Security Within the Heterogeneous Environment and the Impact of Microsoft Windows 2000

April 1999
# Table of Contents

1 Introduction .................................................................................................................. 4  
2 Homogeneous Security In Heterogeneous Environments ........................................... 5  
   2.1 A Homogeneous Infrastructure ................................................................................. 5  
   2.2 Establishing a Consistent Security Framework ......................................................... 6  
3 Today’s Enterprise Environment ................................................................................... 7  
   3.1 Desktops .................................................................................................................. 7  
   3.2 Servers .................................................................................................................... 7  
   3.3 Remote Access ......................................................................................................... 8  
   3.4 Security Issues and Implications ............................................................................. 8  
   3.5 Security Protocols/Infrastructure ........................................................................... 9  
4 Microsoft Windows NT 4.0 and the Impact of Windows 2000 ..................................... 11  
   4.1 Windows 2000 Interoperability .............................................................................. 11  
   4.2 Migrating from Windows NT 4 to Windows 2000 ................................................... 12  
5 CyberSafe Solution ....................................................................................................... 13  
   5.1 Multi-mechanism Authentication ............................................................................. 13  
   5.2 Tools ....................................................................................................................... 13  
   5.3 Application Independent Security ........................................................................... 14  
   5.4 Trusted Solutions ................................................................................................... 14  
   5.5 Customized Solutions ............................................................................................. 14  
6 Conclusion ....................................................................................................................... 15  
   6.1 For More Information ............................................................................................. 15
1 Introduction

Heterogeneous computing environments are typical in most organizations. Desktop clients run local user applications, connect to network file servers, and interface with back-end server machines which run mission-critical business applications. Rarely is a single computing platform utilized. Many companies operate multiple servers, configured with operating systems appropriate to the types of functions required to best meet corporate objectives. Utilizing a diversified enterprise architecture provides an organization with the best available solutions. According to one Gartner Group analyst “enterprise management consists of many Networked Systems Management (NSM) disciplines. No single vendor, including Microsoft, can offer integrated solutions for all management disciplines, even in a homogenous NT environment.”

With the increasing popularity of intranets and extranets within enterprise networks, organizations are realizing that distributed security is an imperative enabling technology. But it can be difficult to ensure that a comprehensive security architecture is in place, since each platform utilizes a different security mechanism. This paper describes how security can be deployed consistently across heterogeneous environments, regardless of the types of systems present. It first addresses the increasing need for security. Then it describes a typical enterprise environment, including security issues and requirements. Next, security for Microsoft Windows NT 4.0 and Windows 2000 is discussed. Finally, it briefly illustrates how CyberSafe solutions can promote interoperability across multiple platforms, providing extensibility and simple migration paths as new products are introduced.

---

2 Homogeneous Security In Heterogeneous Environments

Enterprises may maintain various disparate systems and applications, but the level of security and the security policy that applies to all systems should be the same. Typically, an enterprise environment is quite dynamic, with new requirements being introduced frequently. In addition to maintaining existing multi-platform systems, administrators face challenges related to company growth and strategy, such as refocusing of corporate direction, expanding user bases, and increasing dependence on the Internet. Changing business needs often call for the addition of operating systems and newly developed applications. Organizational boundaries continuously shift and change as the need to share information between employees, customers, and other businesses increases. Roaming users cause network access points to shift.

In order to support environments like these, a security solution must be flexible and it must provide interoperability and extensibility in the future. Such a system must ensure uniform, well-known, acceptable trust across all platforms and applications. Building consist security into a heterogeneous environment is challenging. It requires intensive system architecture planning by the IS department, but the result is the ability to easily add new systems as needed.

2.1 A Homogeneous Infrastructure

A homogeneous platform environment provides consistency within an enterprise, but it means relying on one vendor, which may be limiting, depending on an organization’s particular requirements. Servers have distinct hardware and operating system requirements due to issues such as availability, load, and throughput. Working with a single provider means accepting the capabilities, as well as the limitations, of the vendor’s particular server.

While it may be restrictive, using a single vendor is cost-effective. Working with a single operating system saves valuable system administration time and ultimately, saves the company money. This is especially apparent in the case of desktop systems that do not run business critical or specialized applications.

For the majority of today’s organizations, remaining loyal to one vendor can limit businesses as they work to achieve their objectives. Many organizations have built their infrastructures over time, acquiring platforms one at a time as business objectives dictated, so one vendor may not be able to meet all of their needs. Applying a consistent security infrastructure across existing, disparate systems and applications offers the most practical solution. Uniform security helps establish an acceptable level of trust across the enterprise and ensures a smooth migration path when new platforms need to be added.
2.2 Establishing a Consistent Security Framework

A homogeneous infrastructure may not be practical. The fact is, most organizations are dealing with some type of heterogeneous architecture. Doing so allows them to work with best-available solutions from different vendors and avoid the limitations that single-vendor relationships can create. Building base level, consistent security into a hybrid infrastructure is essential and offers several benefits, including the easy implementation of dissimilar platforms, and seamless coverage from user to application, across the network. Additionally, a consistent infrastructure allows for integration of heterogeneous systems under a common level of trust, ensuring a common security policy that is more easily followed and enforced. In order to be effective, it requires strong security mechanisms, a well thought-out architecture, and diligent planning.

A consistent enterprise security architecture provides the framework for integrating disparate platforms and applications. It allows business opportunities and decisions, not system limitations, to dictate growth. The actual implementation of such a framework requires that uniform levels of trust be established across various systems. Such uniformity may be achieved via the integration of key management systems and protocols with heterogeneous platforms and applications. This allows key applications (such as operating system access or enterprise resource planning applications) to utilize consistent security mechanisms so that a uniform security policy may be enforced.

Kerberos and Public Key systems are examples of standard security mechanisms that may be utilized for deploying a consistent security infrastructure. However, it should be noted that many legacy systems and applications may not be modified to support these systems. In these situations, a system of secure brokering of credentials is appropriate.

Providing a consistent security infrastructure requires thoughtful planning for appropriate phased deployment and integration. Some systems may be secured without any modification to the application. Some applications may require modification in order to "security enable" them. As applications and systems are added, they must be consistent with the infrastructure being deployed; therefore, a solution based on open standards provides greater flexibility and is more easily implemented than a proprietary solution.

Through careful preparation, a consistent security infrastructure not only secures current heterogeneous applications and systems, it provides a scalable infrastructure, allowing organizations to easily grow and extend beyond current enterprise boundaries.
3 Today’s Enterprise Environment

Made up of desktops, servers, and remote access applications, today’s enterprise networks enable users to access the information they need, regardless of network topology or physical location. This, in turn, necessitates the implementation of security measures to ensure valuable information is protected. Typically, an enterprise depends on the various security functions that each individual application provides.

3.1 Desktops

Desktop environments are migrating towards homogeneity, with the majority of organizations using Windows as their client software of choice. This trend is occurring primarily due to the cost of deployment and support. The majority of users work with applications that are not mission-critical for the organization. For example, a typical user may run word processing, spreadsheet, presentation, and email applications. These applications may reside locally or on file servers, and are executed within the local CPU. A single, homogeneous desktop platform presents an easy, cost-friendly solution for an already overworked IT organization.

Such an environment presents a fairly well encapsulated group of machines and applications that may be managed within a separate domain of security administration. For example, Windows NT networks are managed by a domain controller that provides for authentication and authorization.

3.2 Servers

Organizations tend to run mission-critical applications on application servers that have specialized characteristics such as scalability, throughput, fault tolerance, and redundancy. For example, MVS mainframes or UNIX servers may be utilized in high throughput environments; Tandem servers may be utilized in applications that require fault tolerant transaction processing. This valuable functionality, and the mission-critical nature of the applications, justifies the added expenses associated with deployment and maintenance. Whereas an organization may make the decision to standardize on relatively low cost desktops systems, it is business necessity that drives the purchase of servers that support mission-critical functionality. Enterprises should choose the operating systems that best fit their computing requirements. ²

Each system operates within its own realms of security administration. For example, UNIX systems utilize user databases that may be local (i.e. /etc/password files) or centralized (ala NIS). MVS systems may make use of RACF, CA-ACF2, or CA-Top Secret. Tandem and VMS systems each utilize their own security databases as well. Organizations are faced with the integration and

interoperability issues presented by disparate realms of security and security policy among their server and their desktop environments.

### 3.3 Remote Access

Enterprises need to support evolving points of access to their organizations. Companies may have remote or traveling employees. Customers, suppliers, or partners may require access to portions of the corporate network. One obvious vehicle for providing access is the Web, which further complicates the issue of end-to-end security.

Web-based systems present a good example of the shape of multi-tier security issues to come. The web server is used as an intermediary within a multi-tier application. As a result, these systems are faced with issues of true end-to-end authentication, authorization, and delegation of security credentials. In many systems, these issues are dealt with inadequately or are ignored.

Non-web-based network access generally involves either a dial-up connection or a secured connection provided by a Virtual Private Network (VPN) or firewall. Typically, the network access points are administered as a separate realm of security.

### 3.4 Security Issues and Implications

In order to effectively maintain and enforce an organizational security policy, an enterprise must implement a consistent security architecture that covers heterogeneous systems and applications, including remote access. As organizations address their network and application security, they encounter a common set of requirements for successful deployment.

*Scalability and extensibility.* Enterprises are growing and becoming more distributed. In order to effectively secure and support such environments, a security architecture must be able to grow with an organization.

*Toolkits.* Organizations need an easy way to incorporate security into applications, regardless of platform. Since most organizations are not in the security business, they need standards-based security tools they can use to secure their applications, and that provide the benefits of a large pool of talent.

*PKI management.* A Public Key Infrastructure (PKI) is an accepted component of an organization's security framework. Deploying a PKI is a cumbersome task as it involves registering, distributing, and administering large numbers of public key credentials. Enforcement of security policies within a Public Key Infrastructure is not well understood. The most notable example of this is the challenge of certificate revocation.
list management. Additionally, enterprises are faced with the issue of the high per-seat costs associated with the deployment of smart cards and smart card readers.

*Application independent security.* Sometimes, security can not be built into an application because the company does not have the source code or does not wish to incur the cost of code modification. There is a need for securing applications without having to modify them.

*Custom-tailored solutions.* No two sites are identical; each has special security requirements and objectives. Therefore, an ‘out-of-the-box’ security product is rarely sufficient. For a security solution to be effective, it must be integrated within the context of an organization's business objectives. This may require the selection of disparate, off-the-shelf products, the services of a security integration entity, and/or the development of custom components in order to meet unique requirements.

*Proven reliability.* Due to the nature of important business systems and applications, IS managers are understandably wary of introducing security technology that may exhibit unexpected behavior or cause unnecessary periods of downtime. Consequently, field-proven security solutions provide assurance of reliability and delivery of expected behavior.

*Education.* Implementing and securing new platforms involves issues that affect many facets of an organization. From understanding security issues and knowing where to deploy security within the enterprise, to educating end users and diminishing the risk of security breaches, most organizations would benefit from outside assistance from security experts.

### 3.5 Security Protocols/Infrastructure

Both Kerberos and Public Key infrastructures are recognized methods of providing a common security infrastructure for achieving a consistent security policy and providing secure single sign-on within an organization. Each solution has its own set of advantages and issues. Consequently, a hybrid solution within an enterprise deployment can offer the best of both technologies while mitigating the associated issues.

Kerberos is a secret key system that utilizes a central key repository and server (the Key Distribution Center or KDC) for establishing trust between communicating parties. Principals engaged in secure communication utilize limited lifetime tickets that are issued by the KDC. In addition to the computational speed of conventional cryptography, the primary advantage of Kerberos is that it centralizes the administration of both the principals and the security policy.
Consequently, Kerberos is very well suited for providing security for centrally controlled domains in which principals must authenticate sessions (as opposed to store and forward types of scenarios). Kerberos may not be as well suited for applications that require decentralized administration of communicating security principals.

A Public Key Infrastructure (PKI) utilizes public/private key pairs and a trusted third party (a certification authority or CA) that certifies the binding of a public key to a principal name (a distinguished name in X.500 parlance). This type of crypto-system has the advantage of allowing for greatly distributed communication between principals; however, the administration of the principals and the associated security policy is also distributed. Therefore, the administration of a PKI is less centralized than that of Kerberos. Public Key cryptography is also very computationally intense. Measured in CPU time, public key cryptography is hundreds to thousands times more expensive than symmetric key cryptography for comparable strength keys.
Microsoft Windows NT 4.0 and the Impact of Windows 2000

Microsoft has dominated the desktop environments of most organizations. Windows NT 4.0 has presented a cost-effective, homogeneous solution for managing the environments and applications for countless desktop users. By utilizing Microsoft domain controllers to manage the administrative realms of desktop users, IS managers have been able to show efficiencies of scale due to the homogeneity of a Windows NT-based solution. Within the larger, heterogeneous enterprise, there has been the need to integrate Windows NT 4.0 domains with the administrative realms of other platforms and applications.

One of the integration issues within a heterogeneous enterprise is that of security, i.e., how to seamlessly secure disparate platforms without leaving gaps. Windows NT 4.0 utilizes Microsoft proprietary mechanisms for securing Windows NT domains. Other platforms and applications provide their own security mechanisms. The issue enterprises face is establishing a uniform security framework in which all platforms and applications can interoperate with adherence to and enforcement of a consistent security policy. The model then becomes one of brokering trust between these various platforms (such as Windows, UNIX, or MVS) and applications (such as Oracle or SAP).

Kerberos is a security technology that may be utilized as a component of brokering trust between various platforms and applications. Windows 2000 will use Kerberos as its basic form of authentication. The fact that Microsoft has chosen Kerberos as its security technology for Windows 2000 validates the capabilities of Kerberos for securing realms of desktop users and their applications. By choosing to utilize this open standard security protocol, Microsoft has opened the way for consistent integration of security across heterogeneous platforms.

In addition, Microsoft is supporting the Generic Security Services API (GSS-API) token format (an Internet standard) within their Security Support Provider Interface (SSPI) security API. What this means is that applications on non-Microsoft platforms may interoperate with Windows 2000 based on a standard wire-level data format. With Windows NT 4.0, an organization interoperates with Microsoft domains. With Windows 2000, an organization must still interoperate with Microsoft domains; however, interoperability may be achieved via standard security protocols.

4.1 Windows 2000 Interoperability

As stated above, with the introduction of Windows 2000, the options for interoperability improve over Windows NT 4.0. Basically, there are two main ways to address interoperability and enterprise deployment. The first is by improving the configuration that is already in place. By
using the Kerberos protocol, an organization is able to establish trust relationships between
different administrative security realms. This provides consistency for enforcing security policy
across an organization's various platforms. Pre-Windows 2000, organizations had to address
interoperability with basically self-contained Windows domains, i.e. desktop operating systems,
Windows file sharing, and Microsoft-specific server applications such as Exchange. At the core
of the Windows domain has been the Microsoft domain controller, implementing a proprietary
security protocol. With the introduction of Windows 2000, the domain controller will utilize a
standard security protocol. This has the effect of improving the opportunity for establishing a
consistent interface with the rest of a heterogeneous enterprise. The second way to address
interoperability is by using interoperable programming tools. Since the Microsoft SSPI is wire-
compatible with the GSS-API, an organization may develop applications on UNIX, for example,
that will interoperate with applications that were developed on Windows 2000 using SSPI.

4.2 Migrating from Windows NT 4 to Windows 2000

The transition from Windows NT 4.0 to Windows 2000 is an issue that Microsoft has been
addressing with its customer base. For example, Windows 2000 will be backward compatible
with NT 4.0 authentication. From a security perspective, within a heterogeneous environment,
this transition may be relatively painless. For an organization with heterogeneous platforms, the
issues of interoperability with Windows do not change. As stated above, trust relationships may
be established between Windows 2000 and other platforms. Since Windows 2000 is utilizing a
standard security protocol, the interface from a Windows domain to the rest of a heterogeneous
environment is actually more consistent. The same type of trust relationship may be utilized in a
more limited manner now on Windows 4.0 by implementing a portion of a corporate security
infrastructure on Windows NT 4.0. For example, a Kerberos security server may run on Windows
NT 4.0, and applications may be developed to utilize the GSS-API. This may be particularly
useful when developing applications on Windows NT 4.0 that require security. An organization
can develop GSS-API-based applications today on NT 4.0 with the intention that those same
applications will continue to function within a Windows 2000 environment.

3 For more information, see Migrating From Microsoft Windows NT Server 4.0 to Windows 2000 Server
5 CyberSafe Solution

CyberSafe uses its TrustBroker product line and the expertise of its consultants to provide comprehensive security solutions to distributed network environments. Built on open standards to be used in multi-platform, heterogeneous application environments, CyberSafe products utilize an organization’s existing infrastructure to support security and business objectives. As new operating systems, applications, and security mechanisms are introduced, CyberSafe is able to seamlessly integrate them into an existing environment. CyberSafe solutions have always addressed multiple platforms, including Microsoft Windows NT.

5.1 Multi-mechanism Authentication

TrustBroker Security Server from CyberSafe is the first multi-mechanism authentication server; it utilizes the best of both of Kerberos and Public Key protocols, so organizations can take advantage of either, or both. It is designed on open standards, ensuring interoperability between existing security infrastructures and new platforms that may be added in the future.

CyberSafe is the only company providing a Kerberos-based security server on the NT platform, supporting Kerberos Versions 4 and 5. Windows 2000 is built on Kerberos 5. Therefore, organizations can deploy a Kerberos-secured network today, on NT 4.0, using the TrustBroker security architecture. Then, when Windows 2000 becomes available, a simple migration path already exists.

In addition, CyberSafe products work with Public Key authentication mechanisms, allowing organizations to integrate the best of Public Key and Kerberos protocols into their enterprise. TrustBroker Virtual Smart Card (VSC) gives companies the ability to securely store a smart card image and retrieve it on demand for any PK-secured application. It allows for initial authentication with Public Key credentials. TrustBroker VSC eliminates deployment issues and the hassles of floppy disk use and local file storage, enabling centralized Public Key management and eliminating the expense of physical smart cards and readers.

5.2 Tools

TrustBroker Developer Pack supplies tools to secure applications on multiple platforms. The Application Security SDK, found within the Developer Pack, contains the industry-standard GSS-API. TrustBroker Security Suite is interoperable with the GSS-API and the Microsoft SSPI. This means organizations can use Developer Pack to develop security-enabled applications and operate them in a secured fashion today, knowing it will be easy to port to SSPI later when they implement Windows 2000. Also, developers can write SSPI applications for Windows 2000 that also work with GSS-API enabled applications, since SSPI utilizes the GSS-API token format.
5.3 Application Independent Security

Often applications were not designed with security in mind and developers no longer have access to the source code. So using a standards-based SDK is futile. The Defensor product line from CyberSafe creates a secure channel between authenticated users and their applications, eliminating the need to modify the application in order to secure it.

5.4 Trusted Solutions

Founded in 1991, CyberSafe is a recognized leader in the industry, providing security solutions for Fortune 500 companies, including many of the top financial institutions. CyberSafe products have been part of some of the world’s largest security deployments. CyberSafe senior scientists are among the originators of today’s most sophisticated security technology; their knowledge helps design CyberSafe products. As new technologies and platforms are introduced, they will be supported by the capabilities of the CyberSafe hybrid architecture. The comprehensive security solutions from CyberSafe are unmatched by any newcomer to the security server market.

5.5 Customized Solutions

Each enterprise has different, specialized objectives and concerns. An ‘out-of-the-box’ security product rarely provides an effective, comprehensive solution. The experience of CyberSafe security consultants, combined with field-proven CyberSafe products can provide customized solutions that ensure uniform trust across all platforms and applications, supporting an organization’s business and security needs.
6 Conclusion

Securing and deploying new platforms into enterprises containing mixed platforms is challenging but in most cases is preferable to working within a single platform server environment. The ability to easily integrate best-available solutions into existing infrastructures often outweighs the cost-savings associated with single-vendor solutions. Most organizations find operating within a heterogeneous environment allows them to better meet their business objectives, because each platform offers specialized capabilities. As enterprise networks expand, the issue of security is at the forefront of most IT managers’ strategic plans.

When deploying security into heterogeneous platform environments, the most effective method is one that is consistent. Kerberos and Public Key are examples of recognized technologies that can be utilized in achieving consistent security. Rather than each application providing its particular security function, a mechanism for brokering security is needed that incorporates disparate security implementations into one cohesive offering.

As new platforms, such as Windows 2000, are introduced, they need to be easily integrated and deployed into diverse enterprise networks, without sacrificing security. Using the Kerberos protocol allows an organization to build trust relationships between administrative security realms, providing consistent security policy deployment and enforcement. Also, utilizing interoperable programming tools lets an organization develop applications on one platform that interoperate with programs written on a different platform. The fact that Microsoft has based Windows 2000 on Kerberos supports the fact that it is a powerful, relevant mechanism for securing today’s enterprises.

Using CyberSafe solutions, companies are not limited in their enterprise security choices. Based on multi-mechanism security, CyberSafe products allow organizations to establish a security framework that allows for easy integration of new platforms, including Windows 2000.

6.1 For More Information

For further information on CyberSafe products and services, please contact CyberSafe at 1-888-391-9922 or visit the CyberSafe web site at www.cybersafe.com.