HRM Software White Paper

Employee Self Service
Addressing the new security challenge

HRM software

Introduction:

HR Self Service applications, by their very nature, are widely accessible. Employees need to be able to connect to these systems via web browsers at work, on the move, or even at home. The need to secure your network and host infrastructure is a given. But just as important is the application-level security that protects your HR Self Service system.

Research by Gartner found that 75% of malicious attacks happen at the application level. A report by IDC in July 2002 further identified security at the application layer as being the most vulnerable, noting that most efforts at protection are built instead around the network layer.

This paper highlights the importance of application security when deploying HR Self Service applications. It looks at the vulnerabilities associated with legacy client/server applications and their web "add-ons" and discusses how "web-native" applications - those built from the ground up for web deployment - can offer a most robust approach.

Employee Self Service
Addressing the new security challenge

Every month, it seems there's another story in the news about a company exposing their clients' information on the Internet. Credit card numbers, client address lists and even bank account details get into the wrong hands; resulting in embarrassing apologies from the companies concerned and hastily conducted 'security reviews'.

These incidents are serious, but imagine if the data being exposed was the contents of a company's HR system. Not only would employees' personal details be at risk, but also salary information, confidential appraisals, disciplinary and sickness records and other sensitive data. Security breaches involving human resource data can be more than embarrassing, they can lead to prosecution: the Data Protection Act, 1998 obliges data controllers (including responsible managers and staff) to implement security measures that are appropriate to the sensitivity of the data being stored and the harm that might result from disclosure. HR systems usually hold sensitive information, so their security must be taken seriously.

Legacy approaches

In the past, securing employee information may not have caused too much concern. HR applications were only available to a small audience of HR professionals and senior managers, and the data was kept within the reasonably secure confines of a company's internal network.

Executive Summary:

- Security is a key consideration when rolling out access to HR data across an enterprise
- Many "web add-on" modules for HR systems expose security vulnerabilities, due mainly to legacy design and the use of common scripting techniques
- In system design, application security cannot be treated as an afterthought - it must be built in from day one.

With employee and manager self-service, HR systems now enable employees throughout the organisation to access and/or maintain their own personal data, as well as data on their subordinates. The most cost-effective way of delivering this functionality is to use a web application, similar to those used for Internet shopping and banking, to give employees access to the HR system.

As the demand for self-service has grown, HR system vendors have responded by "web-enabling" their systems. In most cases, this has meant creating web "add-ons" for existing client/server systems. Unfortunately, the rush to market that has accompanied the development of many of these add-ons has meant that security has been hampered by inherent limitations of client/server systems that were designed for a different era.

Many web add-ons have been created using server-side scripting technologies, such as Active Server Pages, to create "virtual clients." A virtual client is an application that runs on a web server, acting in a similar way to a regular thick-client but converting the data returned by the HR system into web pages for transmission over an intranet or the Internet. These web add-ons either communicate directly to the HR database (often without any intermediate security) or they may work via an existing application server.

What's a web "add-on?"

- A web add-on is a module that "web-enables", or adds web functionality to, an existing client/server application.
- Typically, a web add-on web-enables some but not all of an application's functionality. System administrators (and sometimes also power users) still need to install and use the older "thick client" user interface.

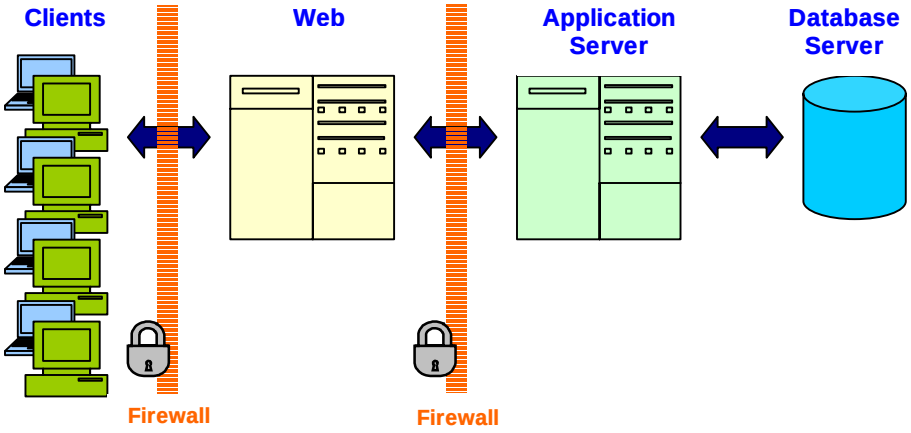
This approach can leave data at risk. In order to provide access to the full range of information required by different users, the web add-on itself needs wide-ranging permissions on the database or application server. This may involve storing the database user name and password in a file on the web server. Once a hacker or rogue employee has gained access to the web server, he or she may only be one step away from obtaining full access to the sensitive employee data stored in the HR database.

New challenges, new architecture

Designing applications for intranet or Internet deployment requires a completely different architectural framework from the more traditional 2-tier client/server applications, in which core applications and data are typically hosted on one server that is accessed by "thick" clients.

HRM Connect™ is a web-native HR system that has been built from the ground up for web deployment. It is designed around the N-tier (or multi-tier) architecture recommended for web applications. This architecture partitions application functionality into independent layers and

has a number of important advantages, one of which is to facilitate a much more robust approach to security than is possible with web add-ons.



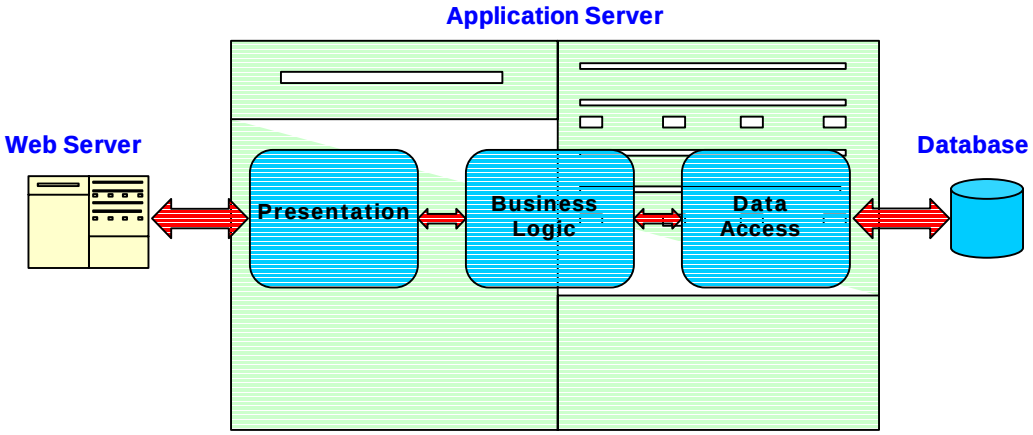
The diagram above shows a typical physical architecture for an HRM Connect installation, with security measures implemented to improve the protection for sensitive HR data. The configuration displayed shows two firewalls: one internet-facing firewall and one protecting the internal network from the web server.

In the HRM Connect N-tier environment the web server never talks directly to the database server. All communication is performed via the application server, which provides its own security checks before permitting client access to the data. The internal firewall can be configured to permit only the standard COM+ remote procedure calls used by the HRM Connect web server components to communicate with the application server, and prohibit any direct connections from the web server to the database.

Web add-ons, on the other hand, typically require the web server components to talk directly to the database. In this situation, an internal firewall would need to be configured to permit direct database connections, reducing the security of the database.

COM+ Security

HRM Connect is built on the Microsoft® COM+ platform and takes advantage of the security facilities of this platform. Application partitioning is used on the application server to increase security by separating the functional areas of the application and restricting the access between each section.



The diagram shows the partitioning of the HRM Connect application into three COM+ packages with responsibilities for the three key areas of the system. In the previous diagram we showed how security is enhanced by preventing the web server from talking directly to the database. This diagram shows that the web server can actually only talk to the presentation package within the application server and cannot directly access the business logic or data access packages. The presentation package can only access the business logic package and not talk directly to the data access package, and only the data access package is able to connect to the database server.

HRM Connect uses COM+ security to enforce these access restrictions within the application server. Typically, this is set up as follows:

- The presentation package runs as User A. User A has no permissions on the server except to request services from the business logic package.
- The business logic package runs as User B. User B is given greater permissions, For example, to read and write to the local hard drive. User B has rights to request services from the data access package.
- The data access package runs as User C. User C has access rights to the database using standard NT security and giving User C access rights to the database. Alternatively, SQL Server security can be used with the appropriate login information stored in a file on the application server. The login data can be secured using NT file security to prevent access other than by User C.

Each of the three COM+ packages is compiled code, and so considerably harder to hack than script-based web add-ons. Additionally, as each package runs with permissions restricted by the operating system, even if a hacker was able to run malicious code within one of the packages the COM+ security model would restrict what could be done on the server.

COM+

COM+ is a component software architecture built into Microsoft® Windows 2000. It provides a large set of services to applications, including robust security facilities.

User Session Identification

Unlike client/server applications, web browsers do not maintain a permanent connection between the browser client and the server. Each request for a page or an item on a page is made by the browser to the web server as a separate request and a new connection is made each time.

For web applications, this means that a mechanism is needed to identify each active user's session so that the correct pages and data are presented to them. This needs to be done in a secure manner to prevent hackers from hijacking the sessions of other logged-in users. The usual method of achieving this is to use a session identifier that is stored in a cookie (a small text file) on the client's PC and is automatically sent by the browser with each request made to the server.

Scripting languages such as ASP and PHP provide their own mechanisms for generating and managing these session identifiers. Typically these involve storing all of the currently in-use session IDs on the web server. Each client's session ID is also stored in a cookie on his or her PC.

Aside from the problems this creates with load balancing across multiple web servers, this approach has security implications. Storing the session IDs on the web server can leave them more vulnerable to attack. If a hacker gets hold of a user's session ID, he or she can send requests to the web server pretending to be that user and get access to any data that the user is permitted to see.

Rather than using the inbuilt session support of a web scripting language, HRM Connect creates its own session IDs, giving each active login a unique identifier which is generated each time a user logs in. These session IDs are stored in the main database rather than on the web server, and so are protected by the security described in previous sections. To ensure that users' requests are valid and consistent with their security permissions, HRM Connect checks the session ID on each request to the application. HRM Connect session IDs are configured to timeout after a specified period of inactivity – typically twenty minutes.

HRM Connect's use of its own proprietary session management provides another advantage. Standard server scripting session management is well known and widely used, which increases the likelihood of security flaws being found and exploited. As most security breaches arise from people using tools that exploit known weaknesses rather than developing their own, this increases the probability of successful attacks on applications that use standard server scripting management. Systems with their own session management, such as HRM Connect, are generally less vulnerable.

Data Access

This paper has demonstrated how the HRM Connect architecture helps protect sensitive HR data from outside attackers.

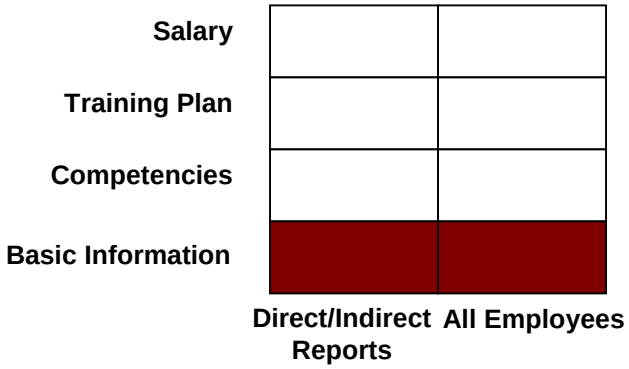
Just as significant is the need to provide employees and managers with appropriate access to data, without forcing compromises to security policies or creating administrative headaches.

When access to HR systems was restricted to the HR department, security models were relatively straightforward. With self-service the requirements for the security model become considerably more demanding. For example, an enterprise-wide HR system may need to support the following:

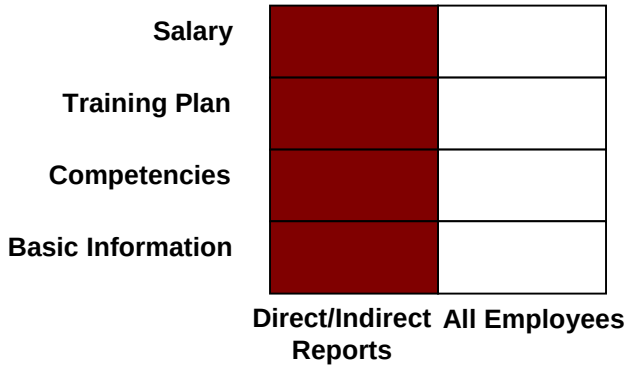
- A senior HR manager who can access salary data on all employees, except board-level directors.
- An HR administrator with responsibility for specific departments, who can only see sensitive personal data on staff in those departments.
- A manager who can access the salaries, performance and competency information of his subordinates, but no other employees.
- A project team leader who can view performance and competency information for members of her team, but who has no access to salary details.
- Regular employees who can update their own personal data, and can only view contact details of other members of the organisation.

Web add-on modules for existing legacy HR systems often inherit the security model of the original system, which is likely to have been designed for use only by the HR department and a few senior managers.

Problems occur where these systems are designed around simple, so-called “rectangular,” security models. For example: Consider the case of a manager, Mr Smith, who is permitted to view non-sensitive information on all employees in the company, plus salary, training and competency information for the employees who report to him. Under the rectangular security model, Mr Smith would be issued with one login that gives him access to non-sensitive data for all employees, but no sensitive data for the employees who report to him.



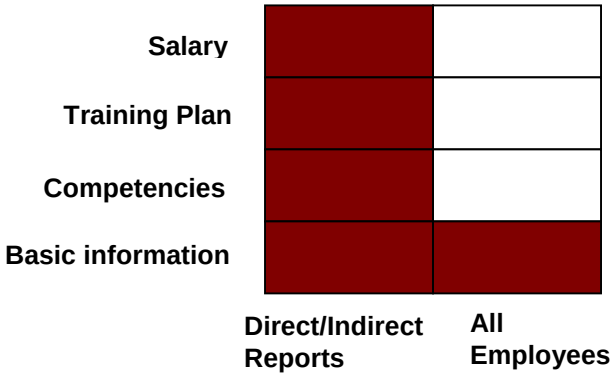
To access sensitive information about the people who report to him, Mr Smith would have to log out of the system and log in again using a different user name with different permissions.



This approach is tiresome for the users who have to remember multiple logins and keep logging in and out of the system when they want to view different data. It also creates an administrative headache for system administrators who have to create and manage numerous extra login accounts.

The security model in HRM Connect was designed to address these issues and support as widely as possible the variety of data access requirements in a typical enterprise. HRM Connect inherits no legacy security models and fully supports flexible non-rectangular security models, allowing users to be given access more precisely to the data they need with a single login.

Using the previous example, HRM Connect's security model would permit Mr Smith to access both basic information on all employees and sensitive information about his own reports through a single login.



Administration

When systems are to be rolled out across the enterprise to hundreds of even thousands of users, it is very important that the processes for creating and managing user accounts are streamlined.

To facilitate security administration, HRM Connect uses a roles-based security model, whereby the administrator defines security privileges according to user roles (and sub-roles) and then simply assigns users to those roles.

When a new employee is added to the HRM Connect database, an inactive login account is automatically created for that person. The administrator then only needs to activate the login and assign the appropriate role. This task can, if required, be included within an “add new employee” process flow definition within the system. HRM Connect also supports the creation of external users (i.e. users who do not have an employee record in the database), for example to give limited access to HRM Connect to supplier organisations, such as training providers and recruitment consultants.

As well as supporting its own user accounts, HRM Connect security can also be integrated with other systems to reduce duplication of effort in creating user logins and to make use of ‘single sign-on’ systems. HRM Connect supports integrated Windows NT security as standard. Interfaces for other single sign-on systems can be created as required.

Auditing & Workflow

For enterprise-wide HR systems to deliver service improvements and cost reductions, self-service users need to be involved in the processes for updating data. Yet, as every HR and IT manager knows, devolving responsibility for data entry can jeopardise data quality and consistency.

HRM Connect's inbuilt workflow system can be configured to automatically route data changes through predefined approval processes ensuring that changes are reviewed and approved before they are committed to the database. This allows responsibility for data updates to be devolved without losing control over data quality.

Auditing is another important facility for an HR system. Changes need to be traceable to the user who made them, so that in the event of a security breach, the activities of a rogue user can be tracked to help restore data to its original state. To this end, HRM Connect can be configured to provide a comprehensive audit trail.

All data that is inserted, updated or deleted through the HRM Connect application server can be tracked. Auditing can be defined on a per-table level. All data changes on audited tables are recorded in an equivalent mirror audit table, along with the time, user name, client IP address and action type. For additional security, audit tables can be stored in a separate database, or even on a different server if required.

Conclusion

The increasing popularity of HR Self Service – where companies provide their employees and suppliers with access to their HR systems through a web browser – is creating new security challenges for system designers and administrators.

Where once HR information was only available to a select audience of HR professionals and delivered across a more or less secure internal network, now hundreds or even thousands of employees, business partners and suppliers are being given access - across intranets, extranets and even the Internet - to systems that contain sensitive data.

Robust, easily manageable security is essential for HR Self Service applications if data is to be kept confidential. In system design, security cannot be treated as an afterthought – to work and perform effectively, it has to be built in to the application from the very start.

References:
http://www.dataprotection.gov.uk/dpr/dpdoc.nsf

About HRM Software Limited

Founded in 1986, HRM Software develops, markets and supports systems for HR planning, HR administration and organisation charting. HRM services customers worldwide through a growing network of distributors.

Our ambition is to continue to provide technically innovative software that meets the needs of organisations, large and small, to better attract, manage, motivate and develop the potential of their most important assets – their people. And, as our ISO9001 certification demonstrates, we're committed to excellence, in system design, implementation, support and services.

The Optimise Group
15 Melrose Street
Sandringham Vic 3191
Australia
Tel: +61 (0)3 9597 0166
Fax: +61 (0)3 9598 0949
E-mail: info@optimise.com.au
www.optimise.com.au