ProtectID®
for
Financial Services

StrikeForce Technologies, Inc.
1090 King Georges Post Road #108
Edison, NJ 08837, USA
http://www.strikeforcetech.com
Tel: 732 661-9641
Fax: 732 661-9647

Introduction

The Financial Services industry is under attack by hackers. The past few years have seen innumerable data breaches, phishing attacks, keyloggers, cross-site scripting attacks, SQL injection attacks, etc. The end result is typically the same – stolen user identities.

As a result, financial regulators in the U.S. have realized that user identities have to be more secure and that the solution revolves around using two factor authentication, among other things. This has led them to pass the FFIEC recommendation and The Red Flags laws that strongly recommend using two factor authentication. Globally, financial regulators are also pushing for and implementing similar regulations. For Example, even the HIPPA regulations for the medical industry are going to incorporate The Red Flags in 2009.

Authentication solutions that were accepted and provided in the past were based on hard tokens, biometrics and smartcard/PKI. These solutions were cost prohibitive for mass deployment. As a result, many vendors started to offer risk based authentication. Risk based authentication systems assign a risk score based on parameters, such as, the IP header, time of access, geo-location, cookies, etc. If the risk score indicates that the access is coming from a PC which is not recognized, the user is challenged to answer a secret question. This is not a two factor solution because if a hacker tries to access the system, they are invariably challenged by the secret question, which is a single factor – what you know.

Some financial companies rolled out these solutions and to their dismay ran into two problems – (1) Legitimate user access would often trigger a risk score that resulted in a secret question being asked and in some cases they would misspell the answer, resulting in a call to the "Call Center" to reset their profile. This is an expensive proposition (e.g $30-$75 per call). (2) Phishers started to target the secret question, invalidating the use of a risk based authentication system.

As a result, financial companies started to look to augment the risk based authentication systems with a phone-based "out-of-band" solution. In this scenario, if the risk score justifies a step-up authentication, a one-time password is generated and sent to the user's phone as an SMS or spoken to the user or sent by an email. The user will then enter the one-time password into the financial company website to gain access to their account. This is a two factor authentication solution where the second factor, what you have, is the phone and becoming welcomed by consumers.

After realizing the cost savings and the ease of achieving compliance with an "out-of-band" two factor authentication solution for their consumers, financial companies are now seeking to replace their in-house employee hard token (keyfob) authentication systems with the "out-of-band" solution. This requires an enterprise grade solution.

Enterprises have many systems which need to be interfaced to. For example, remote access can be via IPSec VPN, SSL VPN, Citrix, Single Sign On systems , such as, CA/SiteMinder or RSA/ClearTrust or Oracle OAM and Reverse Proxies, such as, ISA Server. The solution also needs to interface to existing authentication mechanisms, such as, RADIUS, Active Directory, LDAP, etc. Also, the solution needs to be able to secure access to enterprise applications such as Siebel, PeopleSoft, SAP, Oracle Financial, etc. This is a daunting task.

The ProtectID Solution

The ProtectID® platform is an integrated authentication platform that can be used for in-house access to enterprise systems as well as offering "out-of-band" two factor authentication to the customers of the financial institution.

Currently the platform supports the following two factor authentication methodologies –

"Out-of-band" methodologies –

- *Entering a fixed PIN in a phone* – This scheme works in the following way – (1) the user enters their username and password (first factor) into the application. (2) Their phone rings and they are prompted to enter a PIN (second factor) into their phone.
- *Entering 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 a PIN (first factor) + OTP (second factor) into their phone. The OTP can be displayed to the user in the application or generated by another device or software program.
- *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 a PIN (first factor) + OTP (second factor) 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 a PIN (first factor) + OTP (second factor) 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 a PIN (first factor) + OTP (second factor) into the application.

Token methodologies –

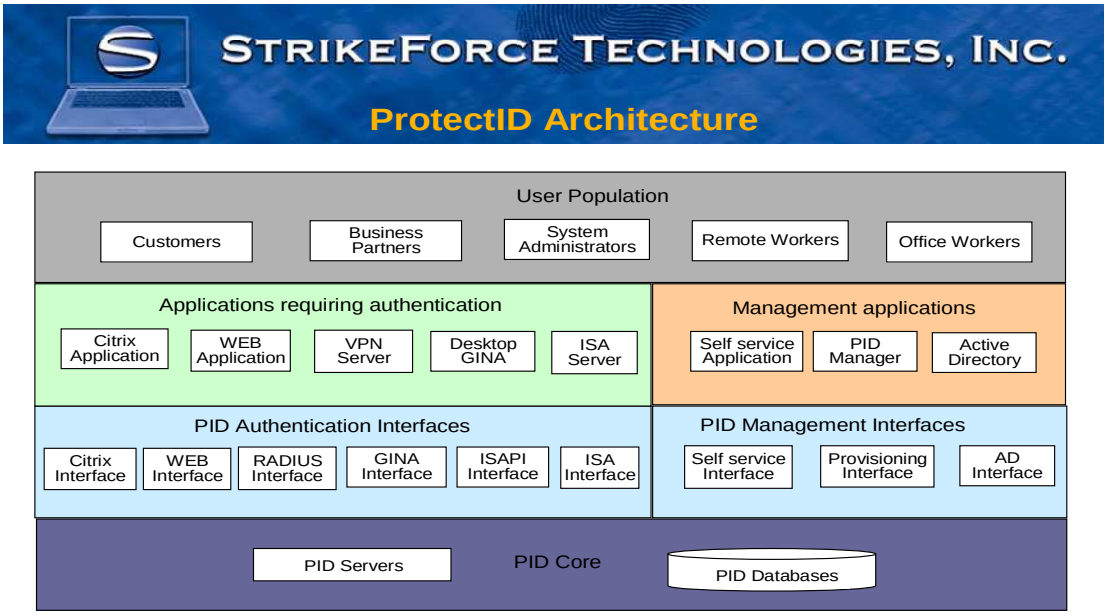
- Hard Token OTP (key fob that displays OTP when a button is pressed)
- Soft Token OTP (OATH compliant software) that can reside on a PC or a BlackBerry or PDA or J2ME compliant cell phone.

Other –

- Magnetic Stripe Card/Smart Card
- Biometrics: Fingerprint or Iris print (can be supported if required)

Architecture

The ProtectID architecture is depicted below -



The ProtectID platform consists of the following components –

Core

This consists of the Controller, the Data Access Layer and the Databases. The Controller interfaces to the other components, processes the messages from the Agents and performs the authentication operations per the profiles and policies stored in the databases. The Data Access Layer abstracts the database operations so that other databases can be used in the future. Currently, SQL Server is the supported database. Active Directory is supported via a directory sync mechanism.

Agents

Agents interface on one side to the resource that generates the user authentication request and on the other side to the Controller. There are several types of Agents. These include –

Web Agent – The Web Agent interfaces to a web application and processes HTTP messages sent by the application seeking to authenticate a user.

RADIUS Agent – The RADIUS Agent processes authentication requests sent to a RADIUS server. Currently the Microsoft RADIUS Server (IAS) is supported. Other RADIUS servers, such as Cisco's and Juniper's can be supported via RADIUS proxy. Support for RADIUS, allows ProtectID to be used in a wide variety of environments such as – VPN, 802.1x Wi-Fi, and UNIX (Linux, Solaris, AIX, HP-UX, Mac 0S-X) PAM.

Citrix Agent – The Citrix Agent interfaces to the MSAM/Secure gateway and Web Interface Citrix products and allows remote Citrix users to access enterprise applications.

Domain Agent – This enables the ProtectID system to be used to authenticate Windows domain logins. This is a custom GINA that hooks into the Microsoft GINA.

ISAPI Agent – This enables the ProtectID system to be used to secure access to MS Outlook and software such as Siebel and SAP which have web interfaces

ISA Agent – This enables the ProtectID system to be used to secure access to the Microsoft ISA server (Microsoft's application firewall).

RSA Cleartrust Agent – This enables the ProtectID system to be used to secure access to RSA's Single Sign On Software - Cleartrust.

CA Siteminder Agent – This enables the ProtectID system to be used to secure access to CA's Single Sign On Software - Siteminder.

Authentication Servers

Authentication servers are responsible for the user authentication process according to different methodologies. There are several types of Authentication servers including –

Telephony Server – The Telephony Server is responsible for phone authentication using a PIN/OTP. The server can interface to analog, digital (T1/E1) and VoIP (SIP / H.323) networks. The Server has capabilities for text-to-speech (to deliver custom messages) and a scripting language to create IVR-like call flows.

CIS Server – The CIS Server enables the use of biometrics and tokens for user authentication.

Administration

Administration consists of provisioning and managing the system. There are two elements that comprise this.

Provisioning Agent – This provides an upstream interface to a provisioning system. The provisioning protocol is HTTP based. Using this interface, a web GUI for user self-administration can be implemented.

ProtectID Manager – This enables role based, delegated administration of the system. The GUI is web based. The functions include administering users and viewing audit logs.

Product Configuration

There are two configurations – standalone and hosted. In a 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.

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 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 Man-In-The-Middle attacks.

Multiple Deployment options – ProtectID can be deployed in the following ways –

- On a single server
- On multiple servers with distributed components
- As an ASP service where the customer interfaces to the service via HTTP API
- As an "out-of-band" service wherein the customer stores the authentication data and uses ProtectID as the "out-of-band" authentication channel.