Contact Information

publications@ipcg.com

ipCapital Group, Inc.
400 Cornerstone Drive, Suite 325
Williston, VT 05495
United States of America
(802) 872-3200 x214

TITLE

VPN Sales System

ABSTRACT

An operating system module secures online transactions by establishing a VPN connection between the User Machine and the online Vendor Server.

1. BACKGROUND

Problem or Opportunity

The massive popularity of e-commerce and internet shopping has lead to an epidemic of credit card and identity theft. Due to this rampant online identity theft, many potential online customers are skeptical and uneasy with online sales, leading to reduced sales volume for online merchants.

While current secure internet protocols, such as https, provide for user-end security and privacy within the user's browser window, information being transmitted over the internet to vendor website servers may still be compromised. Because the internet as a whole is largely non-secure, even data encryption may sometimes fail to protect sensitive information. What is needed is a means of conducting transactions over a secure network such that internet and website security are not topics of concern.

Background Publications

The publications described below attempt to address the problem of transactional security using VPN connections. However, none of the existing literature specifically extends VPN security for to individual customers for conducting online transactions.

US Patent Application Number 20070234061 describes a method for providing transaction security from the user end. Extra security techniques are turned on when there is a need for a secure online transaction. A party other than the end user pushes the security mechanism to the end-user. This adds extra security to the user end of a transaction with minimal effort on the part of the user. This invention mentions a variety of security techniques, including VPN

connections, but it does not specifically address the use of VPNs for transactions between a user and a vendor.

US Patent Application Number 20020023004 describes a system for managing a group of stores. In this invention, an individual may manage a group of stores from home by establishing a VPN between all stores and the home computer. This invention uses VPN to manage transactions between stores and managers, but does not extend this same security to online customers.

2. SUMMARY OF THE INVENTION

Invention Summary

The Operating System contains a Sales Manager Module, which is in charge of verifying an online Vendor's identity and establishing a secure connection with the online Vendor's sales server. Rather than transmit sensitive information using standard internet protocols where such information could be compromised, the User Machine connects to the Vendor Sales Server using a remote access Virtual Private Network, through a VPN Access Server.

When a user wishes to purchase products online from a given Vendor's Website, the user enters any non-sensitive information, such as name, login information, shipping information, e-mail etc., into the Vendor's online checkout system as they would in a typical online transaction. The user submits this information through the Vendor Website, and this information is then transmitted from the Vendor Website Server to the Vendor Sales Server. The Vendor Sales Server then generates an Access File for the VPN Access Server based on the User Machine's IP Address using the Access File Generator. This Access File is then sent to the user as an email attachment.

When the user opens the Access File from their email, the Sales Manager Module is invoked by the Operating System. Using information from the Access File, the VPN Client within the Sales Manager Module establishes a connection with the VPN Access Server over the internet. Once a connection has been established, the Sales Manager Module opens its GUI, where the user can then enter his or her billing and payment information.

Before the user submits his or her payment information to the server, the user is presented with an order summary. After submission of the payment information, the server notifies the User Machine if the transaction was successfully completed. The Sales Manager Module then terminates the VPN connection, and the Vendor Server flags the given Access File as invalid in order to prevent repeated access to the VPN using the same Access File.

Unique Concepts

The present invention is unique in that it provides a method of providing high security for online transactions between an individual customer and a merchant website using VPN connections. Previous inventions have used other, less secure methods for conducting these transactions.

3. DESCRIPTION OF THE INVENTION

Figure 1 illustrates the structure of the Sales Manager Module System.

1.1 User Machine: a processing device, such as a desktop or laptop PC, running an Operating System (i.e. Linux) with a Graphical User Interface and internet connectivity.

1.2 Operating System: The Operating System running on the User Machine, responsible for managing all hardware and software operations, and for managing the Graphical User Interface. Also contains the Sales Manager Module.

1.3 Sales Manager Module: OS Module responsible for establishing and conducting secure online transactions. Acts as a client for access to the Vendor Sales Server through a VPN Access Server.

1.4 VPN Client: Program within the Sales Manager Module, used to establish a Remote Access VPN connection between the User Machine and the VPN Access Server to access the Vendor Sales Server. Uses the Access File generated by the Vendor Sales Server.

1.5 GUI: The Graphical User Interface of the Operating System.

1.6 Vendor Website Server: A Server on the internet which contains the Vendors Website (not pictured), used for showcasing and selling products online.

1.7 Vendor Sales Server: A Vendor Server, located on the Vendor's local network with remote access through a VPN, dedicated to handling sales requests. Allows customers to connect through the VPN Access Server

1.8 Access File Generator: Program running on the Vendor Server, uses the IP Address of the User Machine to generate an Access File for the User Machine to access the Vendor Sales Server over the VPN Access Server.

1.9 E-mail Server: An e-mail server residing on the internet, responsible for mail delivery.

1.10 VPN Access Server: A Network Access Server, maintained by the Vendor, authenticates users based on their VPN Client and Access File data. Allows for secure connection to the Vendor's local network to allow for secure data transfer through a series of internet servers.

1.11 Internet Servers: A plurality of internet servers, used as a secure path over which the VPN can transport data.

1.12 Access File: (Not Pictured) A data file generated by the Access File Generator on the Vendor Sales Server, based on the User Machine's IP Address. Contains the access information for the VPN Access Server, such as the address and login information, which allows the Sales Manager Module to connect to the VPN Access Server.

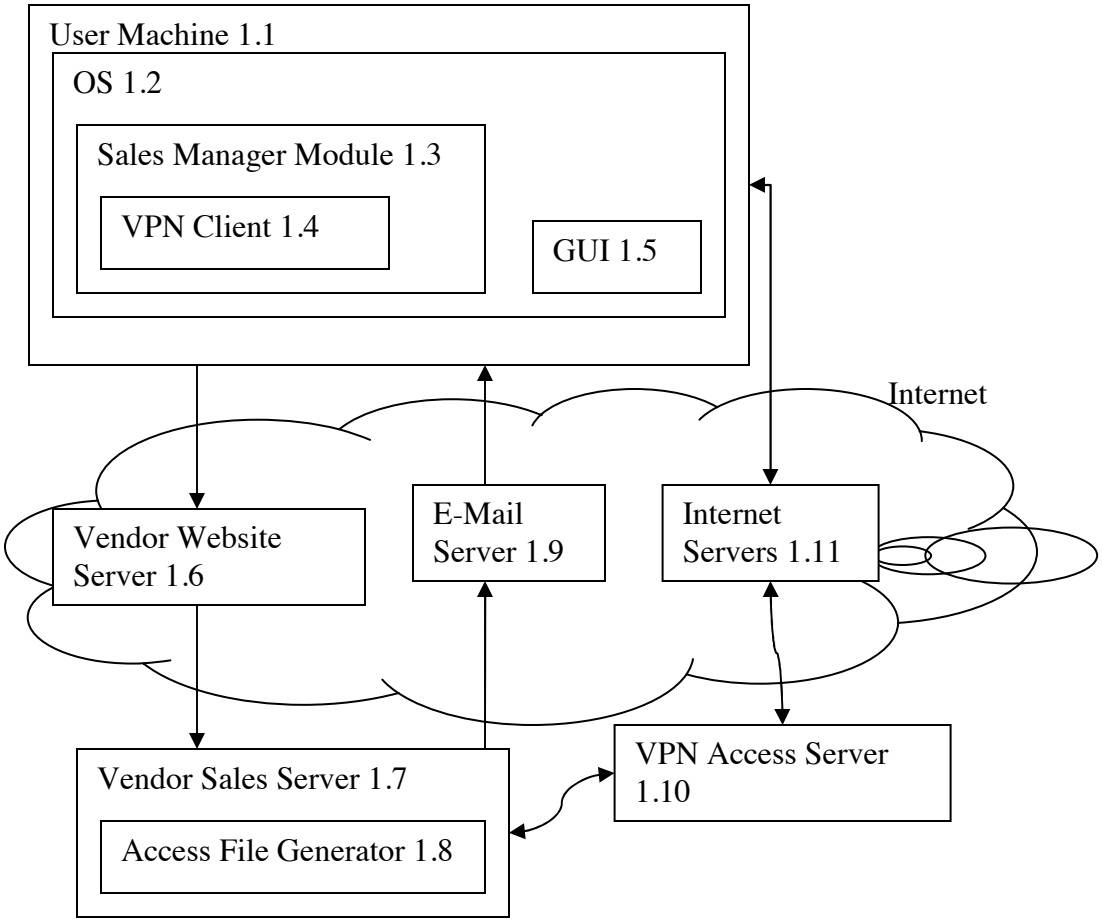

Figure 1: Structure of the Sales Manager Module System

The Operating System contains a Sales Manager Module, which is in charge of verifying an online Vendor's identity and establishing a secure connection with the online Vendor's sales server. Rather than transmit sensitive information using standard internet protocols where such information could be compromised, the User Machine connects to the Vendor Sales Server using a remote access Virtual Private Network, through a VPN Access Server.

When a user wishes to purchase products online from a given Vendor's Website, the user enters any non-sensitive information, such as name, login information, shipping information, e-mail etc., into the Vendor's online checkout system as they would in a typical online transaction. The user submits this information through the Vendor Website, and this information is then transmitted from the Vendor Website Server to the Vendor Sales Server. The Vendor Sales Server then generates an Access File for the VPN Access Server based on the User Machine's IP Address using the Access File Generator. This Access File is then sent to the user as an email attachment.

When the user opens the Access File from their email, the Sales Manager Module is invoked by the Operating System. Using information from the Access File, the VPN Client within the Sales

Manager Module establishes a connection with the VPN Access Server over the internet. Once a connection has been established, the Sales Manager Module opens its GUI, where the user can then enter his or her billing and payment information.

Before the user submits his or her payment information to the server, the user is presented with an order summary. After submission of the payment information, the server notifies the User Machine if the transaction was successfully completed. The Sales Manager Module then terminates the VPN connection, and the Vendor Server flags the given Access File as invalid in order to prevent repeated access to the VPN using the same Access File.

The flowchart in Figure 2 illustrates the operation of the Sales Manager Module System.

(2.1) The user clicks the "checkout" button on the Vendor's Website in a web browser running on the User Machine.

(2.2) The User enters any non-sensitive information into the text fields on the Vendor's Website, and clicks the "submit order" button.

(2.3) The Vendor Website Server transmits the data from the Vendor Website checkout system to the Vendor Sales Server, and the Access File Generator creates an Access File unique to the User Machine's IP Address.

(2.4) The Vendor Sales Server sends an order confirmation e-mail to the User, with the Access File attached.

(2.5) The User accesses his or her email, and opens the Access File attached to the confirmation e-mail. The OS recognizes the file as an Access File and proceeds to open the Sales Manager Module.

(2.6) Using the address of the VPN Access Server and the login information, as contained in the Access File, the VPN Client attempts to establish a connection with the VPN Access Server. If the VPN Access Server authorizes the user, a VPN connection to the Vendor Server is established, and the method proceeds to step (2.7). Otherwise, the VPN Access Server denies access to the User, and the method proceeds to step (2.12).

(2.7) With a VPN connection established, the OS opens a GUI window for the Sales Manager Module, containing text fields for the user to enter their billing and payment information.

(2.8) The user enters his or her payment information into the GUI of the Sales Manager Module, and clicks the submit button.

(2.9) The User Machine submits the information to the Vendor Sales Server over the VPN connection.

(2.10) The Vendor Sales Server processes the payment information, and notifies the User Machine of the success or failure of the transaction. If the transaction was successful, the method proceeds to step (2.11). Otherwise, it proceeds to step (2.12)

(2.11) The User Machine notifies the user that the transaction completed successfully within the Sales Manager Module GUI window, before closing the connection to the Vendor Sales Server. The Vendor Sales Server then invalidates the Access information, contained in the Access File, to prevent duplicate transactions. The method then ends.

(2.12) The User Machine notifies the user that the transaction could not complete successfully, with a brief message concerning the problem, through a pop-up dialog box in the Sales Manager Module GUI window. The Sales Manager Module closes the VPN connection, and the method ends.

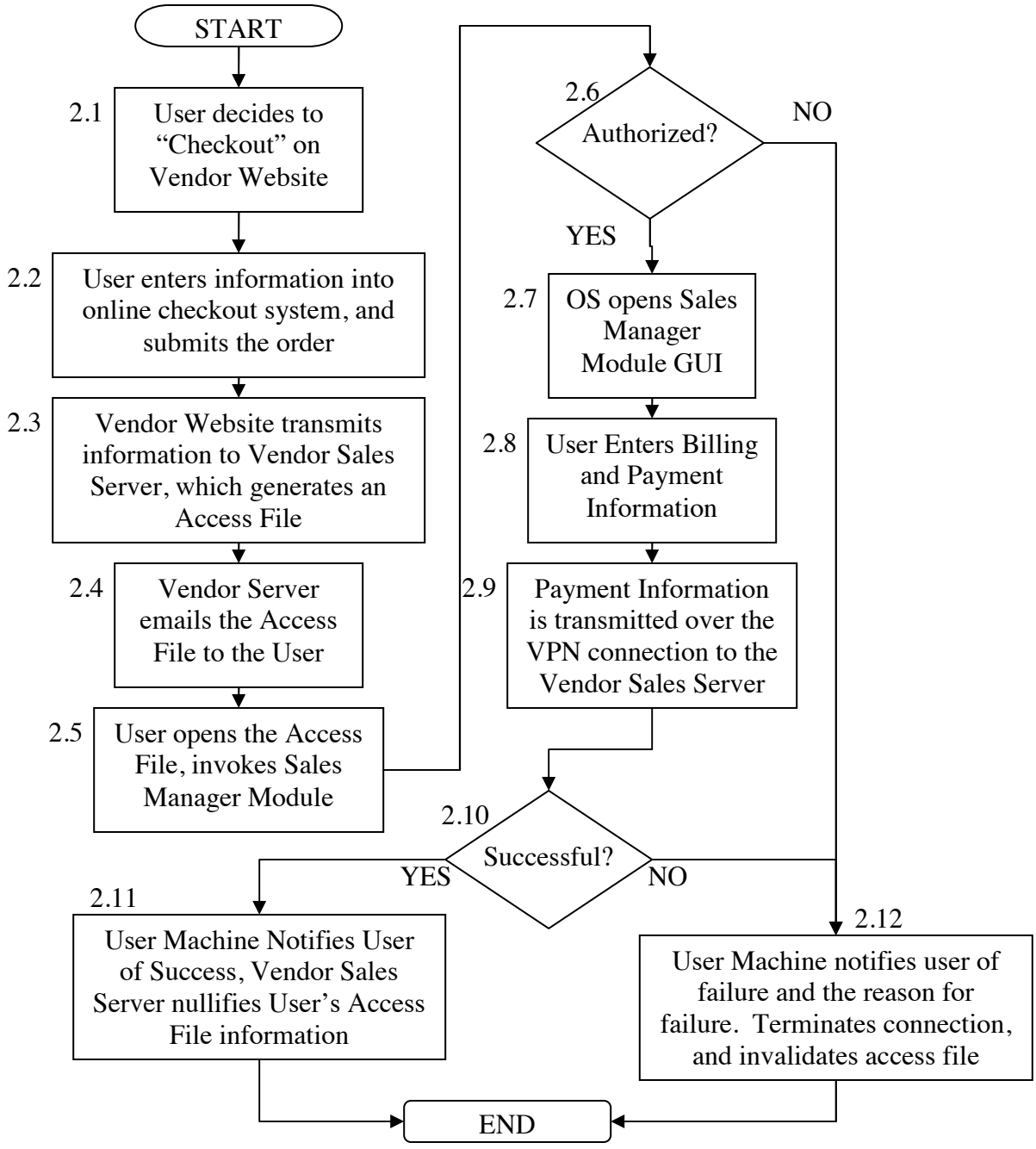

Figure 2: Operation of the Sales Manager Module System