. The amount of work involved exceeds the benefits obtained by such an attack.

1. Clock has Access to the Local Area Network (LAN)

The primary communications method for getting data onto, and off of the clock is a normal TCP/IP network connection. This allows other programs on the LAN to communicate with the clock. It also allows the clocks to communicate with each other.

Web Server

The clock contains a web server. This allows you to access the clock from any other PC on the LAN which has a browser installed.

PC Server

The clock contains a second server designed to be used by other PC software, for example Time and Attendance software, or Access Control software. The clock can also be configured to push data to the other PC program using whatever port number is required by that program.

P2P Server

The clocks are able to speak to each other using a built-in Peer-To-Peer server. This allows the clocks to synchronize direction (allowing employees to clock-in at one clock, but clock-out at another.) Other information necessary for the clocks to work together is also distributed using this server.

Telnet Server

The clock contains a built-in Telnet server. This server allows for extremely low-level access to the device

and is useful for trouble-shooting. However this server is password protected and is only used in extreme circumstances.

Risks involved

There are no significant risks to having the clocks access the LAN. They are unable to “catch” PC viruses or run malware designed for any PC (Windows, Linux or any other operating system).

Technical Information

The web server allows incoming connections, using the HTTP protocol on a configurable TCP Port (default is 80). Web browsers connect to the web server. The web server is unable to make outgoing connections.

The PC Server uses a proprietary protocol on a configurable incoming TCP port (default is 5123). Alternatively, or in addition to this, the PC Server program can make outgoing connections to a specified IP address, on a specified TCP Port.

The P2P server uses the proprietary protocol over “PC Server port +1”, the default port is thus 5124. Since it is Peer-to-Peer it allows for incoming, and outgoing connections on this port.

The Telnet server uses an SSH encrypted connection over Port 22 and is password protected using a better than 148 bit password.

The protocol used by the PC Server and P2P server is documented in the CS TimeClock SDK.

2. Clock has access TO the Internet

There are 3 reasons why having access to the internet is advantageous to the user.

Get Time from the Internet

There are a number of servers on the internet dedicated to providing very accurate time measurements. These are commonly known as Internet Time Servers. Their job is to allow electronic devices, like computers, to maintain a correct time and date. The CS TimeClocks are able to fetch the time from up to 4 time servers, and thus maintain a completely accurate time on the clock, without manual intervention.

The clock automatically fetches the time from the internet from time to time, and in addition you are able to manually request a time update via the keypad.

> **Aside:** Although the clock can make use of the Internet time, it does not rely on it. The Time and Date can be set via the keypad, and the clock has an internal real-time-clock which maintains an accurate time even if the clock is turned off.

Get Firmware Updates

From time to time new functionality is added to the clock, and any errors in the firmware are corrected. This new firmware goes through a stringent testing process before being released for general use. If the clock is attached to the internet then a firmware upgrade can be requested by a clock administrator (and only a clock administrator) from the keypad.

Firmware updates do not happen automatically, they must be requested by a user. There is thus no danger of the clock "changing" without the user being involved in the process.

Communicate with Remote PC Software

The clock is able to initiate connections with remote PC software. The remote PC software has to allow incoming connections, and also has to be aware of the CS TimeClock communications protocol. Often this software is installed on the LAN, however it is possible to install the PC software on a remote computer allowing the clock to access it via the WAN or Internet.

Risks Involved

The risks involved with the clock making outgoing connections via the internet are lower than the risks of a normal PC accessing the internet. The clock is unable to browse web sites. It has a non-X86 processor and thus is unable to run programs compiled for a PC. It cannot catch any virus for PC, Mac or Linux.

The firmware itself is fetched from a secure site using SSL, which is the same encryption used by banks for internet banking.

The specific sites, or IP numbers used by the clock are specifically set, either to the default factory setting, or to addresses specified by the user. It cannot access any other machines on the internet.

Technical Information

Summary:

Outgoing ports 37,443, 5123 and 5124 should be open from the clock for maximum functionality.

This section contains port information which is useful for network administrators. Firewalls and Routers may need to be configured to allow outbound access for these features.

The internet time function uses a standard Linux utility, called rdate, to fetch and set the time. It uses port 37. Outgoing TCP connections on Port 37 are required for this function to work.

The firmware update function uses the standard HTTPS protocol, on port 443. Outgoing TCP connections on this port are required for this function to work.

If the clock initiates connections to remote PC software, then the Port number used by the software needs to be opened. This port is usually configurable at both the PC Software and Clock ends so any suitable port number can be used.

3. Internet has access TO the Clock

Communication with other clocks, and programs, on the LAN as well as making outgoing connections to make use of the internet should cause no anxiety from the user's point of view. These are normal operations conducted every day by hundreds of millions of computers all over the world.

However allowing programs to access the clock, and initiate connections with the clock, from anywhere on the Internet is another proposition altogether. This section describes the benefits to allowing outside access, and discusses the risks involved.

Remote Management of the Clockings and Hours

If you allow remote access to the web server then this allows staff to monitor, and manage the clockings from a remote location. This is useful for business owners wishing to check the clock from home, or for wage officers who are not on site.

Aside: For small companies, that have no on-site computer at all, it's worth getting Internet Access just for the clock. This allows the owner, or payroll officer, to do all the administration from home.

Remote Support

From time to time you may wish to make use of the support services offered by your clock supplier. Their ability to provide you with fast, accurate information is greatly improved if they can access the clock directly, via the internet, from their own office.

Remote Clocks

If you have multiple clocks, and multiple sites, then the clocks are able to synchronize information with each other, even if they are on a WAN. This may be useful where you have staff moving between sites. This allows an employee to clock in at one clock, and clock out at another. In many cases making use of the internet as the WAN makes sense from an economic point of view.

Risks Involved

Opening ports that allow incoming network connections are inherently the most risky thing you can do on the internet. However this risk needs to be quantified in specific situations. Just like crossing the road is always risky, some roads are more risky than others. Crossing a busy freeway on foot is considerably different to crossing a quiet country road.

Attempts to "hack" a system fall broadly into two categories. Some attacks manipulate the device, doing exactly what the device was programmed to do, by using a valid login and password. The second attack gets the device to do things it was not programmed to do, by "exploiting" a hole in the program hosting the port.

If a malicious person gets the login and password of one of the processes, then they are able to corrupt the data on the device, but that's the limit of their action. They cannot make the clock do something it was not programmed to do. In the case of the clock the worst that can happen is that they trash the database and you have to restore the database from a backup.

It should be pointed out that the usefulness of this sort of attack is minimal. The attacker gains nothing from doing this, and it is "uninteresting" to them in the first place. The most likely person to do

something like this is a disgruntled employee who has been issued a login anyway. (And most employee logins limit their access to only themselves, so the damage would be minimal.)

The second form of attack is a lot more common precisely because it is more useful to the attacker. By implanting a program of their own on the device they are able to do things which have commercial value – for example by sending SPAM. This sort of attack is extremely hard to do, and requires a lot of skill to create.

The CS TimeClock however makes a very poor target for this sort of attack. Everything about it is unlike a PC, and this makes it invulnerable to attacks designed for PC's. It would take as much work to design a hack for a CS TimeClock as a PC (possibly more) and the result would be an attack on several thousand devices. A similar effort expended on attacking a PC would result in the number of potential targets exceeding several hundreds of millions of machines.

Opening the web server on the clock (running on Port 80) allows remote users to access the web interface on the clock. It also allows support staff to see the data on the clock, and assist where necessary. Opening access to the web server does not grant access to the device as a whole. External users can only run the specific functions that the web server was programmed to perform. There's no "magic code" that can make the web server perform functions it was not designed to do.
It's worth pointing out at this stage that the whole internet is flooded with web servers, indeed they are the primary server running on the internet today. Security for web sites is a well understood problem, and web servers are typically highly secure programs. The benefits of hijacking the web servers of the world are literally enormous, so the fact that most sites are never hacked is a sign of how good their security is.

Technical Information

Summary:

Incoming ports 22, 80, 5123 and 5124 should be open to the clock for maximum functionality.

The web server uses the standard web port, Port 80 by default. Therefore incoming connections on port 80 are desirable. (This port can be changed if necessary)

The CS TimeClock support staff use the PC Software port (default 5123), and any remote software will use this port as well. This port number can be configured to a different port number if desired.

If you have multiple clocks speaking to each other over the WAN then they use PC Software port + 1 (ie 5124 by default.)

The Telnet connection uses port 22.

If you wish to know more about the servers or protocols involved please ask your supplier.