

C.O.B.A.S

Centralized Out-Of-Band Authentication System

Authentication Security for the 21st Century



Presented by:
QT Worldtel Inc.
Southeast Europe Cybersecurity Conference
Sophia, Bulgaria
September 8-9, 2003

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 C.O.B.A.S. solution.

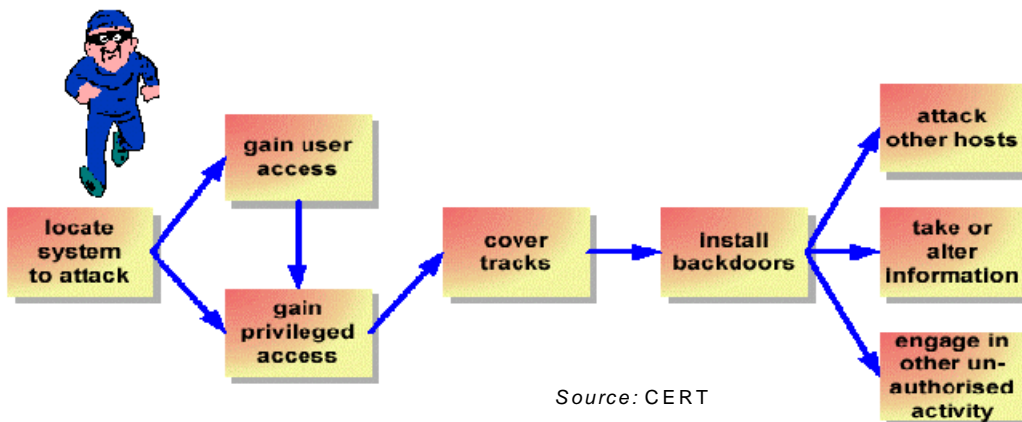
The Problem

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.



How hackers attack networks

To understand why the existing security systems are not working one must understand how a hacker attacks a network. There are three entry points to a network – (1) Dial-up access, (2) Internet access, and (3) A computer on a corporate LAN. There are several phases of an attack. This is depicted below –

Attacks coming from the dial-up network

In this case the hacker identifies the location of the company by looking in the telephone book or asking the phone operator for the phone number of the company. Then he “war dials” a range of telephone numbers around the company’s phone number and identifies those numbers that respond with a modem carrier tone – these indicate the numbers connected to a computer or a Remote Access Server. Next, the hacker tries to gain user level access. To do this he must have a User ID and password. The hacker now tries to obtain a valid User ID. To do this he may use social engineering, looking up the company web site to get e-mail addresses which show valid User IDs (ex. jdoe@ibm.com ...jdoe is possibly a valid User ID) or other techniques include outright guessing. Sometimes common UserIDs such as “admin” can be used. With a valid UserID, the hacker runs a program that tries a number of passwords automatically until the right one grants user level access. Once the hacker has user level access, they will try to gain privileged or “root access”.

Attacks coming from the Internet

In this case the hacker tries to get the range of IP addresses associated with the company. This can be done in many ways. The hacker then runs software that scans the computers associated with the IP addresses. This gives the hacker knowledge of the topology of the network and the OS and applications that the computers may be running. Next, the hacker targets the computers to attack. Easy targets are web and mail servers since they are not protected by firewalls. The other computers are typically behind a firewall. If the hacker is slightly sophisticated, he can bypass the firewall by using “stealth” techniques, spoofing the firewall or inserting a Trojan horse via the mail server. Once the firewall is bypassed, the hacker can attack the desired computers and gain user or privileged level access.

Attacks coming from within the Corporate Network

In this case, the hacker inserts sniffer software in his PC and sniffs all the traffic running over the LAN. Next, he extracts User ID and password data from the sniffed traffic and decrypts the password. This gives him user or privileged level access to desired computers.

Existing security systems

As can be seen, it is relatively easy for a sophisticated hacker to access a computer within a corporate network. The only thing that secures user level access is a password. Hence 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)

One-time-password

The basic scheme to generate an OTP is as follows – Suppose a user at computer A wants to access computer B. B sends a random number to A. A encrypts the random number using a secret key which is known to B. When B receives the encrypted random number from A, it decrypts it using the secret key and compares it with the random number it sent to A. If there is a match, access is granted. So the encrypted random number is the one-time-password. The secret key can be either symmetric (i.e. both A and B have the same key) or it could be asymmetric (i.e. A and B have different keys). Asymmetric keys are based on PKI, which uses a public key to encrypt and a private key to decrypt. The public key is typically contained in a digital certificate.

The secret key can be stored on the user's computer or in a special hardware device called a "Token". A special case of a Token is a "Smart Card" which is a credit card sized plastic card with a microprocessor chip embedded in the card. Smart Cards require a reader on the computer where access is made.

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 fixed output, which acts as a password. Since this fixed is based on an individual trait, it is hard to guess.

Fatal flaw in existing security systems

On the surface, OTPs and biometrics seem secure. But on close analysis, the reality is far different. The security of an OTP is based on a fixed secret key and an encryption algorithm. If the hacker knows the encryption algorithm, the security boils down to knowing the secret

COBAS White Paper

key. In reality, known algorithms such as DES are used. So the security is based solely on the secret key. The secret key is fixed in size based on the algorithm. For example, DES uses a key length of 56 bits. Biometric devices also generate a fixed output. For example, a certain vendor's iris recognition device generates an output of 512 bits.

So whether an OTP or a biometric is used, the security boils down to a word of a fixed length. This is just like a password. One can argue that passwords are more secure since they don't have a fixed length and unlike a secret key or a biometric, they can be changed by the user anytime they desire.

Many experts feel that coupling a Token/Smart Card (what you have) or a biometric (what you are) with a password (what you know) will give better security. This is called two-factor or strong authentication. In reality, this is like using two passwords (one of which is a secret key or a biometric ID). Instead of having to hack one password, the hacker now has to hack two passwords....that is all.

The underlying fatal flaw in all password security systems is that the access and the authentication are in the same network path. As a result, the hacker is given a chance to hack the password. So no matter how difficult the password scheme is made, in theory, the hacker can still hack the password(s) and break into any computer system.

What is needed is an entirely new way of to provide network security ... a paradigm shift: the hacker must be prevented from having a chance to hack the password altogether.

Out-of-Band Authentication

The way to correct the fatal flaw is to separate the access and authentication paths. This can be done by having the authentication done via a separate network that the hacker does not have access to. This scheme is called Out-of-Band Authentication.

For example, when you access a computer via Network 1 (the internet or a corporate data network), you are asked to authenticate yourself via a second network, Network 2. To gain access to Network 1, you have to have access to Network 2. Thus a hacker, who does not have access to Network 2, is not given a chance to break-in.

Interestingly enough, a similar approach was implemented successfully by AT&T 30 years ago in order to stop the theft of telephone time. At that time, the signaling path (used to setup a call) and the voice path were the same. As a result, the telephone hackers could 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. In fact, this was the first business venture for the two founders of the Apple Computer Corporation. Steve Jobs was selling the boxes built by Stephen Wozniak. However, once AT&T deployed a two-network approach, one for signaling, called SS7 ('Network 1'), and the second ('Network 2') for carrying the voice traffic, the signal hacking problem went away overnight.

C.O.B.A.S

C.O.B.A.S (Centralized Out-of-Band Authentication System) is an implementation of Out-of-Band Authentication technology for user authentication both for logical (computer networks) and physical access security. It has the following key features:

- Provides the highest level of security –

It provides the highest inherent security level: In the hierarchy of security authorization, passwords are the least secure (easy to hack). Next come Tokens followed by Smart Cards (which store Digital Certificates). Biometrics are considered the most secure. C.O.B.A.S., when used with a biometric, provides three-factor authorization and thus is significantly more secure than biometric systems alone. Tokens, Smart Cards and Biometrics by themselves offer single factor authentication and when coupled with a PIN they provide two-factor authentication. C.O.B.A.S. is the only product that provides three-factor authentication.

BENEFIT: Highest level of security.

- Provides an open architecture platform for user authentication – Existing authentication products provide point solutions only – for example, finger print verification only. C.O.B.A.S. enables any authentication solution to be used. Different solutions can be mixed, matched or layered. For example finger print verification can be used for domain logon and voice verification via a cell phone can be used for remote access. The architecture also enables integration of third party authentication products into the platform.

BENEFIT: Prevents product obsolescence. The customer can use any current or future authentication mechanism(s) across the enterprise without the need to replace the product in the future.

- Eliminates the need for expensive middleware – Currently biometric solutions for domain logon require special software (called middleware) to interface with the domain controller. This increases the cost to implement a biometric solution for domain logon. The C.O.B.A.S. platform can interface directly with the domain controller, there is no need for any middleware.

BENEFIT: Lower system cost to the consumer.

- Operating System Independence – C.O.B.A.S has a distributed architecture, with a central controller and remote agents. The remote agents are located on the systems that need to be secured. For example, a domain agent is located on the domain controller, a web agent is located on the web server and a VPN agent is located on the VPN server. These agents communicate with the central controller via an encrypted protocol. When a new system with a different operating system needs to be secured, all that is required is an agent for

COBAS White Paper

the new system. For example, if a SUN Solaris server needs to be secured, all that is required is an agent located on the SUN server.

BENEFIT: Easily integrates with existing or future systems.

- Biometric Layering – C.O.B.A.S enables multiple biometric systems to be layered to achieve higher accuracy. For example, a government is interested in layering iris recognition and finger print verification technologies to uniquely identify an individual.

BENEFIT: Higher accuracy in user identification.

- Mobile Authentication – Currently, there is no way to biometrically authenticate a mobile user. This is a major security issue for corporations that have an increasing number of mobile users. However, C.O.B.A.S enables the cell phone to be used as a biometric authentication device, or even a floppy disk. Consequently, a mobile user can be securely authenticated. For example, when a mobile user accesses the corporate network via a cellular data or a wireless ethernet (WiFi) connection, the user is securely authenticated by their cell phone.

BENEFIT: Enables secure authentication for mobile users using a cell phone, or floppy disk, as an authentication device.

- Secure website logon - C.O.B.A.S can be used to secure access to a website. A telephone can be used as an authentication device or alternatively, a biometric device such as an iris reader can be used for authentication.

BENEFIT: Websites can have greater security.

- Biometric VPN access – Currently, VPN and dial-up remote access is primarily secured by passwords. Some VPN vendors support enhanced security schemes such as tokens and certificates. However, these do not uniquely identify the user. VPN vendors do not currently support biometric security schemes. The C.O.B.A.S platform enables any VPN vendor to support biometric VPN access.

BENEFIT: VPN users can be authenticated by highly secure biometric mechanisms.

- Domain Authentication - C.O.B.A.S can be used for domain logon (i.e. logon to the corporate LAN). This can be done using a telephone as an authentication device or alternatively, a biometric device such as an iris reader. C.O.B.A.S interfaces to the domain controller and can also function as a proxy domain controller.

BENEFIT: Corporate LANs can be made more secure.

COBAS White Paper

- Terminal Authentication – Currently, there are millions of “dumb” terminals that have only password security. These include terminals that access legacy mainframes and mini-computers as well as “thin clients” that access Windows and SUN servers. These terminals do not have the capability to have a more secure way of user authentication. However, C.O.B.A.S can be used to provide a much higher level of security, since C.O.B.A.S enables a telephone to be used as an authentication device to authenticate the terminal session.

BENEFIT: Millions of terminals that currently have the lowest form of security can enjoy much higher security.

- “SILO” Authentication – Currently, two people with separate keys is required to launch a nuclear missile. C.O.B.A.S has implemented the same concept for authentication. When this feature is enabled, access is only granted after a two-person authentication process is completed.

BENEFIT: Enables the highest form of security possible.

C.O.B.A.S

Architecture

&

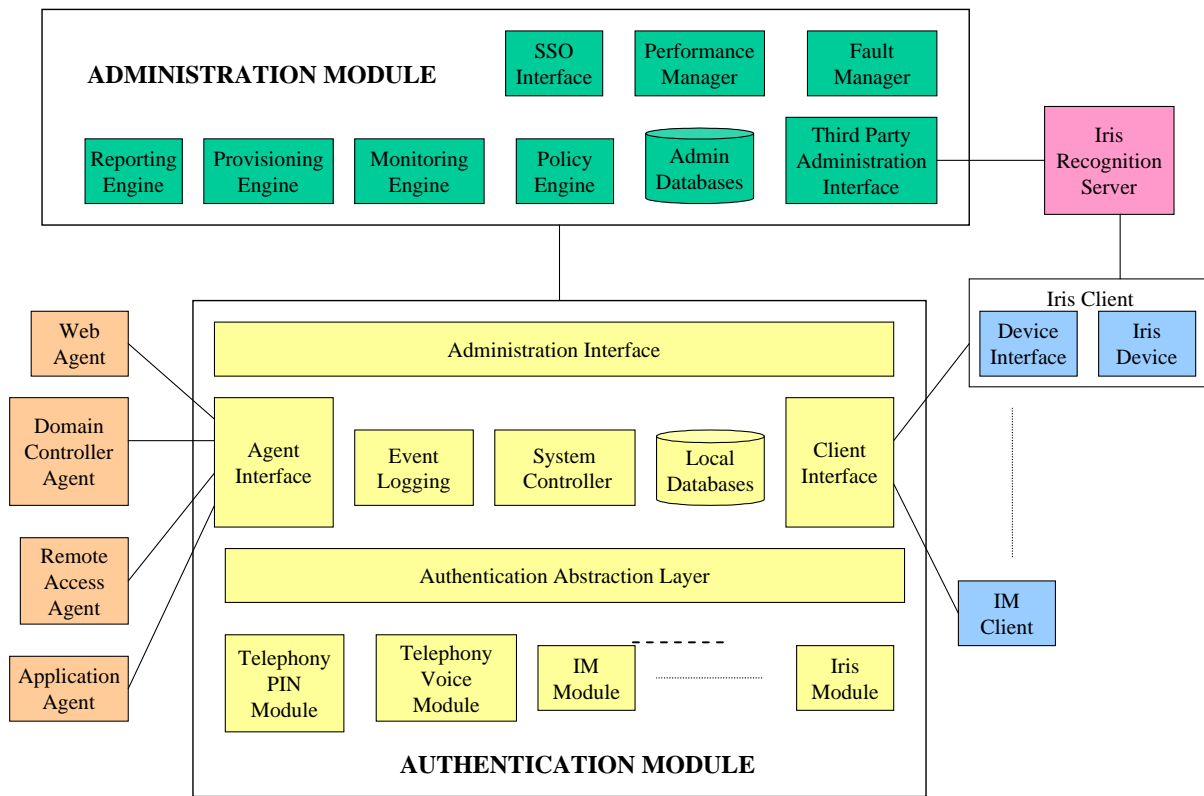
Deployment Scenarios

Architecture

The C.O.B.A.S platform consists of the following components –

- Administration Module
- Authentication Module
- Agents
- Clients

The architecture is depicted below –



Administration Module

The Administration Module provides a web-based interface to the system administrator and consists of the following –

Reporting Engine: This generates various kinds of reports. For example, for the telephony implementation of C.O.B.A.S., it generates audit logs.

Provisioning Engine: This enables an administrator to provision the Authentication Module(s) as well as the Administration Databases. The interface consists of web-based forms for inputting provisioning data or the option of loading a batch file, which contains

COBAS White Paper

provisioning data. For example, for the telephony implementation of C.O.B.A.S., the provisioning data consists of user and system configuration information.

Monitoring Engine: This enables an administrator to monitor the status of the Authentication Module(s) in real-time. For example, for the telephony implementation of C.O.B.A.S., the status of each authentication request is monitored in real-time.

Policy Engine: This consists of the business rules concerning user authentication. For example, the authentication method to use for a user, time of day when access can be granted, etc.

Administration Databases: This consists of user, policy and configuration databases that can be shared across Authentication Modules.

Third Party Administration Interface: This enables an administrator to administer the authentication products of other vendors. For example, an Iris Recognition system belonging to another vendor could be administered via this interface.

Fault Manager: This manages the alarms and critical performance thresholds across Authentication Modules.

Performance Manager: This enables an administrator to monitor the performance of the Authentication Modules. For example, for the telephony implementation of C.O.B.A.S., it generates call statistics, which can identify response time issues and help the administrator identify if additional voice cards are required.

SSO Interface: C.O.B.A.S. has an inherent Single-Sign-On (SSO) capability because it leverages the SSO capabilities of the Windows 2000 Server to run scripts to logon to Netware, UNIX, Apple Mac and Legacy systems upon authentication. However, the SSO Interface can be used to integrate with third part SSO products.

Authentication Module

The Authentication Module consists of the following components –

Administration Interface: This provides an interface to the Administration Module. Also it provides an interface for local administration.

Agent Interface: This provides an interface to the various agents that interface to the resources to be protected.

Event Logging: This enables all user and system related events to be logged. This is useful in real-time monitoring, performance analysis, audit logs and fault management.

COBAS White Paper

System Controller: This is the heart of the Authentication Module and co-ordinates the activities of all the other components.

Local Databases: These are databases used the Authentication Module in its operations.

Client Interface: This enables various authentication clients to interface to the Authentication Module. These clients are located on the user's PC.

Authentication Abstraction Layer: This enables the Authentication Module to abstract the function of authentication so that it can work with many different authentication methods.

Authentication Modules: These enable specific authentication methods to be used. For example - Telephony PIN authentication, Telephony Voice authentication, Authentication using the Instant Messaging network, Iris authentication etc.

Agents

An agent is located at the point where authenticated access is desired. Agents provide an authentication service to the application they communicate with. When a user attempts to access the application it sends an authentication request to the Authentication Module via the Agent. After the Authentication Module performs the Out-of-Band authentication, it sends the results to the Agent, which communicates the outcome to the application. Agents communicate with the Authentication Module via an encrypted XML-like interface. The various Agents include –

Web Agent: This is located on a web server, which has a web application that requires secure access. An example of a web application is an online banking application.

Domain Controller Agent: This is located on a Windows 2000 Server and controls domain (i.e. internal network) logon.

Remote Access Agent: This is located on a RADIUS server and can be used by either a RAS or VPN server for user authentication.

Application Agent: This is associated with specific applications that requires secure access. For example, if secure access to Oracle is desired, the Oracle login process communicates with the Authentication Module via an Application Agent.

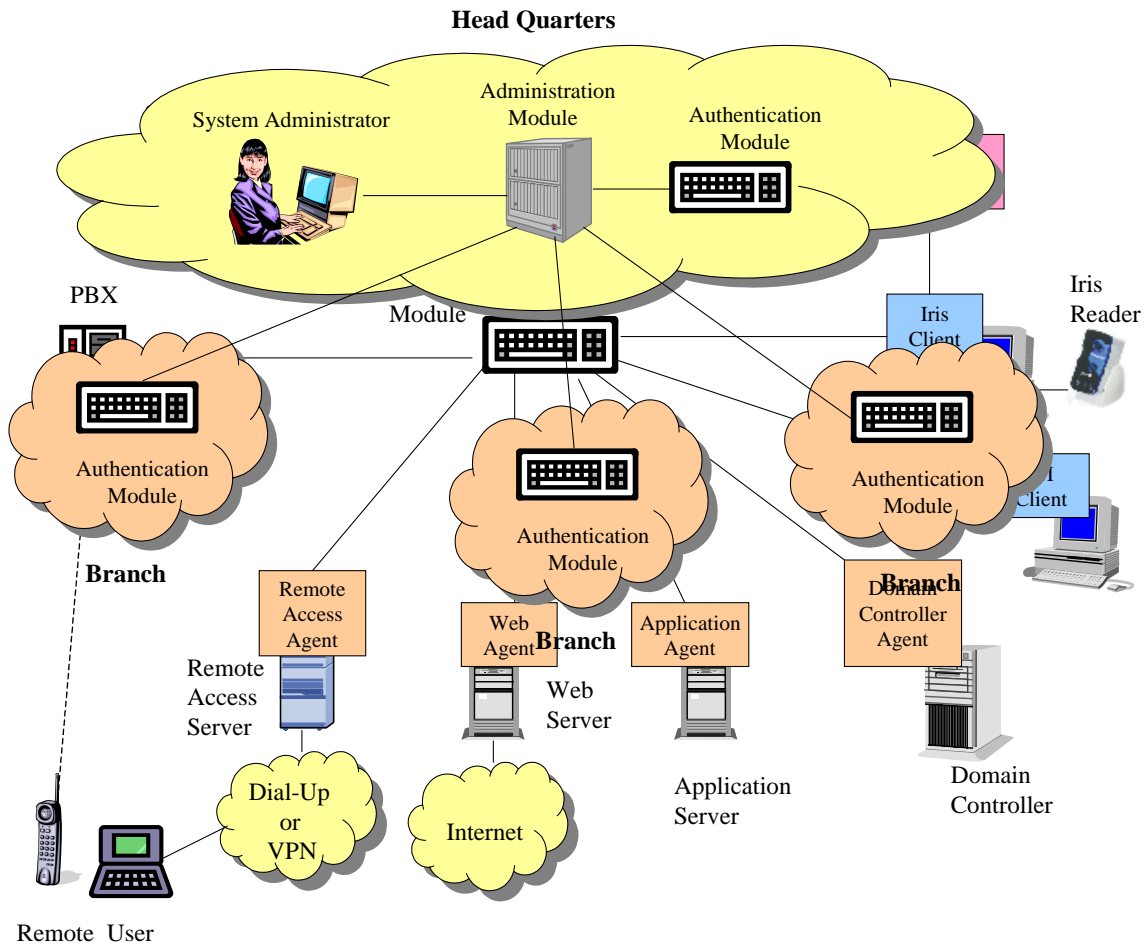
Clients

Clients are resident on a user's PC and communicate with the Authentication Module via an encrypted XML-like interface. There are no Clients for Telephony authentication (PIN or Voice), since the telephone acts as the authentication client. For authentication using an Instant Messaging network an IM Client is required.

To enable other vendor's products to be integrated into the C.O.B.A.S. framework, a device interface provides the point of interface to that vendor's product. For example, to use Iris authentication, the Iris Client consists of two parts – a vendor specific part and the device interface, which interacts with the Authentication Module.

Deployment Scenarios

Enterprise Deployment



Managed Service Provider

