Cell Power Auditor
Installation Overview

Version 2.0

Cell Power Auditor Installation Overview

Document Revision: 201206.1

Expertron Group (Pty) Ltd

The Innovation Hub, Enterprise Building, 6 Mark Shuttleworth Street, Persequor Ext 10, 0020, South Africa

Tel: +27 12 844 0330

Fax: +27 12 844 0331

Web: http://www.expertron.co.za

Email: info@expertron.co.za

Table of Contents

1 Introduction

Cell Power Auditor is a transaction auditing system for monitoring and logging deposit and purchase transactions between 3rd-party electronic voucher resellers and the electronic voucher provider.

Cell Power Auditor is implemented as software that runs on one or more standard computer servers.

Cell Power Auditor can be used by Electricity Utilities and Municipalities to provide an independent audit trail of all deposit and sales transactions performed by 3rd-party resellers of prepaid electricity. The reports provided by Cell Power Auditor can be used as an independent reference to resolve disputes which may arise from discrepancies between the logs provided by the Utility's electricity voucher generation system and the 3rd-party reseller's vending system.

Cell Power Auditor can also be used by prepaid airtime wholesalers to provide an independent log of all deposit and sales transactions performed by 3rd-party resellers.

2 Audience

This document describes how Cell Power Auditor can be implemented in a data network, and to assist the parties responsible for the information and telecommunications technology infrastructure where Cell Power Auditor is to be implemented.

3 Implementation Architecture

There are two ways in which Cell Power Auditor can be installed. In both cases, it is assumed that the auditor will (and should be) installed within the data network of the electronic voucher supplier (e.g. airtime network operator or utility).

3.1 Vending Proxy Installation

Cell Power Auditor can be installed in-line within the live transaction stream as a vending proxy server. This means that connections from external 3rd-party vending systems are terminated on Cell Power Auditor, and then proxied to the internal electronic voucher source. This is illustrated in Figure 1. Note that SSL-encrypted communications from 3rd-party vending systems are also terminated on the auditor.

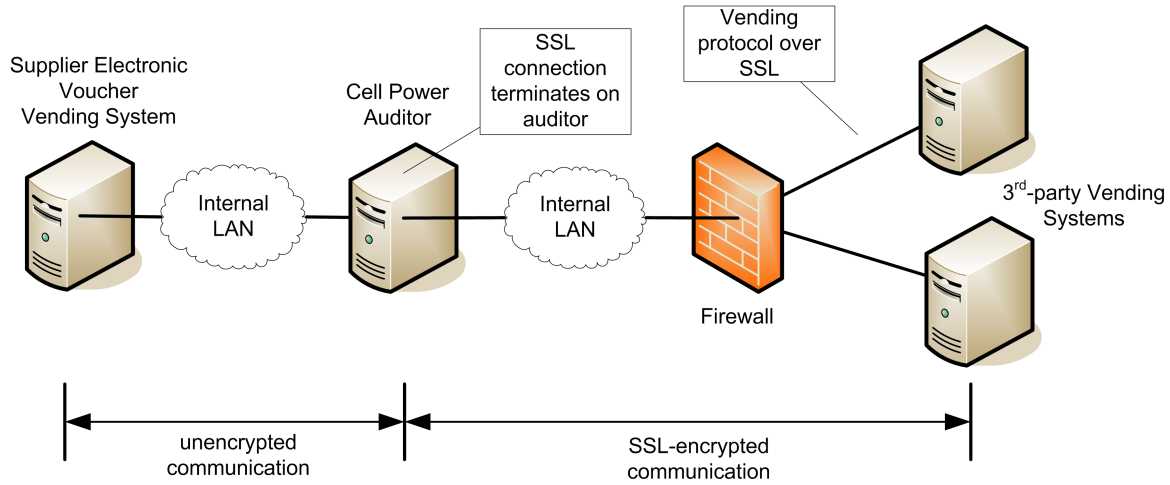

Figure 1: Vending Proxy installation

This solution has the following advantages and disadvantages:

3.1.1 Advantages

- Cell Power Auditor can operate as an active vending platform, and can control the sales transactions flowing through it based on the prepaid balances or credit limits of the 3rd-party resellers registered on the auditor.
- The auditor cannot easily be bypassed, as both internal and external systems would need to be reconfigured.
- The auditor presents the non-proprietary XMLvend API to external 3rd-party vending systems.

3.1.2 Disadvantages

- Cell Power Auditor intervenes directly in the transaction flow by terminating and processing inbound requests from external systems, and forwarding proxy requests to the internal vending system. This may compromise its perception as an independent auditing device.
- The auditor represents an additional vending platform in series with the normal transaction flow, and presents an additional risk of failure equitable with the internal supplier vending system, and with a complex failure mode recovery model.

3.2 Passive Listener Installation

Cell Power Auditor can be installed as a passive listener (“on a stick”) that does not interfere with the direct transaction stream. In this configuration, the auditor is connected to the transaction stream via a port that mirrors all the traffic between the 3rd-party system and the electronic voucher source. This is illustrated in Figure 2.

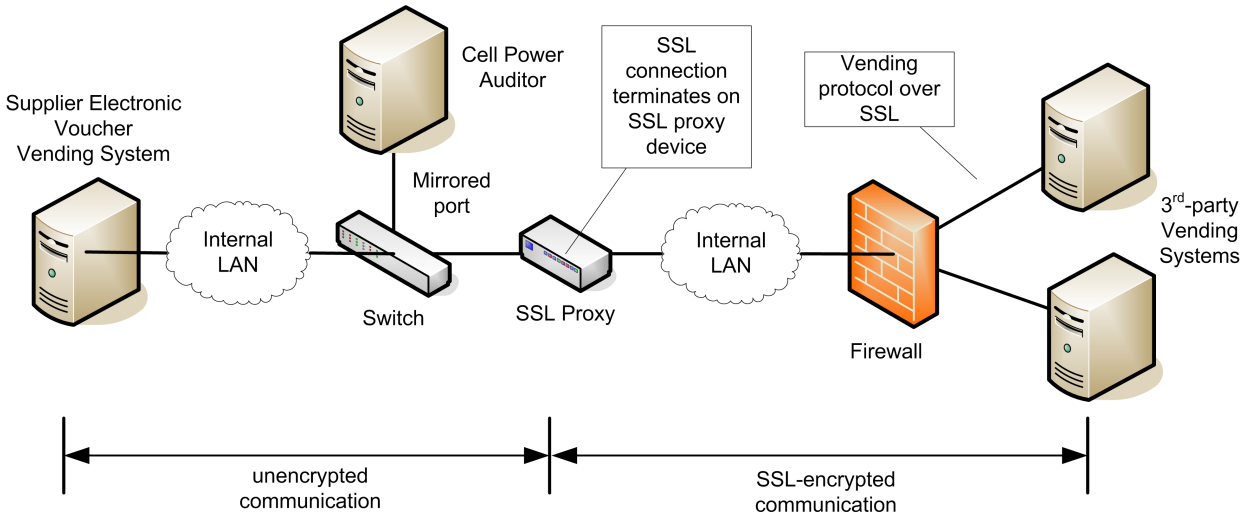

Figure 2: Passive Listener Installation

This installation will require the following changes to the existing networking infrastructure:

- SSL-encrypted communications from 3rd-party vending systems must be terminated (and decrypted) before the auditor. This can be achieved with a 3rd-party SSL proxy device; various products exist in the market, or alternatively, such a device can be implemented using SSL tunnel software (e.g. stunnel) on a standard computer (Windows or Linux).
- A port will have to be configured on the switch (layer 2 infrastructure) to mirror all traffic flowing between the 3rd-party system sand the electronic voucher source

This solution has the following advantages and disadvantages:

3.2.1 Advantages

- Cell Power Auditor passively monitors all transactions in such a way that there cannot be any interference with the monitored traffic stream, and provides a truly independent audit of a process that the auditor itself does not actively participate in.
- The auditor does not lie within the critical data path, and hence, the failure mode recovery model is much simpler: multiple auditors can be installed, each to autonomously monitor data streams mirrored on different ports.

3.2.2 Disadvantages

- The role of Cell Power Auditor is limited strictly to transaction monitoring and logging, and cannot play a role in actively controlling transactions based on the credit balances of 3rd-party vendors whose deposits are recorded on the auditor.
- The auditor can be easily disconnected from the data stream without actively disrupting the flow of the data stream, and without any configuration changes on external and internal vending

systems either side of the auditor. However, this can be mitigated to some extent by triggering alarms if no transactions are monitored within certain thresholds.

- The auditor cannot be used as a vending protocol gateway to translate proprietary vending protocols to the non-proprietary XMLvend open standard.

4 Infrastructure Requirements

The Cell Power Auditor must be implemented on server-class hardware. The auditor can be installed on a single server, or on multiple servers depending on the failure mode requirements. Multiple servers can be configured to share the same database (for the in-line installation), or operate autonomously (for the passive listener installation).

Backups are dumped daily, and can be stored on the local hard drives, external USB drives, a Storage Area Network, or copied to a remote site. Database log tables are rotated and archived on a daily basis.

4.1 Server Specification

4.1.1 General minimum recommended hardware

- Servers must make provision for up to 6 hard drives per server, with hardware RAID interfaces capable of supporting multiple RAID-1, -10 and/or -5 arrays.
- The fastest available SAS hard disk drives are recommended.
- Dual power supplies are recommended.
- Reliable power source with UPS backup is recommended.
- External USB hard drive for backups attached to each database server (500GB SATA hard drive per backup drive recommended), unless backups can be copied directly to a local Storage Area Network (SAN).
- Server chassis should provide at least 4 hot-swap hard drive bays.
- GSM modem (USB or RS-232 interface) for SMS alarm notifications

4.1.2 General software requirements

- Operating system: SuSE Linux operating system (SLES 11 or OpenSuSE 11)
- All other software to be installed by Expertron from Linux distribution, or provided by Expertron.

4.1.3 Recommended minimum hardware specification

CPU	2 x dual-core +2GHz Xeon, or 1 x quad-core +2GHz Xeon
RAM	8 GB ECC
Storage	1 x +200GB RAID-1 array 1 x +500GB RAID-1 array