Wireless Monitoring System *by TempSys*

Security Analysis for the

CheckPoint Wireless Monitoring System

Document No. D1631

Rev. A

April 3, 2012

TempSys, Inc. 5701 Hollis Street, Emeryville, CA 94608
support@tempsys.net • (510) 526-7624 • www.tempsys.net

Introduction

This document explains the security process incorporated in the CheckPoint 900 MHz Wireless Monitoring System and how we address the vulnerabilities that could exist in such a system. We believe our system will not pose a threat to the customer's enterprise computing infrastructure.

System Description

The CheckPoint Wireless Monitoring system consists of three essential components:

- Battery operated Wireless Sensors operating at 902-928 MHz
- Ethernet enabled Access Point
- Checkpoint Service running on a PC or blade server

There are also Repeater units within the wireless network, but for this discussion they are functionally equivalent to Sensors. The following shows a typical installation setup (Figure 1).

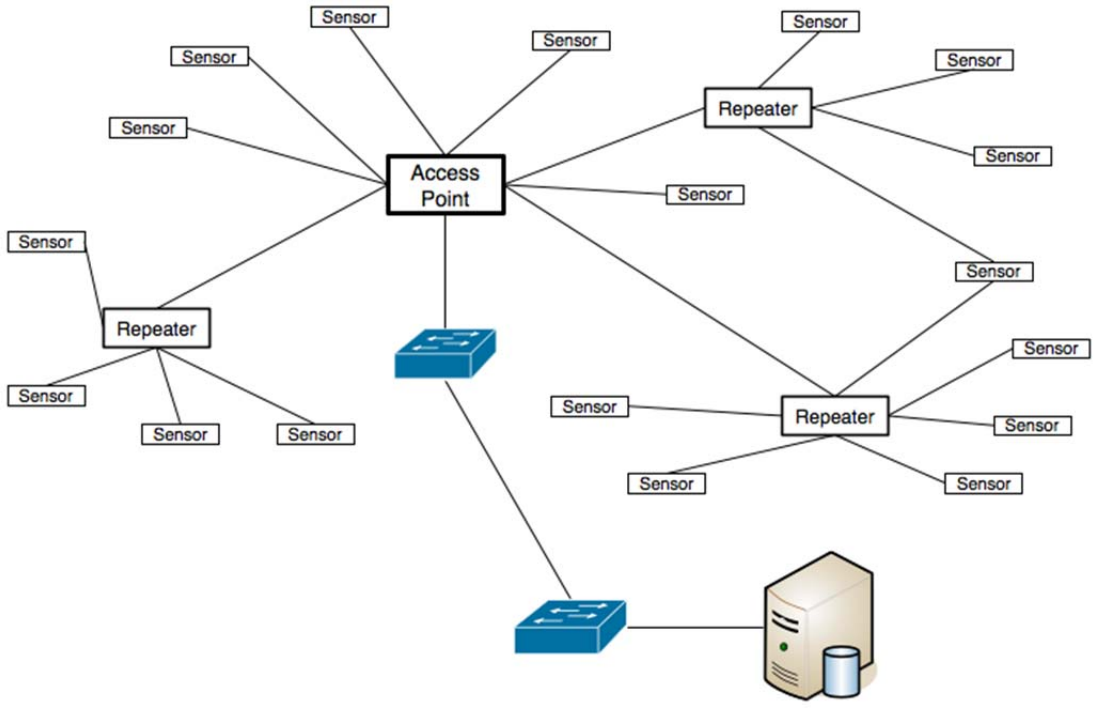

Figure 1 – Typical Installation Setup

TempSys, Inc. 5701 Hollis Street, Emeryville, CA 94608
support@tempsys.net • (510) 526-7624 • www.tempsys.net

Wireless Sensor

The sensor unit consists of a small 8 bit Harvard Architecture micro-controller and a radio IC. The micro controller runs very simple code directly out of ROM, waking up at a pre-programmed interval, taking a sensor reading, then transmitting the data toward a selected Access Point. The data packet consists of a RadioID identification word, a time stamp, up to five data points (sensor readings), and a Checksum. The data packet has a maximum length of 48 bytes. A transmission can contain up to five concatenated data packets with a maximum of 120 bytes total per transmission.

Access Points

There are two components to our Access Points, the radio unit and an Embedded Linux system running a minimum of services.

The radio unit is architecturally identical to the Sensor, with the same 8 bit Harvard architecture micro-controller and radio IC. Its purpose is two fold: first to transmit an identification beacons at periodic intervals, and second to receive transmissions from the Sensors and Repeaters and forward the data to a custom Linux application over a serial port link. The data format used between the radio and the Linux application is in human readable ASCII text format.

The embedded Linux system provides a number of features including local non-volatile storage of wireless data and the ability to use DHCP/domain naming services to greatly simplify the installation and maintenance of the system. The only Ethernet enabled services running on the device are SSH on a non-standard port and our custom application which encapsulates the ASCII data from the radio into UDP packets which are sent to the Checkpoint Service.

Checkpoint Service

The Service runs on a single (or protected) PC or blade, receiving UDP packets from the Access points, processing the ASCII data, and placing it into the SQL database.

System Operation

The Checkpoint Service must be configured before the system can operate:

- The Serial number of every Sensor is associated with a physical object (refrigerator or other asset) and entered into the Checkpoint database.
- The IP address of every Access point is also entered into the Checkpoint database.

TempSys, Inc. 5701 Hollis Street, Emeryville, CA 94608
support@tempsys.net • (510) 526-7624 • www.tempsys.net

At system start, all devices (Wireless sensors and Access Points) are in a listening only mode. The following steps are then followed:

- The Service program sends an identifying UDP packet to all Access Points previously entered into its database.
- The Access points respond and the handshake is complete.
- The Access points are now activated and begin to transmit wireless beacon messages.
- Sensors and Repeaters hear the beacon and being operation, replying to the base Receiver or Repeater with the strongest beacon.
- The Access Points send wireless data only to the Checkpoint Service IP.

The take away here is that only Access Points that are known in the system are activated and able to communicate with the Service. And only those sensors which are pre-configured will be entered into the database. Un-configured Sensors will not be processed by the Service.

Security Measures

While we do not encrypt our data over the air, we believe the system is secure to outside attack.

We are using simple 8 bit Harvard architecture micro-controllers on all the radio devices. By definition, this means that execution code can only reside in the embedded flash memory. Short of physical access to the device, there is no conceivable way to change the factory programming of any radio device. As such the Sensor device will always send the type of data that they were programmed to send.

At the interface between the CheckPoint Wireless network and the customer's enterprise network, the communication link is a slow speed (19200 baud) serial port sending a specifically formatted ASCII datagram.

The Radio in each Access point is designed to receive data generated by our Sensors and Repeaters using a proprietary air protocol. Upon reception of a radio transmission, the radio checks that the message's destination address matches that of the receiver and that the air protocol's CRC matches. If it does, it will process the packet into an ASCII representation of the received binary data using a defined frame format and a human readable datagram descriptor. An example of the two expected datagram types is:

<data:2012e3f7 ed5c5812 01 c7 01 a1 5944>
<status:2012c712 ed5cc712 01 c7 01 a1 83a7>

TempSys, Inc. 5701 Hollis Street, Emeryville, CA 94608
support@tempsys.net • (510) 526-7624 • www.tempsys.net

Should the receiver receive a packet that conforms to our air protocol, has the proper destination address, and has a valid CRC, the receiver will output the data with the following datagram descriptor:

<unknown 69 f860582 82b9fa01 41 64 61 02 00 00 13 41 35 ae 1a6f>

Note that this method of using ASCII to represent *all* received binary data results is a character set of only 16 symbols [0-9][a-f] between the radio network and the enterprise network. Further, the maximum length of this ASCII message is 48 bytes. Even if the receiver gets a longer transmission of concatenated packets, it will output each datagram individually to our Linux application.

Once received over the serial port, the Linux application simply encapsulates the exact ASCII datagram into a UDP packet which is forwarded to the Checkpoint service. Therefore even over the Enterprise network, we are transporting all data received at an Access Point using the limited character set [0-9][a-f].

At the Checkpoint Server, the received UDP encapsulated ASCII datagrams are extracted and processed according to the human readable datagram descriptor. If the packet descriptor is <data...> then the data is parsed and stuffed into the database. If the packet descriptor is either of the other two (<status...> or <unknown...>), the service does not even parse the message beyond the datagram descriptor but simply writes this information to a text based Log file and moves on to the next message.

The Linux based Access Point

The embedded Linux AP is running a recent version of the kernel (2.6.30) and has a minimal set of services running on it. The unit should only respond to specifically formatted ASCII data on port 1324 (sent by the Checkpoint Service), and SSH requests on a non-standard port. There are no other listening services running on the device such as a Web or FTP server. SSH is run using embedded dropbear implementation, and access by the root account is disabled. The root account is not shared outside of the development team (it is not ever needed in the field), with a 12 character high entropy random password using all available letters, numbers, and symbols. The password for the user account can only be set with physical access to the device using a USB cable connected to a Terminal program on a PC. We encourage each customer to customize the password for each of their APs. SSH is primarily used to perform remote diagnostics (i.e. read log files) and to apply software patches to the system. Software patches are encrypted by Tempsys and must be successfully decrypted by the AP using a private key before they are applied.

The entire Linux root file system is running from a RAM drive on our AP. During boot the contents of a protected flash partition are expanded into the RAM drive and the boot started

TempSys, Inc. 5701 Hollis Street, Emeryville, CA 94608
support@tempsys.net • (510) 526-7624 • www.tempsys.net

from there. If a patch file exists, it will be decrypted during boot and applied to the RAM based file system. As such, a reboot will always bring an AP back to the known factory state.

What-If Scenarios

Scenario #1 - A CheckPoint Sensor Falls into the "Wrong Hands"

- In this scenario, someone has a sensor and wishes to inject data into the network. There is nothing stopping them from doing this, however if they are running our standard firmware, they will simply generate known packet types which will be received by the Access points and forwarded to the Checkpoint Service. The Service will check for a match of the RadioID to the pre-configured database, and since they won't match the datagram will be written to the log file and then dumped.

Scenario #2 - Reverse Engineers Sensor Firmware

- We expect this to be very hard to do. First off, the contents of the Flash memory are protected from read-back. An attempt to read the flash memory will only result in random garbage, not the actual contents. So direct reverse engineering would not be possible. They could develop a complete new application using the Sensor hardware and our RFIC, but even if they were able to generate packets that conform to our unpublished air protocol, these packets would likely result in <unknown...> messages which are dumped on the floor by the Checkpoint service. Even if they recreated a <log_sensor_data...> message, the contents of that message are well defined and if the Service can't parse the ASCII datagram, it will just write it to the log file and dump it.

Scenario #3 - Unauthorized SSH Access to the AP

- For this to occur, the intruder would have to already have access to the enterprise network. Our embedded Linux system would be a rather minor target relative to everything else an intruder would have access to within the network. Once in, an intruder would then need to gain root access before much of significance could be done. If they did manage to setup some form of DoS or Spam Bot, a reboot of the device would erase everything and bring the AP back to the factory default state.

Conclusion

The CheckPoint 900 MHz Wireless Monitoring system has been designed to meet enterprise security requirements. Unauthorized access, although theoretically possible, is highly unlikely. With a proven security track record of over ten years in over 300 installed locations nationwide, CheckPoint security has met design and performance requirements.

TempSys, Inc. 5701 Hollis Street, Emeryville, CA 94608
support@tempsys.net • (510) 526-7624 • www.tempsys.net