

# **ADVANCE AUTHENTICATION TECHNIQUES**

## **Introduction**

1. Computer systems and the information they store and process are valuable resources which need to be protected. With the current trend toward networking, compromise of one computer on a network can often affect a significant number of other machines connected to the network.

2. The first step toward securing a computer system is the ability to verify the identity of users. The process of verifying a user's identity is typically referred to as user authentication. Passwords are the method used most often for authenticating computer users, but this approach has often proven inadequate in preventing unauthorized access to computer resources when used as the sole means of authentication. We will now discuss advanced authentication technology which can be used to increase the security of computer systems and provides guidance in the selection and use of this technology.

## **What is authentication?**

3. Authentication is the process of determining if a user or identity is who they claim to be. Authentication is accomplished using something the user knows (e.g. password), something the user has (e.g. security token) or something of the user (e.g. biometric).

4. The authentication process is based on a measure of risk. High risk systems, applications and information require different forms of authentication that more accurately confirm the user's digital identity as being who they claim to be than would a low risk application, where the confirmation of the digital identity is not as important from a risk perspective. This is commonly referred to as "stronger authentication".

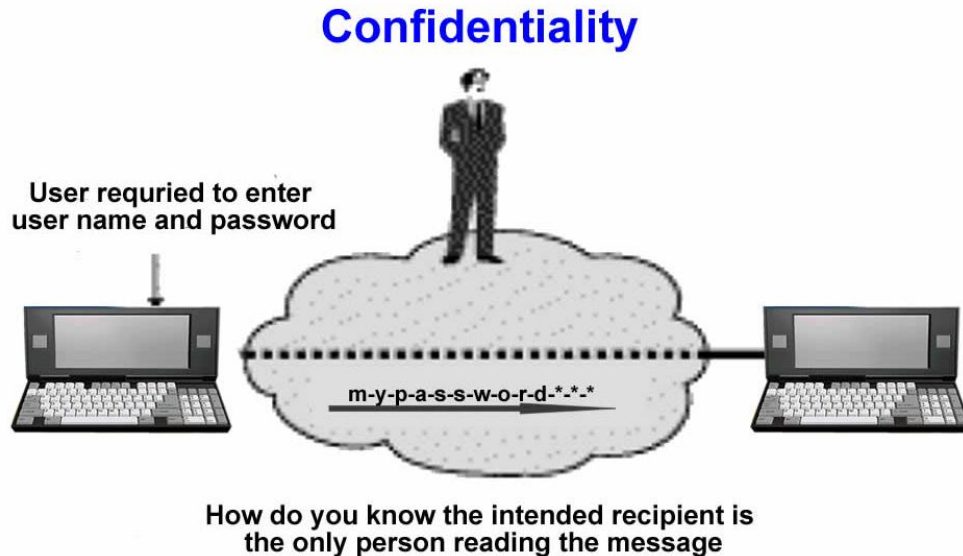
5. Authentication technology provides the basis for access control in computer systems. If the identity of a user can be correctly verified, legitimate users can be granted access to system resources. Conversely, those attempting to gain access without proper authorization can be denied. As used in this bulletin, authentication is defined as the act of verifying the identity of a user. Once a user's identity is verified, access control techniques may be used to mediate the user's access to data. Authentication processes are dependant upon identity verification and registration processes.

## **Why Authentication is required?**

6. Networks, both internet and intranet, provides amazing opportunities, but not without some risk. Without the proper controls, your data is subject to several types of attacks. These problem areas are discussed in the sections that follow.

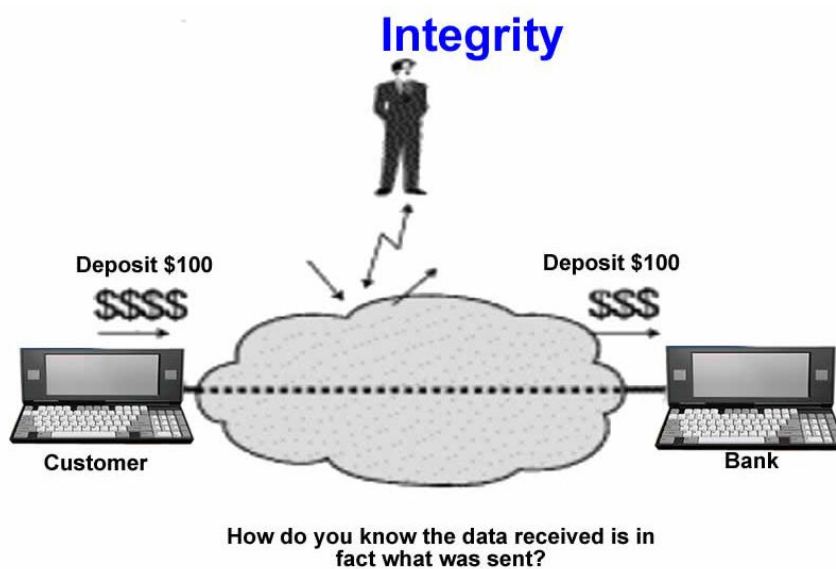
## Loss of Privacy

7. A perpetrator may observe confidential data as it traverses the Internet. This ability is probably the largest inhibitor of business-to-business communications today. Without encryption, every message sent may be read by an unauthorized party.



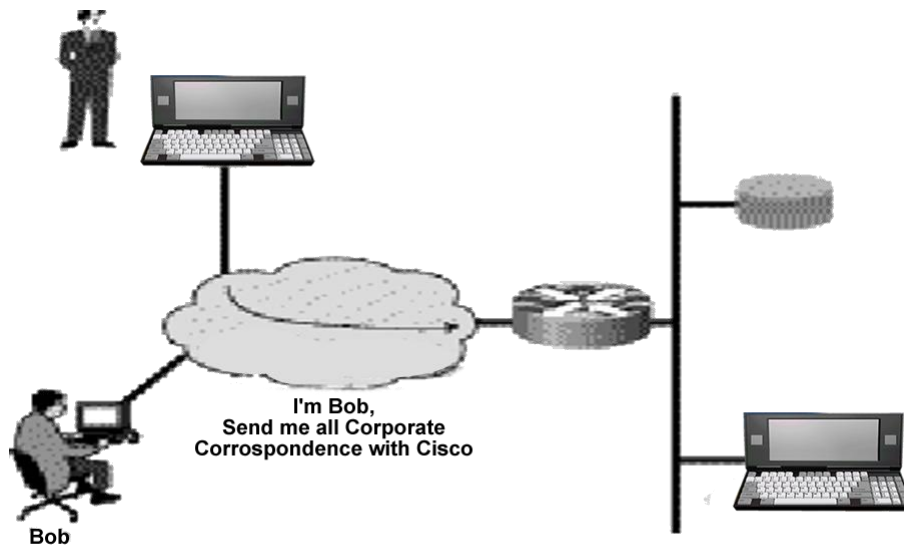
## Loss of Data Integrity:-

8. Even for data that is not confidential, one must still take measures to ensure data integrity. For example, you may not care if anyone sees your routine business transaction, but you would certainly care if the transaction were modified. For example, if you were able to securely identify yourself to your bank using digital certificates, you would still want to ensure that the transaction itself is not modified in some way, such as changing the amount of the deposit.



## **Identity Spoofing:**

9. Moving beyond the protection of data itself, you must also be careful to protect your identity on the Internet. A crafty intruder may be able to impersonate you and have access to confidential information. Many security systems today rely on IP addresses to uniquely identify users. Unfortunately this system is quite easy to fool and has led to numerous break-ins.



**How do you know the request is from Bob only?**

## **Authentication**

10. Authentication technology provides the basis for access control in computer systems. If the identity of a user can be correctly verified, legitimate users can be granted access to system resources. Conversely, those attempting to gain access without proper authorization can be denied. As used in this bulletin, authentication is defined as the act of verifying the identity of a user. Once a user's identity is verified, access control techniques may be used to mediate the user's access to data. A variety of methods are available for performing user authentication.

11. The traditional method for authenticating users has been to provide them with a secret password, which they must use when requesting access to a particular system. Password systems can be effective if managed properly (Federal Information Processing Standard [FIPS] 112), but they seldom are. Authentication which relies solely on passwords has often failed to provide adequate protection for computer systems for a number of reasons. If users are allowed to make up their own passwords, they tend to choose ones that are easy to remember and therefore easy to guess. If passwords are generated from a random combination of characters, users often write them down because they are difficult to remember.

12. Where password-only authentication is not adequate for an application, a number of alternative methods can be used alone or in combination to increase the security of the authentication process. The three generally accepted methods for verifying the identity of a user are based on something the user knows, such as a password;

something the user possesses, such as an authentication token; and some physical characteristic of the user, such as a fingerprint or voice pattern. A variety of methods are available for performing authentication.

- (a) Password Authentication
- (b) Lightweight Directory Access Protocol (LDAP) Authentication
- (c) Biometric Authentication
- (d) PKI Authentication
- (e) Security Token Authentication
- (f) Smart Card Authentication
- (g) Wireless Authentication

### **Password Authentication**

14. In most enterprises, the use of passwords is the primary means of authenticating a user. Unfortunately, it is also the weakest form of authentication. In today's digital world, the ways to bypass this form of security are trivial. While many enterprises focus on strengthening passwords, these efforts are by and large meaningless in the face of the tools that attackers can use. The tools provide criminals with easy ability to hack, trap, or crack most passwords easily.

15. The first attack tool against password authentication is a hardware keyboard logger. Legally available online for \$40, these devices plug into the connection between the keyboard and the computer. They record every keystroke, with some models able to do time and date stamps against the data. A hardware keyboard logger looks like a small hardware piece of computer connections, takes only 10 seconds to install and is not detectable by any means of commercially available software.

16. The use of password authentication is further weakened by software attacks. This year alone, it is estimated that there will be several thousand different malware password logging attack programs will be created. Some of these are very sophisticated and can be ordered by the internet to attack certain types of firewalls. These password authentication logging software programs are embedded in email that are activated by clicking on the links in the email or by visiting a fake site that looks like the normal commercial site (phishing attack).

17. Some of the password authentication attacks are so sophisticated that they embed themselves on the core root operating systems kernel (rootkit attacks). Rootkit attacks are now acknowledged by Microsoft to be so insidious that the only way to remove them is to re-image every computer on the infected enterprise network!

18. Does this mean that passwords shouldn't be used in your enterprise?

19. No. The use of passwords can be used in a layered identity defense strategy. What this means is that your enterprise will allow the use of user id and password to gain general access to low risk enterprise applications and information e.g. the enterprise portal. However, when the user tries to access applications or information that is higher risk, the enterprise single sign on system will require stronger

authentication. This may include the use of security tokens, digital certificates, biometrics, smartcards or combinations thereof in addition to the password.

### **LDAP Authentication**

20. Lightweight Directory Access Protocol (LDAP) directories and LDAP authentication have become one of the enterprise user infrastructure cornerstones. As the enterprise has digitized and opened itself up to customer, business partner, vendor and wide-spread employee access to pieces of most enterprise applications, the need to know who the user is has significantly increased from a security perspective. Who is the user trying to access an application? What is the strength of authentication by which the application can trust the user trying to access the application? What are the user's authorization privileges?

21. The frequency with which to authenticate who a user is has also increased. Thus in medium to large enterprise it is not uncommon to have several thousand to several hundred of thousand identity look-ups per second.

22. The above are the reasons why LDAP directories and authentication have taken on such a dominant role in enterprise authentication. LDAP directories offer the following features:

- (a) They are very quick for doing identity reads against as compared to traditional databases.
- (b) They are low cost - in fact some LDAP directories are available for free
- (c) Virtual LDAP directories enable quick linkage between multiple databases and multiple LDAP directories.
- (d) LDAP directories are excellent for doing rapid LDAP authentication against for any digitized authentication.
- (e) LDAP directories have a universal protocol enabling quick interaction and exchange of identity information between enterprises.
- (f) LDAP directories can be easily partitioned to place the directory close to the end user, thus improving performance and reducing network load.

### **Underlying Key Points in LDAP Authentication**

#### **Authoritative Identity Sources**

23. In most medium to large enterprises, the authoritative source for employee information is usually the Human Resource Management System (HRMS). Figuring out what system is authoritative for customers, contractors, temps, business partners and vendors is usually much more complicated. It is very important before LDAP authentication is implemented the enterprise first determines which system or application will be authoritative for the identity data. This also means cleaning up the associated business processes dealing with identity creation, role changes and terminations. Often the authoritative identity source will have many identities in their data stores listed as active who are no longer active. This can create security holes in any LDAP authentication.

## **Unique Enterprise ID**

24. Next it's important that in cases where multiple data sources have the same identity information that a universal identity id be deployed. For example, if a user named John Jones is in the HRMS as J Jones, in the payroll system as John Jones, in the shipping system as JJONES etc, then it becomes important to know at the enterprise level a common id for John Jones. This usually means creation of a unique alphanumeric id for each user. Without this, the enterprise LDAP authentication won't work since John Jones won't know which id to use in authentication. Further, the handoff to the applications after LDAP authentication won't work since the LDAP directory has to communicate with the application that John Jones has successfully authenticated.

## **Linkage of Authoritative Sources with the LDAP Directory**

25. LDAP authentication relies upon the LDAP directory having the most up to date identity information with which to do an authentication against. This requires that the authoritative source be linked, at a minimum, on a nightly batch basis, and in many cases, on a identity event basis. In the old days, of a few years ago, interfacing LDAP directories with authoritative source data bases was expensive and time consuming to do. The synchronization of the LDAP directories with the databases was critical and costly. Today however, LDAP virtual directories are now mainstream tools. A LDAP virtual directory is one which sits in a virtual environment and has its sources of identity information derived from pointers to specific tables in data stores or, in other LDAP directories. LDAP virtual directories can usually be created in several hours or a few days and put into operation very quickly.

## **LDAP Authentication in Practice**

26. LDAP authentication is now very common in network operating systems. Microsoft uses this in Win2003 with its Active Directory. All network operating systems today support the integration of LDAP Authentication including Solaris, Novell, AIX, Linux and HP-UX. In each of these cases, the user usually enters in their id and password. The information may be presented as an online form or simply have an entry point for the id and password. This information is then sent to the LDAP directory (make sure the information is sent encrypted and not in open text). The directory takes this information and compares it to the id and password stored in the LDAP directory. If it is the same, the LDAP authentication is successful. In network operating systems, the network then takes over and proceeds with user authorization and allows them to use the network.

## **LDAP Authentication and Single Sign On**

27. Single Sign On (SSO) systems mostly use LDAP authentication. The enterprise user logs on in the morning and sees normally a form based enterprise login screen. The user enters in their id and password. The SSO software then takes the information and sends it to the security server using an encrypted connection. The security server in turn then logs on to the LDAP server on behalf of the user by providing the LDAP server with the user's id and password. If successful, the security server then proceeds with

any authorization and/or lets the user proceed to the application or resource they require.

### **Authentication - Biometrics**

28. Biometrics used for authentication is currently in fashion in the authentication industry. The UK and US governments are rapidly deploying them in their visas, passports and personal identification cards. Many other industries are adopting biometrics as authentication mechanisms for accessing bank machines, doorway access control and time card reporting and general computer desktop access. Authentication is the process of determining if a user or identity is who they claim to be. The authentication process is based on risk. Higher risk situations require more identity verification certainty. Biometrics can play a useful role in verifying the identity along with other factors.

### **What is biometric authentication?**

29. Biometric authentication is the process of verifying if a user or identity is who they claim to be using digitized biological pieces of the user. This can include finger scans, finger prints, iris scans, face scans, voice recognition and signature scans. Other biometrics in research for authentication includes vein scans and DNA.

### **Are all biometrics equal?**

30. No. The type of biometric used and the way it is used results in different authentication results. The table below lists current estimates for common biometric authentication systems:

	Finger	Voice	Iris	Face
Type	Physical	Behavioral	Physical	Physical
Method	Active	Active	Active	Passive
Equal Error Rate	2-3.3%	<1%	4.1-4.6%	4.1%
Failure to Enroll	4%	2%	7%	1%
Nominal False Accept Rate	2.5%	<1%	6%	4%
Nominal False Reject Rate	0.1%	<1%	0.001%	10%
Liveness Aware	No	Yes	Bo	Possible
System Cost	High	Low	Very High	High

### **Why Biometrics Will Not Solve Identity Theft**

31. Biometrics is very useful, in certain situations, as an authentication device. It is useful when someone is watching the user use a biometric authentication device. This way the enterprise can be relatively certain that there is no malfeasance being done

between the user, the biometric hardware reader and the enterprise security system. However, when biometrics are done remotely, with the enterprise not able to see and control the authentication hardware, the chances increase that the identity presenting their biometric may not be the person who is registered with the biometric. Therefore, the use of multi-factor authentication mechanisms is used.

32. The use of biometrics as a deterrent against identity theft is being much touted at the moment. However, the use of biometrics alone will not likely deter criminals from finding ways around the use of biometrics. Remember that what is being presented are a set of computer bits that represent the biometric to the authentication server. Therefore, it is extremely likely that criminals will adjust their attack vectors and try to capture the biometric from the person, and then replay these on the enterprise.

### **Authentication - PKI (Public Key Infrastructure)**

33. A public key infrastructure is a system that provides for trusted third party user identity inspection and assurance. Normally, this is done by a Certificate Authority (CA) and uses cryptography involving public and private keys. A typical PKI system consists of:

- (a) Client software
- (b) A Certificate Authority server
- (c) May involve smartcards
- (d) Operational procedures

### **How PKI infrastructure works:**

34. The Certificate Authority checks the user. Different CA's have different identity validation procedures. Some may grant the user a digital certificate with only a name and email address, while others may involve personal interviews, background checks etc. The user is granted a digital certificate. Often there are two components to these private and public keys.

35. The user wishes to send an email to a business associate. The user digitally signs the email with their private key. The email is sent to the business associate. The business associate uses the sending user's public key to decrypt the message. The use of digital certificates in this example provides confidentiality, message integrity and user authentication without having to exchange secrets in advance.

36. PKI was oversold on its capabilities when it was originally introduced several years ago. There were serious problems with browser incompatibilities, costs associated with issuing and managing digital certificates and a business environment that had not yet widely adopted the internet to rethink business processes between enterprises.

### **Authentication - Security Tokens**

37. Authentication is achieved by asking something you know, something you have or, providing something you are or combinations thereof. Something you have, like a physical token, is used often in real life e.g. a driver's license. In the digital world

security tokens are now commonly used. They are often one time password security tokens and/or smart cards.

### **One Time Passwords**

38. One time password security tokens, like secureID by RSA, are one way of significantly reducing the risk of using passwords. Unlike passwords which are changed every 60-90 days or longer, a secureID token works differently. On the small screen of the key fob the user carries with them are numbers that change every 60 seconds. The numbers displayed on the screen change randomly to the end user. They are generated by a mathematical algorithm that is only known to the enterprise security server.

39. The user logs on to the enterprise network. During the logon sequence the user is requested to enter in their id and then the number displayed on the screen. This information is sent via encryption to the enterprise security server. If the number on the screen matches the mathematical algorithm and the id, then the user is authenticated.

40. The devices are tamper proof/resistant. They are pre-programmed from the factory and ready for immediate use. By combining a secret that the user knows (their id) with the one-time password, the authentication is much stronger than that from a traditional password.

### **Authentication Weaknesses with Security Tokens**

41. There are weaknesses with using only this approach. For instance, if someone is able to steal or fraudulently obtain the key fob and, they also know the user's id, then they will be able to successfully masquerade as the identity. Additionally, there are significant management costs with the key fobs or credit card size tokens. Recent announcements in February 2007 by Entrust selling one-time password tokens at \$5 means that the price points are now much lower and more affordable. Users need to be issued them physically, they need to be replaced when lost (which is common) and recovered or terminated when an identity leaves the enterprise. Poor de-provisioning processes may result in security holes being created by the identity still having access to the network using their secureID token and id.

### **Access Control Cards - Contact less Smart Card**

42. The contact less smart card has a microchip embedded in the card with internal memory. This enables the card to:

- (a) Securely manage, store and offer data access to the card
- (b) Perform complex functions and calculations (e.g. encryption)
- (c) Interact with an RF device in an intelligent manner

### **Common applications of contact less smart cards include:**

**Mutual authentication:**

43. The contactless smart card can verify that the card reader is authentic and then verify itself to the card reader before starting a secure transaction

**Strong information security:**

44. The ability of the microchip and memory enable the card to encrypt any identity information contained in the card as well as encrypting the RF connection between the contact less smart card and the card reader.

**Tamper resistant security:**

45. There are a number of hardware and software capabilities that is built into contact less smart cards to detect and react to tamper methods and help counter attacks on the card.

**Authentication and Authorization Information Access Control:**

46. The contact less smart card can protect the information contained within the card by authenticating the information requestor and then allowing only the release of information the requestor is authorized for. The card owner may have additional methods such as a PIN number or a biometric to approve release of the information. This is an example of strong authentication.

47. Selection of the access control cards should be done in context of the enterprise access control and identity management systems. For example, will the cards and readers integrate with the enterprise Lightweight Directory Access Protocol (LDAP)? Can the access control provisioning system create, modify or terminate an identity on the access control card identity server? What is the strength of authentication required for the access control card? Is it easy to tamper with?

**Authentication - Wireless**

48. Most modern wireless networks do user authentication using Remote Authentication Dial-In User Service (RADIUS) protocol. RADIUS handles the overall authentication process of the user's session on the wireless device as well as also handling the authorization and auditing.

49. Typically, when you logon to your ISP using a wireless device, you are required to provide authentication information. Often, this uses Extensible Authentication Protocol (EAP). The type of authentication you use is determined by the EAP authentication method. There are many different EAP methods. This can range from the use of an id and password (very insecure), to digital certificates, security tokens and even biometrics.

50. The RADIUS system takes the EAP Authentication Method, challenges the user with the appropriate authentication method, receives the authentication response and then verifies it, often against an enterprise LDAP directory. If the authentication is successful, the RADIUS server will then authorize IP addresses, the tunnelling protocol used to create virtual private networks, etc. Further, the RADIUS server keeps tracks of when a user session begins and ends.

## **Wireless Authentication Challenges**

51. Many wireless deployments continue to use the least secure authentication methods - id and password. The use of this results in very insecure communications between the enterprise and the wireless device. If you are forced to use this, then my advice is to lock down what the user can access and severely restrict the information the user can obtain. Use a network security appliance like Caymas to check the wireless device platform and ensure it is up to date re software updates and then restrict access to network and applications.

52. For senior executives, who do require fairly open access to the applications and information systems via their wireless device, issue them with something like a secureID from RSA one time password generator and have the executives be required to enter this in order to authenticate their wireless device to the network. This reduces the risk that the user on the end of the wireless device is not the identity you issued the id and password to.

## **Conclusion**

53. As the enterprise risk rises for networks, applications and information access, so too must the layers of authentication strength. The financial system, payroll and payables are all higher risk. So too are users who hold super-user privileges like senior network administrators. For all of the medium and higher risk applications, your enterprise should be using a graded series of stronger authentication. For instance, low to medium risk might be addressed by the user providing their id, password and a digital certificate. Medium risk should be addressed by the user providing things like a secureID token along with their id and a password. Medium to high risk should be addressed by the user providing something like a smart card, a secure id token, a biometric and a second unique password.

54. Password-based authentication is the most widely used method for verifying the identity of persons requesting access to computer resources. However, authentication based only on passwords often does not provide adequate protection. The use of authentication tokens, biometrics, and other alternative methods for verifying the identity of system users can substantially increase the security of an authentication system. The proliferation of networked computer systems and the corresponding increase in the potential for security violations makes it even more critical those who design and operate computer systems to understand and implement effective authentication schemes. There are many ways of authenticating a user. These range from the id and password (commonly referred to as "basic authentication"), digital certificates, security tokens, smart cards and biometrics. There are different reasons to use each type of authentication.