STRIKEFORCE TECHNOLOGIES

ProtectID®
Out-of-Band Authentication

White Paper

★★★★★
Awarded 5-Stars by SC Magazine

StrikeForce Technologies, Inc.
1090 King Georges Post Rd.
Edison, NJ 08837
www.strikeforcetech.com
Tel: (732) 661-9641

Table of Contents

Executive Summary

Organizations of all sizes are utilizing the Internet to lower costs, boost efficiency, improve communications with customers and partners, and connect remote offices and workers together. Unfortunately, these benefits don't come without risks and corporate and customer data is vulnerable to threats which have grown exponentially in recent years. These threats have made passwords obsolete and resulted in legislation that mandates two factor authentications.

Historically, two factor authentication using hard tokens has been used for securing remote access. However, as the number of employees requiring remote access has increased, hard tokens are proving to be expensive to deploy and support enterprise wide. So, enterprises are looking to alternatives to hard tokens, such as Soft Tokens or Out-of-Band authentication using a mobile device. In addition, they are looking for a single authentication platform that is interoperable with their existing token installation and allows them to provide different authentication schemes to different classes of users and customers.

The ProtectID solution enables the enterprise to use their existing tokens but deploy lower cost authentication schemes, such as Soft Tokens and/or Out-of-Band authentication to other employees and customers. The purpose of this paper is to introduce the ProtectID solution developed by StrikeForce Technologies.

The Challenges

Today corporations face a number of challenges in securing their data –

- Complying with regulations such as FFIEC, FACTA, PCI, SOX and HIPAA.
- Providing stronger authentication to their customers in an affordable manner.
- Complementing Risk-based authentication systems with step-up Out-of-Band (OOB) Authentication.
- Migrating away from hard tokens within the enterprise to mobile tokens and/or OOB authentication.
- Transaction Authentication to prevent man-in-the middle attacks
- Securing cloud applications.
- Flexibility in deploying the solution either in-house, or with a cloud provider or a hybrid configuration wherein critical data is stored in-house and the telephony and SMS service is provided as a cloud service.

ProtectID Overview

ProtectID is a patented Out-of-Band two factor authentication platform designed to authenticate individuals and employees and/or authorize transactions in real-time. ProtectID can be integrated into many types of environments i.e. remote access (VPN), domain access, website access, risk-mitigation and transaction-based systems.

ProtectID can be installed locally on premise, or accessed through our "Cloud Service." ProtectID's advanced authentication redundancy feature minimizes password/device related help desk calls by providing users a backup authentication method. This mission critical benefit delivers Return on Investment, the very first day the system is installed.

Authentication Methods

OOB methodologies –

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.

Token methodologies –

- Hard Token (key fob that displays OTP when a button is pressed).
- Soft Token (OATH compliant software) that can reside on a PC or mobile devices such as a Black Berry, iPhone, Android or J2ME compliant cell phones.

Enterprise Applications secured by ProtectID

Remote Access

- VPN (IPSEC or SSL) – The interface to ProtectID is via RADIUS. In case the enterprise has an existing RADIUS server, proxy RADIUS can be used to connect to ProtectID. This enables us to support Cisco, Juniper and any other VPN server that has a RADIUS interface.
- Citrix – The interface to the service is via RADIUS for the Citrix Access Gateway or HTTP API for older Citrix products such as nFuse and Citrix Web Interface.

Web Applications

- Web Applications – The interface to the service is via HTTP API. The login page of the web application needs to be modified to connect to the service for authentication. Alternatively, an 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.
- 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 Applications

- Microsoft Outlook Web Access – The interface to the service is via an ISAPI filter that resides on the IIS Server on which OWA is running.
- Microsoft ISA Server – The interface to the service is via an ISA filter that resides on the ISA Server.
- Microsoft ASP.Net Applications – The interface to the service is via HTTP API. The application must be using forms authentication and the login page must be modified to connect to ProtectID.
- Microsoft SharePoint – Via ASP.Net Forms authentication.
- Windows Domain Logon - Via modified GINA.

Financial Applications secured by ProtectID

Transaction Verification

ProtectID can be used to verify a transaction such as a banking transaction or an e-commerce transaction. This capability has become critical due the surge in man-in-the-middle attacks by malware such as Zeus, Carberp and Ramnit.

This scheme works in the following way – (1) The user performs a transaction deemed risky by the fraud system (such as transferring an amount exceeding a risk threshold). (2) The financial provider sends an XML request to the ProtectID service with the transaction details. (3) The ProtectID service contacts the user at their phone number (via a SMS message or voice) and provides the details of the transaction. (4) The user authorizes the transaction. This can be via entering an authorization code sent to the user's phone into the financial application or authorizing the transaction by entering a # or PIN into the phone.

Risk Based Step-up Authentication

ProtectID can be used to provide step up authentication in conjunction with risk-based authentication systems. ProtectID is invoked when the risk score requires two-factor authentication. ProtectID has been used with Oracle OAAM and RSA Adaptive Authentication products.

Account Provisioning

ProtectID can be used to verify the identity of users prior to creating new accounts or provisioning existing users into new services.

Password Resets

ProtectID can be used to verify the identity of users prior to delivering them a new password.

Cloud Applications secured by ProtectID

Public Cloud Applications

ProtectID can be used to secure cloud applications (also called Software As a Service and Authentication As a Service). ProtectID has interfaces for the following applications.

- Google Apps
- Salesforce.com
- Triciper's (now VMware) MyOneLogin

Federated Identity

ProtectID can act as an Identity Provider to authenticate users in a Federated Identity scenario. In Federated Identity, a user is allowed to log on to partner sites as long as they are authenticated by their Identity Provider. ProtectID implements the SAML 2.0. standard.

OpenID

ProtectID can act as an OpenID Service Provider. This enables the ProtectID system to be used to provide two-factor authentication for websites that accept OpenID.

ProtectID Implementation

ProtectID Deployment

ProtectID can be deployed either on-premises, or as a cloud service or in a hybrid configuration.

On-Premise deployment – ProtectID can be deployed completely on-premises either as software installed on a Windows Server or as a pre-configured Virtual Machine.

Cloud Service – In our SAS 70 hosted environment, multiple companies can be supported on the same system with each company having a partitioned database and administration. The system is architected in a modular fashion for high reliability, scalability and availability so as to support millions of users. The cloud service can be accessed via an XML web service secured by SSL and access credentials.

Hybrid Configuration – In a hybrid configuration. critical data is stored on-premises and the telephony and SMS service is provided as a cloud service.

ProtectID 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, three tier, delegated administration of the system. The functions include provisioning users, administering users and viewing audit logs.

ProtectID Self Service Portal – This enables authenticated 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.

What makes ProtectID different from other products

Platform Approach – Unlike other products which typically offer a single authentication method, ProtectID offers multiple authentication methods. This enables an enterprise to have a choice 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.

Out-of-Band Authentication – The ProtectID platform supports six 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.

Multiple Deployment options – On-premises, cloud or hybrid configuration.

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 Man-In-The-Middle attacks.

Conclusion

The ProtectID system is the only authentication platform that can support hard tokens, soft/mobile tokens and out-of-band authentication as well as support transaction verification. As such, it can enable graceful migration from today's tokens to more cost effective and secure out-of-band authentication. Moreover, it is the only authentication platform that can be deployed on-premises, cloud or hybrid configuration.