Brief

Tech Café Market

Vending Machine Security

Basics of Machine Communication

The HP supply vending machine is used in employee work areas for the distribution of Personal Protective Equipment (PPE), tech peripherals or other items as required. The machine is a spiral-based vending machine that dispenses a product after an employee has been authorized by entering their authorization number via keypad, prox card, or barcode card. When an employee enters their authorization code, the machine requests verification of the employee's number from the server. Once verification is received by the machine, the employee may dispense a product. Once the product is dispensed, the machine sends the transaction information, including date-time stamp, authorization number, and item vended, back to the server.

Internet Connectivity

For the dispenser to communicate with the server, an Internet connection must be set up. The dispenser is equipped with a 10/100BASE-T Ethernet adapter that communicates using TCP/IP over Port 80.

Port 80 on the client firewall must be open to allow proper communication between the server and the dispenser to approve each and every transaction. The machine network hardware is capable of both STATIC and DHCP for configuring a network TCP/IP address.

If the dispenser loses communication, all transactions will be saved in flash memory on the dispenser's controller. When the machine reconnects to the server, the data will be uploaded to the server database and available for reporting.

If a proxy server is implemented at the client site, it must be transparent proxy otherwise the client must allow the vending machine to circumvent the proxy.

The dispensers will only establish connections with a specific back end server (www.vendnovation.com), whose IP address is **50.112.128.240** (hosted in the Amazon cloud). Network administrators are free to restrict the device's communications to this address.

Alternatives to a wired network

The advent of cellular broadband networking has broken down barriers for organizations whose IT policies strictly forbid 3rd party devices on the corporate infrastructure.

Using cellular air card and broadband adapter, or an available single purpose cellular device, HP is able to connect the vending machine directly to the Internet without connecting to the client's internal network. This solution is best where a strong cellular data connection is available.

Security

- The dispenser will not initiate a connection with an incoming communication. It will only establish a connection with a specific IP address using secure keys and an established handshake.
- The message through which the data is sent is encrypted using both 128-bit Advanced Encryption Standard (AES) encryption as well as RSA Cryptography schemes. Meets US Government (NSA) certification for securing classified information.
- The dispensing device manufacturer utilizes a proprietary architecture that is simply not compatible with any general-purpose computer operating system including: Microsoft Windows®, UNIX and its variations or Novell®.

Furthermore, the dispenser's controller is designed in such a way as to require manual intervention on the vending machine before any configurations or programming can be sent to the controller. In this way, it is impossible for hacker to download a virus to the terminal.

Message Encryption

The dispensing solution encrypts data using a combination of RSA-2048 and AES-128. The data is transmitted over HTTP (TCP 80). Included in the payload is a digital signature (using RSA-2048) to prove that the client is a known device. All data sent to or from the device is encrypted in this manner.

AES keys are randomly generated and exchanged every time the device contacts the server.

A typical transaction with the server will send a total of about 2 kilobytes of data.

Summary

- A Local Area Network (LAN) connection must be available.
- TCP Port 80 must be open to access outbound.
- Proxy server authentication is not supported, and a proxy server workaround must be implemented using a static IP address.
- The connection at the network switch must be set to auto detect. The controller network adapter is capable of 10/100/1000 Mbps connectivity.

Sign up for updates
hp.com/go/getupdated

Share with colleagues

4AA7-1419ENW, October 2017