StrikeForce
Specializing In Preventing Identity Theft

ProtectID
Whitepaper

StrikeForce Technologies, Inc.
1090 King Georges Post Road #603
Edison, NJ 08837, USA
http://www.sftnj.com
Tel: 732 661-9641
Fax: 732 661-9647

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. Unfortunately, these benefits don't come without risks. Internet connected networks are vulnerable to a wide range of security threats. Organizations are under attack from both inside and outside their network parameters from a wide range of different types of security threats that often result in serious financial losses.

As businesses place massive investment in their information and computer/network infrastructure, effective arrangements are needed to identify individual users of system resources and to confirm that they are who they purport to be and that they are entitled to use the resources required. The purpose of this paper is to present information on various methods of authentication, identify their limitations and introduce the ProtectID solution developed by StrikeForce Technologies.

The Problem

The 2001 Computer Crime and Security Survey published by the FBI and Computer Security Institute shows just how pervasive security threats are for organizations:

- 85% of respondents detected computer security breaches within the last 12 months
- 64% acknowledged financial losses due to computer breaches
- 70% of respondents cited their Internet connection as a frequent point of attack. Up from 59% in 2000
- 31% of respondents cited their internal systems as a frequent point of attack

According to a recent study by Price Waterhouse, the worldwide loss of revenue due to security breaches totaled $1.4 trillion.

Clearly the existing security systems are not working. Passwords continue to be stolen and systems continue to be breached.

How passwords are obtained

There are several ways to obtain a password –

When a hacker tries to break into a network - i.e. the hacker expends effort

- *Social Engineering*: This is the oldest game in town. The most prevalent type of social engineering attack is conducted by phone. Dumpster diving, is another popular method of social engineering. A huge amount of information can be collected through company dumpsters.
- *Hacking from the outside*: In this scenario, the hacker breaks into the corporate network and obtains the password.
- *Hacking from the inside*: In this scenario, an employee of the company can introduce a scanner into their computer, capture passwords flowing over the corporate network and crack them at a later time.
- *Hacking wireless networks*: Wireless networks (Wi-Fi) are growing in popularity these days. Typically, username and passwords are sent in the clear when using public Wi-Fi networks. Where encryption is used, tools can be used probe, capture wireless packets and crack the passwords.

When an authorized user unwittingly "catches" something from the internet – i.e. the victim unknowingly helps the hacker

- *Key Stroke logging*: Key Loggers, like the name suggests, are programs that record keystrokes from the computer keyboard and either logs it to the computer or sends it to its maker through a built in e-mail engine. Key logging allows a prospective hacker to gain access to the user name, passwords, and even credit card numbers.
- *Remote Administration Tools*: RATs are remote administration programs that have been embedded into an unsuspecting victim's computer. This is the most dangerous of all hacking tools as it allows complete and total control of the infected computer.
- *Trojans*: All Trojans are hidden programs that are disguised within another program.
- *Spyware*: Spyware as the name suggests is software that is embedded on a computer and records passwords, Internet visits, cookies and can sometimes control computers services and remotely execute commands. There are many computer programs offered on the Internet for free that have hidden Trojans with spyware embedded in them.
- *Worms*: Worms are programs that propagate by themselves via e-mail or file shares. Newer variants of these also include Trojan horses and software to capture key strokes. So imagine this – all a hacker has to do is introduce a worm into the internet and the worm wiggles its way into millions of computers. Once resident in the computer, passwords can be captured and sent to the hacker.
- *Phishing*: This is perhaps the most ingenious screen wherein a user unwitting gives the hacker the username and password willingly by going to a fake site.

As can be seen, it is relatively easy for a sophisticated hacker to get hold of passwords.

Making the password scheme stronger

The thrust of security has been to make the password scheme stronger. There are two ways to make a password stronger –

Use it only once... called a one-time-password (OTP)

Make it hard to guess (Biometrics and PKI)

One-Time-Password

There are three types of OTP implementations –

- *Time based*: In this scheme, the current time (64-bit representation) is used as an input into a cryptographic hash algorithm (a 64-bit secret key is the encryption key) that spits out a 6 to 8 digit numeric token code.

- *Challenge Response based*: In this scheme, a randomly generated challenge is sent to the user. The challenge is used as an input into a cryptographic hash algorithm that generates a response.

- *Event based*: In this scheme, the response acts as a challenge for the next authentication event. The response is generated in the manner as above.

Typically hardware devices called tokens, implement the OTP scheme.

PKI

PKI stands for Public Key Infrastructure. It is based on Public Key Cryptography wherein a public key is used to encrypt a message and a private key is used to decrypt the message. The public key is typically obtained from a Certificate Authority (CA) and is part of a digital certificate which is digitally signed by the CA. In one type of a PKI user authentication scheme, the server sends a challenge to the user. The challenge is encrypted by the user's private key and is sent back to the server, as a response along with the user's digital certificate. The server validates the certificate and decrypts the response using the user's public key. If it matches the challenge, the user is authenticated. The user's PKI credentials can be stored in a smartcard or a USB Token.

Biometrics

Biometric devices use some measurable feature of an individual to authenticate their identity. The devices are built on the premise that physical human characteristics are unique and cannot be borrowed, misplaced, forged, stolen, duplicated, or forgotten. There are a number of different human characteristics that can be used in biometric recognition – Fingerprints, Hand geometry, Facial recognition, Hand written signatures, Retinal Patterns, Iris patterns and Voice patterns.

The biometric device generates a template (a parameterized representation of the biometric) which acts as a password. Since this is unique to an individual, it is hard to guess.

Strong Authentication

Typically OTP, PKI and biometric authentications are implemented in conjunction with password authentication … so called two-factor or strong authentication. The first factor is the password (what you know) and the second factor is either an OTP generated by a hardware token (what you have) or PKI credentials stored in a smartcard / USB Token (what you have) or a biometric credential (who you are). The reason two factors are needed is that in case the token or smartcard is stolen, it can't be used as is. The password must also be known.

How to defeat strong authentication

To defeat strong authentication, both the factors … password and the second factor (OTP/PKI/biometrics) have to be compromised. We have already seen that passwords can be compromised. Let us look at the vulnerability of the second factor.

OTP: The security of an OTP is based on cracking the cryptographic hash. Cracking the cryptographic hash is not trivial but is a relatively easier proposition since the input is known (for ex., the time variable or the challenge). What the hacker needs to do is to gather data (input and output) for a certain number of sessions. To do that, the hacker would have to monitor the authentication sessions (which can be done via a key logger and/or spyware). Once this data is obtained, the hacker would need to crack the cryptographic hash to obtain the secret key. This can be done offline and the hacker can also harness several machines (that have previously been compromised) to aid in the process. This task is getting easier with the advances in CPU power.

PKI: It is difficult to crack PKI encryption. So the way to defeat a PKI scheme would be to steal the PKI credentials stored on a smartcard or a USB Token. In many cases, these are protected by a PIN. For example, a user would have to enter a PIN before the software on the PC will read the smartcard. If this PIN was captured by a keystroke logger and the hacker had a Trojan that could communicate with the smartcard, it would be possible to steal the PKI credentials.

Biometrics: Typically, when a biometric template is sent to a central server for authentication, it is in encrypted form. So the way to defeat a biometric authentication scheme would be to capture the biometric template before encryption. This can be done via a suitable designed Trojan (similar to a key logger but logging the biometric device instead).

So it is difficult but not impossible to crack a strong authentication scheme.

The real problem

The real problem is that the hacker has a chance to enter the stolen credentials. Consider this …

The threat profile is growing by the day and has changed significantly in the past couple of years -

- More people around the world can afford PCs and internet connections.
- Broadband penetration is increasing rapidly.
- PC processing power is increasing.
- Hybrid viruses/worms/Trojan horses have the ability to "break into" computers automatically and steal data (aided by unwitting users).
- The focus of computer crime has changed from hacking for fun to hacking for profit and increasingly criminal gangs are operating in cyberspace.
- Hacking has been made easier with the proliferation of hacking websites and toolkits. If you enter "hacking made easy" on Google, you get millions of hits!
- With compressed software release cycles, less attention is being paid to writing secure code, resulting in vulnerabilities which can be rapidly exploited before patches are released.

Basically, it is a given that vulnerability is only increasing and no network is safe even with strong authentication.

The Solution

The only solution is to physically isolate the network and permit access only to trusted users. This way the hacker will not have a chance to enter the credentials, even if they are known to him. This may be possible for certain national security applications where it is possible to lock-up a few computers isolated from the outside world and biometrically authenticate users who physically enter the room. However, this approach is impractical for the real world which is dependant on a networked economy.

So the next best thing is to isolate the network logically.

"Out-of-Band" Authentication

"Out-of-Band" Authentication (OOBA) is a way to logically isolate a network. In OOBA, the user's authentication credentials are passed in a network that is logically isolated from the access network.

This "Out-of-Band" approach was implemented successfully by AT&T many years ago in order to stop the theft of telephone time. In those days, the signaling path (used to setup a call) and the voice path were the same. As a result, the hackers would trick the phone switch into not billing the party making the call thru the use of what was commonly called "red, blue, and black boxes" that would mimic the signaling carried by the network. However once AT&T deployed the OOB Signaling scheme (SS7), wherein the signaling path was *logically isolated* from the voice traffic, their hacking problem went away immediately.

ProtectID

Combining OOBA with Strong Authentication enables the threat profile to be reduced drastically. The ProtectID platform is an implementation of the OOB Authentication methodology providing strong authentication via a number of different authentication technologies.

Authentication Methods

The following OOB methodologies are supported –

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 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 Black Berry or iPhone or J2ME compliant cell phone.

Applications secured by ProtectID

The following applications can be 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. The RADIUS interface is implemented by extending the Microsoft RADIUS Server (IAS).
- ***Citrix –*** The interface to the service is via RADIUS for the Citrix Access Gateway or PID HTTP API for older Citrix products.

Web Applications

- ***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. Alternatively, 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.
- ***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 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 ProtectID.
- ***Microsoft SharePoint –*** Via ASP.Net Forms authentication.
- ***Windows Domain Logon*** **-** Via modified GINA.

Risk Based Authentication

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

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 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 (implemented by over 30,000+ websites).

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.

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.

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

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

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

Logically isolating the network and using strong authentication to authenticate valid users is the only way to combat the escalating threat to our networks. Because no matter how good a defense we put up, as long as the hacker has a chance to break-in, the network is not safe.