

Topics

- Overview
- Scope of Primer
- Business Considerations
 - Authentication
 - Authorization
 - Encryption
- Summary

Business Challenge

Sharing critical business data inside the firewall poses little problem when using a traditional “wired” network. It is usually straightforward to secure physical access to connected computers and thus prevent external hacking from occurring. All of this changes when moving to wireless, as the physical connectivity requirements are removed and new types of hacking can occur. This document covers the basic security issues and strategies for deploying Visual KPI in a secure, wireless corporate environment.

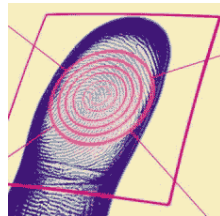
Scope of this Document

Safeguarding data and systems means allowing legitimate users relatively pain-free access while preventing unintended use. Security mechanisms typically fall into one of three broad categories: Prevention, Detection and Response. These three categories span an impossibly large technological space, so this security Primer will only deal with Prevention as it pertains to Transpara’s Visual KPI system.

Business Data Access Considerations

Prevention of unintended access to corporate systems can be accomplished by paying attention to just a few ingredients. These elements ensure that the people who gain access to your business data or systems are identified, given only specific access rights and securely receive data that you intend to send them.

Authentication



In a distributed computing environment where important data resides on more than one computer, the most basic element of security is User Authentication. Simply stated, the computer which “owns” the data to be accessed needs to believe that the inbound access request comes from a known User. It is therefore the job of User Authentication to provide assurance to the data owner that the request for data is from a legitimate source. The most common methods for securing access to web-based content are listed in Table 1 below. Visual KPI supports all of these methods, and it is typically the corporate IT Group that selects how a web site user is to be authenticated.

Table 1 – Typical Authentication Methods

Method	Security Level	Sends Passwords How?	Usable Across Proxy Servers and Firewalls?	Client Requirements
Anonymous Authentication	None	N/A	Yes	Any browser
Basic Authentication	Low	Base64 encoded clear text	Yes; however, sending passwords across a proxy server or firewall in clear text is a security risk because Base64 encoded clear text is not encrypted. Basic authentication should be partnered with SSL. This encrypts all data, including passwords, on the wire.	Most browsers
Digest Authentication	Medium	Hashed	Yes	Internet Explorer 5, or later
Advanced Digest Authentication	Medium	Hashed	Yes	Internet Explorer 5, or later
Integrated Windows Authentication	High	Hashed when NTLM is used. Kerberos ticket when Kerberos is used	No, unless used over a PPTP connection	Internet Explorer 2.0 and later for NTLM, and Windows 2000 or later with Internet Explorer 5 or later for Kerberos
Certificate Authentication	High	N/A	Yes, using an SSL connection	Internet Explorer and Netscape
.NET Passport Authentication	High	Encrypted	Yes, using an SSL connection	Internet Explorer and Netscape

Authorization (Rights Determination)



Knowing who you are dealing with is a prerequisite to deciding whether or not to grant access to the requested data. The next step is deciding just what this known requestor has the right to access. It may be certain Functions of a complex Line of Business application like SAP or it could be as simple as certain Pages of a web site. In either case, there needs to be a database of some type

where the Users can be mapped to allowed Functions or Pages. This is where it becomes convenient to define Groups of Users, so that a collection of people with the same characteristics can be granted the right to access data or business functions they have in common.

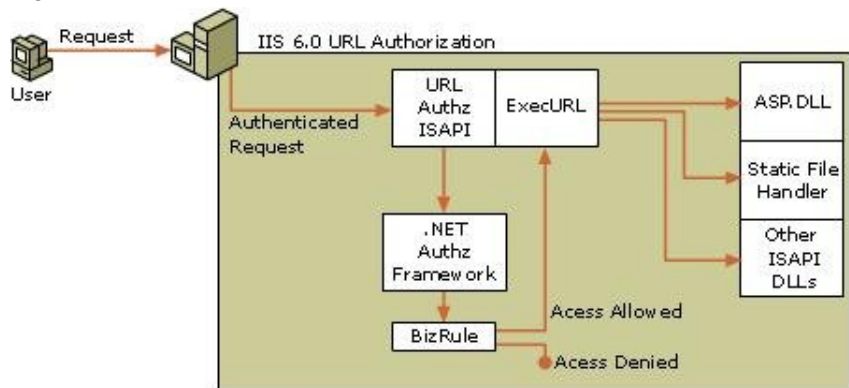
Authorizing user access to Web application resources requires the management of Windows Access Control Lists (ACLs). In turn, maintaining ACLs requires administrators to track precisely which permissions are needed on each resource for each user or group to perform meaningful tasks. IIS URL authorization allows Windows administrators to simplify access management by authorizing user access to the URLs that comprise a Web application.

When a user requests access to a URL, IIS URL authorization validates the user's access based on that user's roles, which can be defined in Lightweight Directory Access Protocol (LDAP) queries, custom user roles, and Authorization Manager scripts (BizRules). This allows administrators to simplify access control management by controlling all user access to URLs instead of controlling access per ACL on each resource.

IIS URL authorization is implemented as an Internet Server API (ISAPI) interceptor (in the diagram below, URL Authz ISAPI). When an application, virtual directory, or URL is configured to use IIS URL authorization, each request to a URL will be routed to the URL authorization ISAPI interceptor. The URL authorization ISAPI interceptor will use Authorization Manager (in the diagram, .NET Authz Framework) to authorize access to the requested URL. The URL must be associated with an Authorization Manager policy store that contains the authorization policy for the URL. Once the client has been authorized to access the URL, the URL authorization ISAPI's Execute URL feature (in the diagram, ExecURL) will pass the request to the appropriate handler for the URL, such as ASP.dll, another ISAPI, or the Static File Handler.

Authorization Manager can be used to enable role-based security. However, if it is important to control access to individual database objects, the AzMan is not enough. In this case, it will be necessary to apply a Windows ACL to individual database objects.

Figure 1 – User Authorization Information Flow



By using IIS 6.0 URL authorization, an administrator can control access based on information that is only available at runtime. For example, if

you have a Web page that should only be available to employees in a given cost center or to employees of a certain age, you can assign roles to the correct users based on LDAP queries that will check the cost center or age attributes on a user's object. If employees can only access certain pages on certain days of the week or during a certain time of day, a BizRule can be created which grants access to the URL based on these values or any value that can be asserted at runtime, including IIS Server Variables.

Data Stream Encryption



Once the data owner has elected to provide the User with the requested Data or Function, it might be a good idea to encrypt or hash the data stream as it is sent, to prevent any unintended recipients along the way from understanding or using the data. Visual KPI supports all of the IIS-compatible encryption methods described below.

How Encryption Works

Encryption is the process of scrambling information by applying a mathematical function in such a way that it is extremely difficult for anyone other than an intended recipient to retrieve the original information. Central to this process is a mathematical value, called a *key*, which is used by the function to scramble the information in a unique and complex way.

Your Web server uses essentially the same encryption process to secure communication links with users. After establishing a secure link, a special *session* key is used by both your Web server and the user's Web browser to both encrypt and decrypt information. For example, when an authenticated user attempts to download a file from a Web site requiring a secure channel, your Web server uses a session key to encrypt the file and related HTTP headers. After receiving the encrypted file, the Web browser then uses a copy of the same session key to recover the file.

This method of encryption, although secure, has an inherent drawback: During the process of creating a secure link, a copy of the session key might be transmitted across an unsecured network. This means that a computer vandal intent on compromising the link need only intercept and steal the session key. To safeguard against this possibility, however, your Web server implements an additional method of encryption.

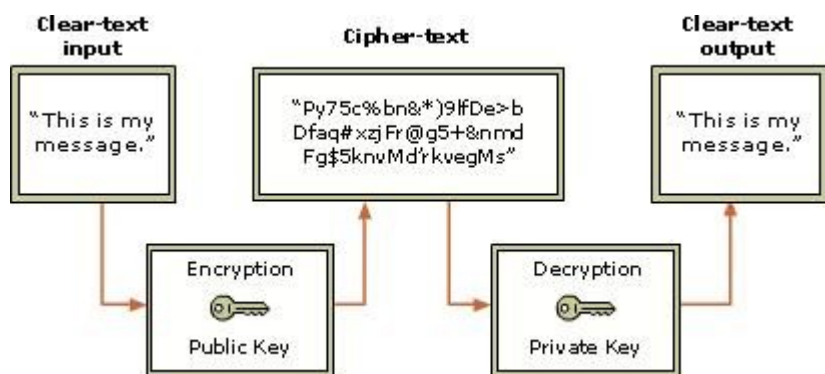
Public Key Encryption

The Web server's Secure Sockets Layer (SSL) security feature utilizes a technique known as *public key* encryption to shield the session key from interception during transmission. Public key encryption, which

involves the use of two additional keys, a *private* and a *public* key, works in the following manner (see Figure 2):

1. The user's Web browser establishes a secure (https://) communication link with your Web server.
2. The user's Web browser and your server engage in negotiation to determine the degree of encryption to use for securing communications.
3. Your Web server sends the browser its public key.
4. The Web browser encrypts information used in generating a session key with the server's public key and sends it to the server.
5. Using the private key, your server decrypts the message, generates a session key, encrypts it with the public key, and sends it to the browser.
6. Your Web server and the browser both use the session key to encrypt and decrypt transmitted data.

Figure 2 – Public Key Encryption



Notice that the private key serves an important role in ensuring that your communication link remains secure. You should take every reasonable precaution to protect the private key from loss or theft. If you suspect that your private key has been compromised, notify your certification authority, use the Web Server Certificate Wizard to create a new certificate request, and then obtain a new server certificate.

Session Key Encryption Strength

A session key's *strength* is proportional to the number of binary *bits* comprising the session key file. This means that session keys with a greater number of bits have a greater degree of security, and are considerably more difficult to forcibly decode.

When a user attempts to establish a secure communication channel with your Web server, the user's browser must negotiate the strongest possible level of encryption, or session key strength, that can be used to secure communications over that channel. This means that both your Web server and the user's browser must be equipped with compatible

session key encryption and decryption capabilities. For example, when you configure your Web server to require a session key with a minimum 40-bit (default) encryption strength, a user attempting to secure a connection must have a Web browser capable of processing information with a 40-bit session key.

Selectable Cryptographic Service Provider

Selectable Cryptographic Service Provider (CSP) allows you to select a Microsoft or third party cryptographic provider to handle cryptography and certificate management. Each cryptographic provider can create a public and private key to encrypt and decrypt data. The private key is stored at the server in the file system, on a PCI card, on a SmartCard, or in the registry, as it is for the two default providers that Microsoft installs: Microsoft DH SChannel Cryptographic Provider and Microsoft RSA SChannel Cryptographic Provider.

Visual KPI Specific Elements

Visual KPI has many security-enhanced features “baked in” to the software design.

Web Site Protection

- The web site uses IIS to require user authentication via local named user (Workgroup scenario) or Active Directory user (Domain scenario).
- The web site uses SSL to encrypt data on the wire and over the airwaves.
- The application server uses file security DACLs to limit access to individual web sites and web pages.

Meta Data Security

- All configuration data is stored in SQL Server 2005 or SQL Server 2005 Express.
- The application server is granted the minimum privileges required to read/write configuration data using secure stored procedures.
- The application server uses parameterized stored procedures to defend against SQL injection attacks.
- The application server connects to SQL Server using Windows integrated authentication, and no password is stored in a configuration file.
- The application server web service account does not need any database role other than db_VKPIrole, which is granted only the right to connect to the Visual KPI database and execute the Visual KPI stored procedures.
- At install time, the installer needs the db_sysadmin role, or must pre-create the VisualKPI database, and create a login for the Visual KPI server account.

Historian Security

- The Visual KPI application server connects to the Historian as a specific, named user. The Historian must only grant read permission to this login identity.
- Version 2.0 of Visual KPI does not write to the Historian.

Other data sources

- Encryption can be configured on the web services for use between the client browser and Visual KPI Server and between the application server and web service to the external data source.
- Encryption can be configured between the Visual KPI application server and SQL Server 2005.

Summary

Visual KPI is an enterprise-ready platform for managing and distributing KPIs, Scorecards and real-time Trends to users throughout an organization using only browser technology on the client device. Since the nature of KPIs often involves extremely sensitive corporate information, care should be exercised in distributing these KPIs, especially to wireless devices. This primer is meant to expose the reader to a few options available that implement the important task of *Preventing* unauthorized access. A complete security strategy needs to account for *Detection* and *Response* as well.

About Transpara

Transpara delivers business intelligence software that provides mobile professionals in the process and utility industries with real-time asset and operating data on any web browser, whether on hand-held devices or the desktop. Transpara's Visual KPI ensures that responsible parties throughout the organization and supply chain, from plant floor managers to executives, have real-time access to business-sensitive information, enabling stakeholders to create and distribute Key Performance indicators in order to monitor their entire asset base. With Transpara, customers reduce operating costs and lower business risk by promoting corporate transparency and ensuring compliance with regulatory requirements such as Six Sigma, Title V, and Sarbanes-Oxley.

Transpara *Real Time. Right Now.*

865 Piemonte Drive
Suite 100
Pleasanton CA 94566
Phone 925-218-6983
www.transpara.com