White Paper

IP Network Authentication

A Comparison of Competing Technologies

Username/password

Dynamic Tokens

PKI Digital Certificates

Biometrics

Edited by Kenton G. Dallas

Intelispan, Inc.

www.intelispan.com

Introduction

Data communications networks of all varieties, Local Area Networks (LANs), Wide Area Networks (WANs), Virtual Private Networks (VPNs), Intranets, Extranets and the Internet; are playing an increasingly strategic role in the way business is conducted in the world today. Security is a key factor in determining the usefulness or appropriateness of various network architectures.

Security is a broad and varied topic that is appropriately discussed in relative terms. Since there is no such thing as absolute security, discussions on this topic typically focus on the vulnerability of a system to specific types of security attacks that might occur. This information in combination with knowledge of the value, or cost of exposure of the data or resources in question are necessary to make an informed decision as to the appropriate level of security required. In the end the issue of security is essentially a financial one. It seldom makes sense to spend more to secure a resource than the cost which would result should the resource in question be stolen or compromised.

This paper will provide a comparative analysis of the strengths and weaknesses of various methods of authenticating user access on an Internet Protocol (IP) network.

Security Concepts

One useful context for the evaluation of alternative technologies is to characterize the types of security breaches that might possibly occur during a data communications session.

- a third party intercepts a message and reads it's contents (Confidentiality)
- a third party changes the contents of a message (Integrity)
- the contents of a message are inadvertently changed (Integrity)
- a third party gains access to a resource or becomes a party to a transaction by misrepresenting their identity (Authentication)
- a party to a transaction denies having authorized the transaction (Non-Repudiation)

In order to guard against these and other potential breaches of security, the following security attributes have evolved over time:

Authentication - proof of the identity of the party or parties to a network transaction

Integrity - proof that message contents have not been altered during transit, intentionally or unintentionally

Confidentiality - certainty that the contents of a message have not been disclosed to third parties

Non-Repudiation - proof of an entity's participation in a transaction, so that the transaction cannot later be denied.

Authentication

Authentication is the network security service that is familiar to most of us, typically due to the critical role it plays in access control. In a discussion of various authentication methods, it is useful to

characterize them in terms of how an entity (a person or a device) can prove its identity across a network. Generally, only three methods are used, either individually or in combination, for an entity to identify itself.

Something You Know - The most common form of authentication, and it typically takes the form of a password or Personal Identification Number (PIN). It is better than no authentication at all, but is the weakest method of authentication examined here.

Something You Have - Physical analogies range from such common methods as passports, driver's licenses, or credit cards. The problem these methods present in a network environment is that they cannot be transmitted over a communications network. What is needed is a digital equivalent of these methods that can be implemented over a network.

The digital equivalents in the market today are commonly referred to as digital "tokens". This paper will focus on comparing the relative merits of alternative digital tokens such as symmetric keys, asymmetric keys, smart cards and dynamic tokens. The value of these methods of authentication can be virtually useless or very strong depending upon the technologies employed and the design of the overall security solution.

Something You Are - The most common manifestation of this in the network world is biometrics, such as iris scan or fingerprint verification. Clearly the strongest form of authentication when properly implemented, but the technologies introduce considerable cost and operational obstacles which make it impractical for most applications today. However, where the costs of implementing such a system are justified, biometrics technology provides a high degree of authentication certainty.

Integrity

Many generally accepted technologies exist and are in use today to ensure that a message or transaction has not been intentionally or unintentionally altered. Key based cryptographic systems provide integrity through the use of a Hash Algorithm (e.g. MD2, MD4, SHA-1) which is used to create a checksum (a checksum is a unique mathematical value generated by processing digital data through specific algorithm process) of a message called a message digest. The message digest, generated by the message originator, is sent along with the original message. The recipient of the message re-creates the message digest using the received message and compares it to the message digest received. If the two message digests match, the recipient can be confident that the message has not been altered during transmission.

Confidentiality

Confidentiality is assured through the use of secret codes to encrypt the message. In order to decode the message, the recipient, and no one else, must have the appropriate key. Only an individual in possession of the secret key can decrypt the message to determine its actual content. A variety of cryptographic algorithms are in use today with varying performance and operational characteristics. Cryptographic algorithms are divided into two main categories: symmetric or asymmetric

Symmetric algorithm - Is a cryptographic algorithm where a single key is used both for encryption and decryption of a message.

Asymmetric algorithm - Is a cryptographic algorithm where a unique key pair is required to ensure the confidentiality of a message. A message encrypted using one key from the pair, can only be decrypted using the alternate key from the pair. Even the original key used to encrypt the message cannot decrypt the message.

Of course, the problem that must be overcome in the use of cryptographic confidentiality systems is the secure distribution of the appropriate key to the recipient.

Since the two classes of algorithms have distinct performance and operational characteristics, each must be considered carefully when designing a cryptographic system. Symmetric key algorithms offer a significant performance advantage over asymmetric key algorithms, in terms of processing requirements. However, symmetric key based systems have practically insurmountable key distribution problems. Asymmetric key algorithms have the considerable advantage of overcoming the key distribution problems inherent with symmetric key based systems through the use of public key/private key pairs. One such solution has become the de facto standard within the communications industry, and is referred to generically as Public Key Infrastructure (PKI). The methods employed in PKI to overcome the key distribution problem are discussed later in this document.

Non-Repudiation

Non-repudiation is a quality possessed by messages or transactions which have been digitally signed with the secret key of an asymmetric key pair, provided that the secret key is in the possession of one and only one individual. It is this quality that makes public key based systems so well suited for, and fundamental to, the growth of electronic commerce applications.

What non-repudiation provides is a means where two entities can enter into a contractual agreement over a network and feel confident of the identity of the other party. This is all predicated upon the existence of a trusted third party that can guarantee the identities of the parties to a transaction and the association of these entities with their public keys. This is the role that is filled by the Registration Authority (RA) in association with the Certification Authority (CA), in the context of PKI.

The IP Network Environment

With the foundation of the security concepts described above, a discussion of the implementation of such concepts in an IP network authentication scheme follows. The discussion will be limited to technologies currently in use by IP networks as well as technologies that are likely to be implemented in the near future.

Authentication

Most IP networks, such as ISPs, currently employ a username/password (something you know) approach for authenticating users wishing to gain access to its IP services. Due to its low cost of implementation and administration, this technique has been the prevailing form of access control for networks and applications of all kinds. Although this method is adequate for most basic applications, many applications share an increasing demand for stronger authentication schemes.

Network authentication schemes that only require username/password (something you know) are generally referred to as “weak” authentication systems. Schemes that require both a username/password (something you know) combined with a digital token (something you have) are referred to as “strong” authentication systems.

Due to the higher costs of strong authentication systems, an optimal strong authentication system will be one that minimizes the costs of implementing and administering the system, including the burden placed on the end user.

Of the strong authentication technologies, biometrics provides the strongest authentication solution available today. However, due to the requirements for physical equipment necessary to capture biometric data, it presents deployment and administration costs which, for the foreseeable future, make it an impractical alternative for widespread use.

Dynamic token based systems command the market leadership position in the strong authentication market for IP networks today, when compared to the emerging technology of PKI based strong authentication. An analysis of the general strengths and weaknesses of each of these two strong authentication schemes follows.

Dynamic Tokens

Security Dynamics, Inc. (http://www.securitydynamics.com) product, SecurID, is the market leading dynamic token-based authentication product. When used in conjunction with it's ACE/Server product, the end-user is authenticated based upon a combination of "something you know" (their secret PIN) and "something you have" (SecurID token) to provide an improved level of access control security over a weak authentication system. The SecurID token is actually random number that changes every minute and is generated by a SecurID token generator. The generator may take the form of a physical card with a Liquid Crystal Display (LCD) screen the size of a credit card, or it may be a software based token generator located on the end user's hard drive. Besides SecurID, other dynamic token-based authentication systems exist on the market today, and all share many similar attributes, despite operational and implementation differences.

Because the dynamic token simply presents a unique access code to the end-user, which the end-user enters at the keyboard in combination with the unique PIN known only to the end-user, dynamic tokens do not require any special computer hardware (just the token generator) at the client system. Dynamic tokens are a proven strong authentication technology that has been in use for some time. However, the technology does have a number of important drawbacks.

- The technology is proprietary and designed to work within a well-defined closed environment.
- Because the systems are not based on public standards, they are not compatible with the industry standards currently gaining wide acceptance in the market today, which will present significant impediments to interoperability with new applications.
- Each access control system or application system must be equipped with a corresponding proprietary server.
- Most users of the system have found the interface to be cumbersome and annoying.
- Although the price of the tokens (which typically expire over time) have come down, the per user costs can be significant.
- This system provides only authentication. The technology does not lend itself to the provision of confidentiality, integrity or non-repudiation.
- The costs of administering such a system are non-trivial.

Public Key Infrastructure Digital Certificates

Intelispan, Inc (http://www.intelispan.com) is the first company to publicly announce a Public Key Infrastructure IP network authentication solution. Intelispan, through a subsidiary, has announced a strategic alliance agreement with WorldCom, Inc. (http://www.wcom.com) to incorporate the solution into a network managed by the WorldCom Advanced Networks (http://www.wcom.net) division.

A Public Key Infrastructure network authentication solution is similar to a dynamic token solution in that they both employ a combination of “something you know” and “something you have” to authenticate a user. However, this is the extent of their similarities.

With PKI network authentication, the “something you know” is the username/password, while the “something you have” is a secret key unique to each user and known only by that user, stored on a digital certificate (cert, for short). One of the most appealing features of this solution is its nearly transparent integration with most existing authentication schemes, from the end users perspective.

PKI cert-based authentication actually incorporates a two phase logon authentication process. The first phase of authentication is performed just as is performed today as part of any standard weak authentication system, verifying the end-user’s network username/password. In the second phase of authentication, the end-user’s secret key, which has been secured with a separate password, is used to digitally sign a response to a challenge issued by the network based authentication server. Only users in possession of a valid secret key will pass this second authentication phase and be granted authority to access their pre-defined network resources.

Note that the user interface has not been significantly complicated to achieve this two phased logon. The end-user is still only required to enter their username/password at logon. The only new requirement is that the user’s secret key and associated cryptographic software is present on the client system. Currently the secret key is secured to disk or diskette with a user-selected password, but in the future these keys may be stored on a “smart” card.

Some other features of the PKI cert-based authentication system:

- Based on a non-proprietary architecture, industry standard PKI implementations will simplify interoperability with future applications.
- PKI is gaining acceptance as the technology of choice for provision of other security services such as integrity, confidentiality and non-repudiation. The same PKI used for cert-based network authentication provides the infrastructure for delivering additional security services.
- The corporate customer or designated third party controls the issuance and revocation of all public keys, addressing customer’s concerns over relinquishing management of the control of access to its critical resources.
- Can be used to authenticate devices as well as end-users.
- Administration of the system is straightforward and typically is performed by the customer.
- Combined with the deployment of “smart cards”, which are easy to carry, inexpensive and are gaining wide acceptance as the standard for portable tokens, such solutions are very “end user friendly”.

Integrity

A degree of data integrity is provided as a function of virtually all modern data communications networks as an integral part of the network transport protocols, including TCP/IP. However, network level data integrity does not provide the application level integrity required by most electronic commerce applications.

Digital signatures are rapidly becoming the accepted means for providing application level proof of integrity. To create a digital signature a party to a transaction runs the message text through a hash algorithm generating a message digest. The message digest can be viewed as a compressed “fingerprint” of the message itself. The message digest is then encrypted using the secret key of the originating entity to create a digital signature. The digital signature is then sent along with the original message text to the recipient who can verify the integrity of the message using the originator’s public key (published by a network-based Certificate Authority) and the digital signature received with the message. If even 1 bit of the message has changed in transit, this process will detect it.

Dynamic Tokens

Dynamic token implementations do not address message integrity.

Public Key Infrastructure Digital Certificates

Public Key Infrastructure currently provides assurance of message integrity as part of the authentication protocol when a user attempts to gain access to a network resource. The response to an authentication challenge issued by the authentication server is digitally signed with the user's secret key. The process provides assurance not only that the response was signed with a valid secret key, but that the contents of the response have not been corrupted.

Message integrity is considered to be best addressed at the application level and are not an appropriate function of the authentication process. Any time cryptography is employed, processing resources are required, it is therefore prudent to only apply this processing to communications which require it.

However, PKI used for network authentication does provide the standards-based infrastructure which enables the provision of application level integrity. The number of applications that can be developed to take advantage of this infrastructure is unlimited.

Confidentiality

Confidentiality can be achieved in a number of ways, typically through the use of encryption. Many network-based encryption solutions exist in the industry today. All of the emerging "tunneling" protocols incorporate some type of encryption. Any encryption supplied by network components only provides transport level confidentiality. Transport level confidentiality ensures that a third party cannot access the message by capturing the data while it is in transit.

Much of the fear with regards to transport level security has been a direct result of the inherent vulnerability of any data traversing the Internet. Because there is no way of knowing where this data will be routed or what servers it may traverse in its path from origin to destination, there is justifiable concern over who might have access to this data.

For confidentiality to be effective, however, it must be assured beyond the transport of the data. A message will inevitably be stored to disk or some other storage medium. Assurance must be provided to guarantee that the confidentiality of this data is maintained wherever it might be stored.

Dynamic Tokens

Dynamic token implementations do not address message confidentiality.

Public Key Infrastructure Digital Certificates

As stated previously, with the exception of the user authentication protocol, the PKI cert-based network authentication does not provide confidentiality for messages after authorization to the network. Rather, the PKI serves as the basis for the development and provision of application level transaction confidentiality.

Non-Repudiation

More so than even confidentiality, non-repudiation is a function that must be provided at the application level. Transactions take place between people or legal entities, not between servers and communications controllers, therefore non-repudiation at the transport level has little practical application.

Dynamic Tokens

Dynamic token implementations do not address non-repudiation.

Public Key Infrastructure Digital Certificates

PKI cert-based network authentication currently employs non-repudiation at two points within the system architecture. The first is as part of the end-user authentication protocol, where the response to a challenge issued by the authentication server is signed using the end-user's secret key. This provides an audit log containing a digitally signed transaction as proof that the logon was completed by an entity in possession of the user's secret key. The second is as part of the user registration process.

User registration is the process where the end-user's identity and credentials are verified before the user is issued their secret key and public key certificate attesting to the identification of the owner of the associated secret key. The registration process is critical to the overall security of the system as it controls the "keys to the kingdom".

It's well known that most breaches of system security are a result of accidental or intentional violation of security policy by the customer's own employees. For this reason it's vital that all certificate issuance and revocation requests be digitally signed with the secret key of the RA administrator. PKI provides this level of assurance today, and will only accept certificate requests signed by a RA administrator in possession of a valid key and certificate.

As with confidentiality, non-repudiation will need to be provided at the application level, and may leverage the public key infrastructure provided by the same PKI used for network authentication.

Summary

Many IP network authentication schemes are available for consideration today. The optimal implementation for a specific application requires a careful analysis of the potential costs of compromised security.

Username/Password

Authentication based only on username/password is an accepted and proven technology which will continue to be acceptable to a significant number of customers. Clearly, it is not appropriate for customers needing any level of strong authentication, or application level integrity, confidentiality or non-repudiation. Over time, username/password authentication will likely become inadequate for a growing number of corporate customers as newer technologies gain broader acceptance.

Dynamic Tokens

Dynamic tokens provide improved end-user authentication over username/password solutions. However, dynamic tokens do not provide the infrastructure necessary to provide application level confidentiality, integrity or non-repudiation. Dynamic token architectures benefit from the fact that the technology is proven and that there is a significant installed base of users. However, many customers use the system grudgingly due primarily to the fact that most end-users find the system to be cumbersome and annoying. Further, Dynamic token solutions in the market today are proprietary, available from a single vendor, and are based upon dated technology providing limited growth opportunity and virtually no interoperability with other systems.

Public Key Infrastructure Digital Certificates

Public Key Infrastructure cert-based network authentication provides end-user authentication equivalent to, or superior to, that provided with dynamic tokens. System administration is easier than for dynamic

tokens, and there is a lower initial investment in infrastructure required by the customer. The user interface is easier and more user friendly providing a nearly transparent experience when compared to existing authentication schemes.

Intelispan's implementation of this solution is network based. Use of the system by customer requires no capital investment in the technology, unlike dynamic token solutions, minimizing the customer's risk and exposure to shifting technology architectures.

In addition to strong end-user authentication, the same PKI used for network authentication also provides the PKI required for existing and emerging electronic commerce applications. Based on open industry standards, PKI provides a framework for corporations planning to take advantage of emerging technologies that will provide the application level confidentiality, integrity and non-repudiation that electronic commerce requires.

Biometrics

Biometric network authentication is an interesting technology with excellent potential. But deployment and administration costs present real barriers in the short term. Also, like dynamic tokens, the technology only provides authentication, not integrity or confidentiality. The technology could be used to provide non-repudiation but most likely only in combination with public key technology.