StrikeForce Technologies, Inc.

Protect ID®

“Out-of-Band” Multi-Factor Authentication Cloud Services Whitepaper

□

StrikeForce Technologies, Inc.
1090 King Georges Post Rd.
Edison, NJ 08837, USA
Tel: 732 661-9641
Fax: 732 661-9647
http://www.sftnj.com

Table of Contents

Introduction

Organizations of all sizes are utilizing the Internet in ever-increasing numbers to boost business efficiency, improve communications with customers and partners, and connect remote offices and workers together. Applications are migrating to the cloud to take advantage of the economies of scale and the ease of administration. Security services are also moving to the "Cloud". Along with the increased push of regulatory bodies to mandate two factor authentication, this has created a need for a cloud based authentication service.

The purpose of this paper is to present the ProtectID® two factor authentication "Cloud Service" developed by StrikeForce Technologies.

The Drivers

The following are the major drivers for a cloud based authentication service –

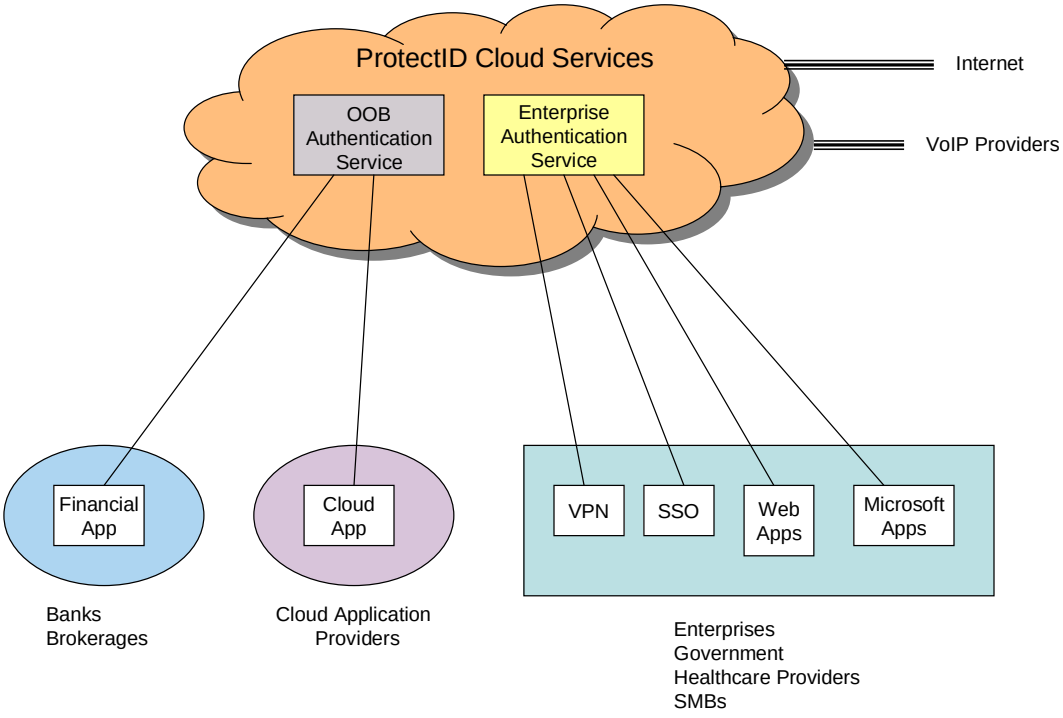
- ***Computer crime is increasing –*** Computer crime has been increasing steadily with a number of high profile hacks on company databases causing breach of identity and financial data. In addition, phishing, keylogging and man-in-the middle attacks have made consumers more vulnerable even though anti-virus software is widely deployed. The best way to prevent this is to deploy two-factor "Out-of-Band" authentication, as noted by the technology analysts.
- ***Regulatory drivers*** – The government is mandating two-factor authentication to control access to vital data via a number of directives including, - (1) FFIEC for financial companies, (2) PCI and FACTA Red Flag rules for companies that handle credit cards (i.e. merchants and processors), (3) HIPPA for healthcare providers, (4) CPNI for telecom providers, (5) NERC for energy utilities/companies and (6) SOX for public companies.
- ***Applications are moving to the cloud*** – Virtually every major (and minor) software vendor is moving their software to the cloud. Also, many enterprises and the government are deploying cloud based applications for their employees, customers and partners, increasing productivity and cost avoidance.
- ***Higher costs associated with in-house deployments –*** The advantage of a cloud service is that it is quicker to deploy and easier to administer. This leads to lower TCO and greater flexibility for the customer.

ProtectID Cloud Service Overview

The ProtectID "Cloud Service" has the following services -

- ***"Out-Of-Band" (OOB) Authentication Service –*** This service is targeted at companies that need to authenticate their customers. These include banks and brokerages that need to comply with FFIEC and Red Flag regulations and cloud application providers that need better security than a password. In this scenario, the authentication credentials are sent to the OOB Authentication Service when authentication is required. This can be at any of the following times – (1) during initial customer registration, (2) during login, (3) during a transaction, or when risk mitigation methods flag a transaction.

- ***Enterprise Authentication Service –***This service is targeted at companies that need to authenticate their employees. In this scenario, the authentication credentials are stored by the service and the authentication entity, for example the VPN Server, connects to the service to authenticate the user. This is typically done during login.



How the "Out-Of-Band" (OOB) Authentication Service works

In this scenario, the authentication credentials are sent to the OOB Authentication Service when authentication is required. The customer application interfaces to the service via the PID Web Service API.

The OOB Authentication service has been used in conjunction with Risk based analytics products, such as Oracle OAAM and RSA AM, to provide step-up authentication when the risk of the transaction necessitates two factor authentication.

The following OOB methodologies are supported by the service –

True "Out-of-Band" Authentication, wherein the PIN/OTP is entered in a second channel

- ***Entering a fixed PIN in a phone –*** This scheme works in the following way – (1) the user enters their username and password into the application. (2) Their phone rings and they are prompted to enter a PIN into their phone.
- ***Entering an OTP in a phone –*** This scheme works in the following way – (1) the user enters their username into the application. (2) Their phone rings and they are prompted to enter an OTP into their phone. The OTP is typically displayed to the user in the application.

"Out-of-Band" credential passing, wherein the PIN/OTP is sent to the user via a second channel

- ***Sending an OTP to a phone via SMS –*** This scheme works in the following way – (1) the user enters their username into the application. (2) An OTP is sent to their phone as a text message. (3) The user then enters the OTP into the application.
- ***Sending an OTP to a phone via text to speech –*** This scheme works in the following way – (1) the user enters their username into the application. (2) Their phone rings and they hear an OTP spoken via text to speech. (3) The user then enters the OTP into the application.
- ***Sending an OTP via email –*** This scheme works in the following way – (1) the user enters their username into the application. (2) An OTP is sent to their email address. (3) The user then enters the OTP into the application.

How the Enterprise Authentication Service works

In this scenario, the authentication credentials are stored by the service and the authentication entity connects to the service to authenticate the user. The following authentication methodologies are supported by the service –

"Out-of-Band" Authentication methodologies:

- Entering a fixed PIN in a phone.
- Sending an OTP to a phone via SMS.
- Sending an OTP to a phone via text to speech.
- Sending an OTP via email.

For enterprise applications, the user can also enter a PIN in addition to the OTP to access the application.

Token methodologies

- ***Hard Token OTP*** **-** Key fob that displays an OTP when a button is pressed.
- ***Soft Token OTP*** **-** OTP generation software (OATH compliant) that can reside on a PC or a Black Berry or iPhone or PDA or any J2ME compliant cell phone.

The following applications can be secured by the service –

- ***VPN (IPSEC or SSL)*** **–** The interface to the service is via RADIUS. In case the enterprise has an existing RADIUS server, proxy RADIUS can be used to connect to the service. Alternatively, a RADIUS Agent, which connects to the service, can be deployed on a Microsoft RADIUS Server (IAS) located at the customer premises.
- ***Web Applications*** **–** The interface to the service is via the PID HTTP API. The login page of the web application needs to be modified to connect to the service for authentication. Alternative, a PID ISAPI filter, which connects to the service, can be deployed if the web application is running on an IIS Server. In this case, no modification to the web application is necessary.
- ***Citrix*** **–** The interface to the service is via RADIUS for the Citrix Access Gateway or PID HTTP API for older Citrix products.
- ***Single Sign On*** **–** The interface to the service is via connectors deployed on the SSO server. There are connectors for CA SiteMinder and RSA Cleartrust.
- ***Microsoft Outlook Web Access*** **–** The interface to the service is via a PID ISAPI filter that resides on the IIS Server on which OWA is running.
- ***Microsoft ISA Server*** **–** The interface to the service is via a PID ISA filter that resides on the ISA Server.
- ***Microsoft ASP.Net Applications*** **–** The interface to the service is via the PID HTTP API. The application must be using forms authentication and the login page must be modified to connect to the service.
- ***Microsoft SharePoint*** **–** Via ASP.Net Forms authentication.
- *Cloud Applications* - Such as Google Apps and Salesforce.com
- *Federated Identity* **–** Via a SAML 2.0 interface.
- *OpenID*
- Triciper's MyOneLogin

Administration:

Administration consists of provisioning and managing the system. There are several ways to accomplish this.

ProtectID Manager – This is a web based manager used by administrators. This enables role based, delegated administration of the system. The functions include provisioning users, administering users and viewing audit logs.

ProtectID Self Service Portal – This enables limited user self administration and provisioning.

Active Directory Sync – This enables the users to be provisioned in the ProtectID service via Active Directory.

Provisioning Interface – This enables an enterprise provisioning system to provision users into the ProtectID service. The provisioning protocol is HTTP based.

ProtectID's competitive advantages

Platform Approach – Unlike other products which typically offer a single or limited authentication method(s), ProtectID offers multiple authentication methods on one platform. This enables an enterprise to have choices and have different authentication methods for different user populations based on risk level, cost and deployment strategies. Because the platform is extensible, newer authentication methods and interfaces can be added making the platform viable into the future, without having to replace it or purchase additional products.

"Out-of-Band" Authentication – The ProtectID platform currently supports five different out-of-band authentication methods, making it the most comprehensive "Out-of-Band" authentication solution in the market.

Backup Authentication – ProtectID enables any authentication method to backup any other method. For example, the phone can be used as a backup to a token. Thus existing token installations can deploy ProtectID as a backup authentication scheme and save on help desk costs.

Support for Transaction Authentication – Due to its text-to-speech capability, ProtectID can deliver a summary of the transaction to be authenticated. This is useful in preventing increasing Man-In-The-Middle attacks that most solutions don't prevent.

Cloud Services Platform

The services platform has the following features –

- SAS 70 compliant.
- Fully redundant routing and switching executed with Cisco routers and Juniper firewall hardware.
- 100% Gigabit Ethernet Internet connectivity from 5 diverse carriers.
- Redundant application servers for failover protection.

Who can use the ProtectID Cloud Service

Customers that can use the ProtectID Cloud Service include –

- Financial Companies
- Health Care providers
- Enterprises
- Small to Mid Size businesses
- Government
- Cloud service providers
- Energy Utility Companies

Summary

In summary, ProtectID Cloud Service enables a company to offer two factor "Out-of-Band" authentication, using a variety of methods, to their customers and employees at effective pricing. In addition, for employees, hard and soft tokens are supported in instances where they are required.

The advantages of a "Cloud Service" is its ease of deployment and administration, with a lower Total Cost of Ownership.