SAFECommerce: Ensuring Online Authenticity of Transactions

Luce Chandon
E-Commerce Analyst
Com Tech Communications
lchandon@comtech.com.au

Chris Martin
Strategic Consultant
Com Tech Communications
cmartin@comtech.com.au

Abstract

eCommerce heralds a revolution in which businesses interact, collaborate and communicate electronically. Typically, this is based on the Internet; a global public network in which chaos seems to reign supreme.

Companies at the forefront of the eCommerce revolution are developing business strategies that incorporate advanced technologies to redefine industries to their advantage. Many of the fastest growing companies operate solely as an eBusiness. Many global enterprises are now recognising that the development of a sound eCommerce strategy is not just a prerequisite to remaining competitive – it is paramount to survival. As a result, every company is faced with the question of how to rapidly grow and extend their eBusiness, at the same time ensuring that all interactions are authenticated and can be audited.

Dealing with this transformation, or making use of the revolution to one's competitive advantage, requires transcending the technology landscape. SAFECommerce involves underpinning an eBusiness with a set of services that allow for a secure foundation to be built upon. It is essential that the development of an eBusiness incorporates services that track its complete lifecycle from developing an eBusiness concept through to implementing a solution and finally to transforming it as the marketplace demands.

1. Introduction

eCommerce heralds a revolution in which businesses interact, collaborate and communicate electronically. Typically, this is based on the Internet; a global public network in which chaos seems to reign supreme.

Companies at the forefront of the eCommerce revolution are developing business strategies that incorporate advanced technologies to redefine industries to their advantage. Many of the fastest growing companies operate solely as an eBusiness. Many global enterprises are now recognising that the development of a sound eCommerce strategy is not just a prerequisite to remaining competitive – it is paramount to survival. As a result, every company is faced with the question of how to rapidly grow and extend their eBusiness, at the same time ensuring that all interactions are authenticated and can be audited.

Dealing with this transformation, or making use of the revolution to one's competitive advantage, requires transcending the technology landscape. SAFECommerce involves underpinning an eBusiness with a set of services that allow for a secure foundation to be built upon. It is essential that the development of an eBusiness incorporates services that track its complete lifecycle from developing an eBusiness concept through to implementing a solution and finally to transforming it as the marketplace demands.

This paper discusses an approach to the implementation of a secure eCommerce solution. In Section 2, we cover some background information to business processes and the reasons why organisations arise. We view these from a transaction cost perspective and attempt to convey the forces at work that are reshaping our idea of organisations. We introduce the concept of the Network Economy that has become a de-facto model for operating in the digital age.

In Section 3, we propose a practical methodology for designing solutions that effectively deal with the requirements of a Network Economy. We discuss the importance of an integrated view of a solution that commences with business drivers.

In Section 4, we develop an Internet-based technology infrastructure that supports the requirements for authentication and security of an organisation's valued information.

In the context of this paper, two definitions need to be considered. Namely that:

- **eCommerce** is the use of technology to create a positive impact on an organisation's revenue generating activities; and that
- **Security** refers to the implementation of processes, practices and technology to achieve desired results along with a high level of predictability.

2. Why Organisations Exist

Ronald Coase, a student of industrial management at the London School of Economics, wanted to show that the state could be a more efficient manager of the economy than the free market. In order to do this, he travelled to the US to study the closest thing he could find to a nonmarket economy – the growing American phenomenon of the Organisation – typified by companies like Standard Oil, General Motors and US Steel. Inside these organisations, the full range of market functions – purchasing, marketing, sales, manufacturing, distribution – were performed internally. Travelling around the country, Coase became aware of the failure of economists of the day, to answer a few basic questions:

- Why did organisations form at all?
- Why were they the size they were and not larger or smaller?
- How did entrepreneurs decide which functions to bring inside and which to leave to the open market?

He made a significant discovery, and in 1937 published an article entitled "The Nature of the Firm". Coase's discovery was centred on the notion of transaction costs. Transaction costs relate to a set of inefficiencies in the market that add, or should be added, to the price of a good or service. He discovered six basic types of transaction costs:

1. **Search costs**: buyers and sellers finding each other inside the increasingly broad and disorganised marketplace.
2. **Information costs**: for buyers learning about the products and services of a seller and the basis for their costs. Similarly, it includes the cost associated with a seller understanding the need of the buyer.
3. **Bargaining costs**: buyers and sellers setting the terms of a sale or contract for goods and services.
4. **Decision costs**: for buyers evaluating the terms of a seller against other sellers. Similarly, decision costs are incurred by sellers to evaluate whether to sell a product or service to one buyer versus another (or not at all).
5. **Policing costs**: buyers and sellers taking steps to ensure that the goods and services and the terms under which the trade was made, do in fact translate into real goods and services.
6. **Enforcement costs**: buyers and sellers ensuring that unsatisfied products and services are corrected.

Coase concluded, by examination of the basic transaction cost types, that organisations arise because the additional cost of organising and maintaining them is cheaper than the transaction costs involved when individuals conduct business with each other via the marketplace. Coase also found that an organisation will continue to expand to the point where the cost of carrying out the transaction internally equals the cost of performing the transaction on the open market.

The Changing Environment

The advent of technology has had a tremendous effect on the appearance of the organisation. In particular, new technology is reducing transaction costs. These cost reductions are, in many cases, significant. Equally, they are allowing functions to be performed much more quickly in the marketplace than they are for firms.

If organisations, as Coase discovered, increase in size until they reach the point where the next transaction would be just as cheap if done outside, what would be the likely outcome when the outside world gets cheaper?

The natural effect is that the organisation shrinks as many of the activities are “contracted” out to the market.

A number of examples exist whereby organisations have shrunk as a result of the decreased transactions costs largely attributed to the deployment of advanced technology. None is more apparent than our financial institutions that, until recently, had a monopoly on certain financial activities. Now, with a deregulation of the financial industry, anybody can potentially become a financial institution and they can do so at an extremely low cost through the use of ATMs and the Internet. For the existing banks, branches have become an expensive overhead.

The diagram below illustrates the average cost of performing a transaction in retail banking for the different delivery vehicles. It can be seen an increased reliance on technology, results in a significantly reduced cost.

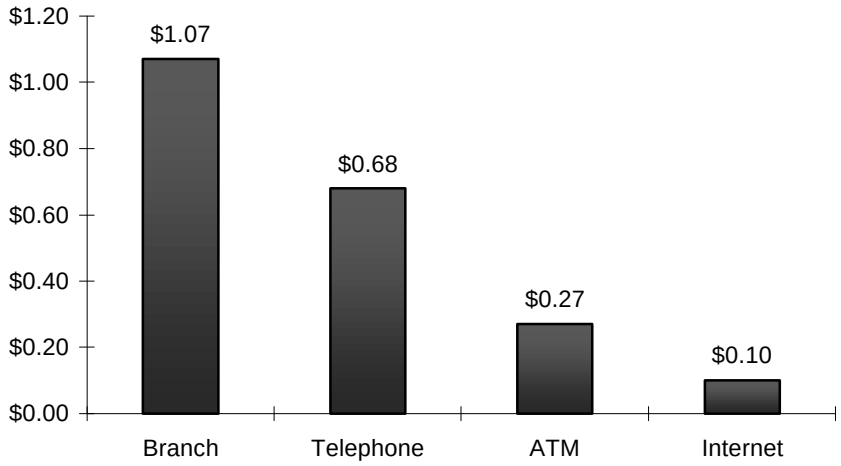

Figure 1: Average Cost per Transaction in Retail Banking

The Network Economy

The contracting out of activities by an organisations to many others creates a dependency framework whereby the activities of one organisation becomes dependent on others which in turn are dependent on others still.

The Network Economy is characterised by the fact that multiple organisations maintain transactional relationships in order to produce one or more good or service. It gets its name from the diagrammatic similarity to the telecommunications networks we are now familiar with.

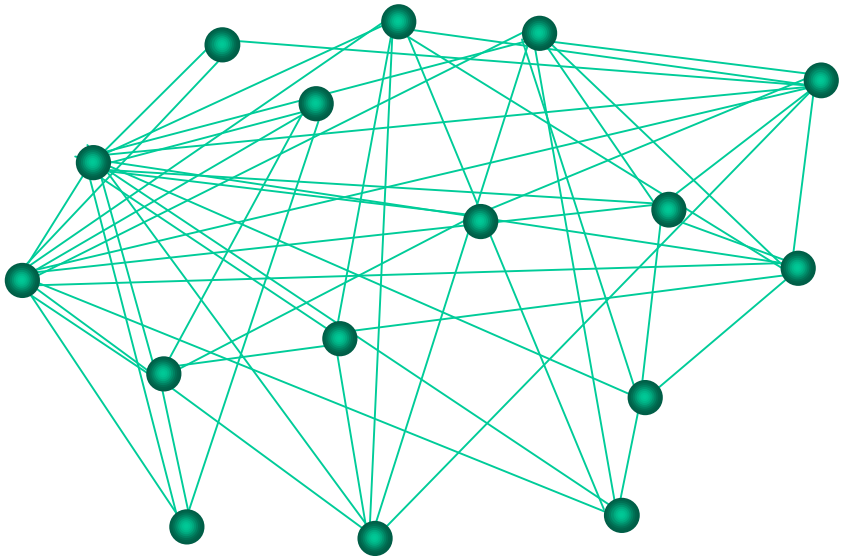

Figure 2: Graphical Representation of the Network Economy

It can be seen that within a Network Economy, any two organisations may directly engage in a transaction. The notion of a mediator or an organisation that facilitates transactions between two or more organisations has disappeared – largely because, as Coase suggested, the cost of performing the transaction would not be less. Similarly, because the organisations themselves are tightly coupled with an increasing dependency on other organisations for success, the notion of stakeholders within an organisation must be extended to include all entities that are part of the supply chain.

Challenges Faced by Organisations

This current model presents many challenges previously not experienced by leaders in determining a role for their organisation's future. The pervasiveness of technology as an enabler to organisational process improvement has added another dimension of complexity to effective planning. Leaders must now ensure their decisions are balanced across both technological as well as business factors. The decisions range from changing organisational models, collaboration amongst supply chain members, return on investment and penetration into a global market through to technology decisions such as technology purchasing. They must be balanced with the varying (and sometimes competing) standards to ensure that interoperability is maximised and ensuring that whatever technology decisions are made can be effectively deployed in an Internet environment.

Furthermore, leaders must be mindful of the need to decrease the time to market for products, decreasing financial settlement windows as well as increasing opportunities to extend into new markets and services, along with the competitive forces that come into play with increasing competition.

Accuracy in forecasting, based on extrapolation of past trends, is giving way to the installation of flexibility as a core competences in many disciplines. Securing a role in eCommerce involves carefully balancing the opportunities that exist with the need to react extremely quickly as markets are reshaped. Arriving at such a position involves a well-defined approach to planning; one that is driven by the business and elicits the needs of an increasing number of diverse stakeholders.

The outcome of planning in such an environment, from a technological perspective at least, is a secure framework that is sufficiently extensible to be able to support the increasingly diverse range of solutions required to enhance an organisation’s competitiveness in the Network Economy.

3. Secure Application Framework Enablement

Analysis of Internet-enabled applications has highlighted six highly integrated components. These include:

- **Content Services**; the traditional basis for propagation of information. Regardless of the function of an application, it must provide some information to the user.
- **Data Services**; the collection of data from a variety of sources enables the application to analyse and perform some action – which, at some later time, gets converted into content for presentation to a user.
- **Network services**; Internet-based applications are increasingly distributed – i.e. operate across networks. The application needs to be aware of the services available to it to ensure it can be effectively deployed across a range of networks.
- **Security services**; the Internet is a public network which means that without the necessary protection, an organisation's valuable informational assets may be compromised. Data protection and user authentication, are rapidly becoming essential to any business-related application deployed across the Internet.
- **Host integration**; much of an organisation's intellectual assets already exists within existing systems located in the "glass house". An Internet-based application must leverage these assets by integrating to the very systems that house this information.
- **User services**; in the Network Economy, the effectiveness of a relationship is determined by the ease with which two parties can communicate. An Internet-enabled application should be intimately aware of the user using it and be capable of presenting data and information to suit.

Each of these services must be brought together in an integrated way, which allows for the changes in one, to be appropriately reflected in the behaviour of others. For example, if a user is reliably authenticated as being an internal staff member, then the User Services and Content Services ensures that information (determined by the Data Services) is presented to them in a format that would be most valuable to them. The application can be extended to support an external organisation, with no modification, so that based on authentication of the external user; the information will be presented differently according to an organisation's policies.

Similarly, as new applications are deployed within the framework, the same interaction amongst services holds and the different users receive their own specific functionality and interpretation on data. In this way, organisations are able to increase their application return on investment.

The deployment of a Secure Application Framework does not come without some focused planning however. Six lifecycle services have been identified that optimise the effectiveness of new Internet-enabled applications.

- **Business Exploration**; as the Network Economy demands new ways of conducting business, it also presents new opportunities. Business exploration should provide a formal method for identifying these opportunities based on an organisation's existing core competences.
- **Concept Formation**; the identification of an opportunity requires detailed analysis from a variety of "perspectives" to ensure that a solution is appropriately architected. These perspectives range from identifying business and user

requirements through to decisions on technology selection and the impact on resources during implementation.

- **Specification**; the decision to implement an Internet-enabled application follows with a detailed analysis of all integrated components, as identified above, and the behaviour expected from the interaction between two or more services.
- **Construction**; the actual development of an Internet-enabled application and ensuring it follows well-defined methodologies and adheres to the quality constraints required.
- **Deployment**; the implementation of an application in a timely and cost-effective manner and with minimal impact on existing systems and infrastructure.
- **Ongoing Management and Support**; it has been shown that unlike previous generations of applications, Internet-enabled applications must be tightly managed to ensure continuance. This is especially true in the area of security.

4. Deploying Secure Architectures

The effective deployment of an Internet-enabled application for the Network Economy, requires a high level of technical knowledge as well as vigilance. Most organisations planning a modest Internet architecture will find that a well-maintained firewall, combined with a comprehensive security policy offers an appropriate level of protection. This is of course assuming that regular review and auditing of a firewall's logs is carried out.

Organisations planing a more ambitious Internet presence, providing Extranet applications linked to core applications & systems, will also need to pay attention to application level security, authentication and access control.

Standard Firewall Configuration

The first stage of an organisation's Internet presence is usually to display some informational pages on the World Wide Web (brochure ware). Generally, the organisation has identified that it must have an online presence, and commits to one – albeit with minimal functionality.

The following diagram illustrates common firewall architecture, typically used by organisations that provide such a simple set of Internet services. The primary goal of the design is to prevent anyone from the Internet from accessing any of the systems on the corporate network behind the firewall.

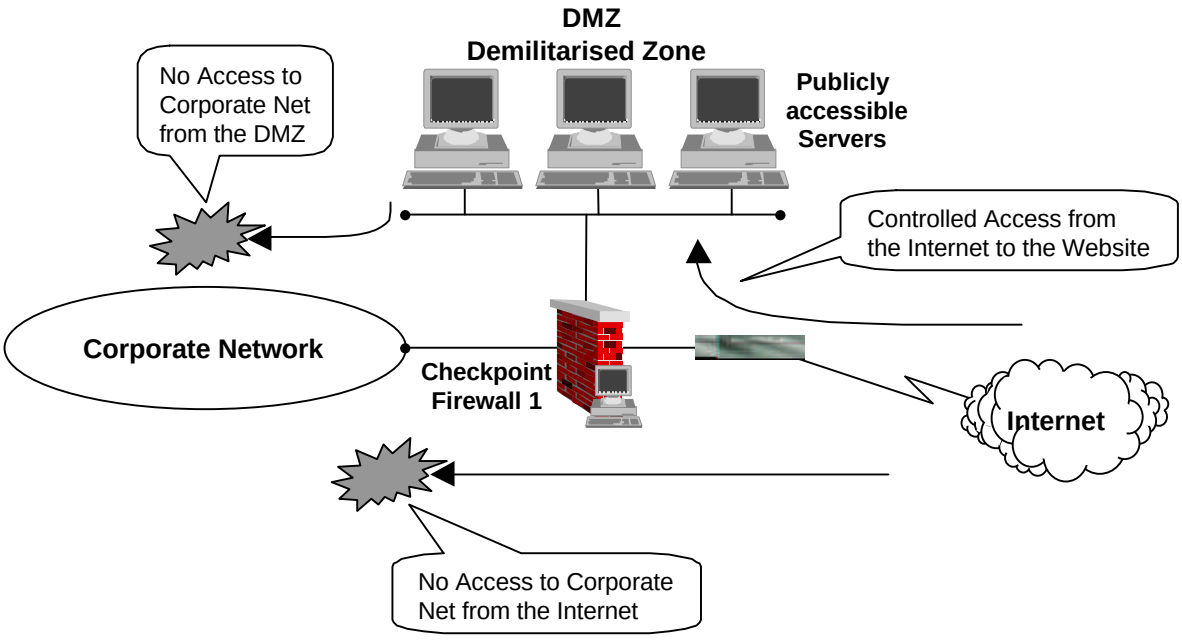

Figure 3: A typical firewall configuration

A separate network, referred to as a DMZ (Demilitarised Zone), is created to house all of the systems to be made available to the Internet. The firewall isolates the DMZ and the Internet from the corporate network.

Access to the DMZ is controlled by the security policy implemented on the firewall. This would allow Internet users access to only the servers on the DMZ, and using only the protocols that these systems are configured to accept. HTTP access is granted to the web

server only, and FTP access is granted to the FTP server only. These restrictions minimise the options available to an intruder attempting to enter the system, while allowing the intended services to be readily accessed.

While every effort is made to protect the services on the DMZ, it is important to realise that these services are publicly available and may possibly be compromised. The software used to implement the services is complex and, inevitably, due to miss-configuration or bugs that may be leveraged to gain unauthorised access. This makes it virtually impossible to secure any publicly accessible service, and as such the services on the DMZ cannot be trusted. The security policy implemented on the firewall must prevent any access from the DMZ to the corporate network.

Integration with Corporate Database Resources

After some familiarity with the Internet, the organisation identifies an opportunity to enhance its Internet offerings by allowing users to access sensitive and confidential information located on internal systems and databases inside their corporate networks. They usually design an infrastructure as per the following diagram:

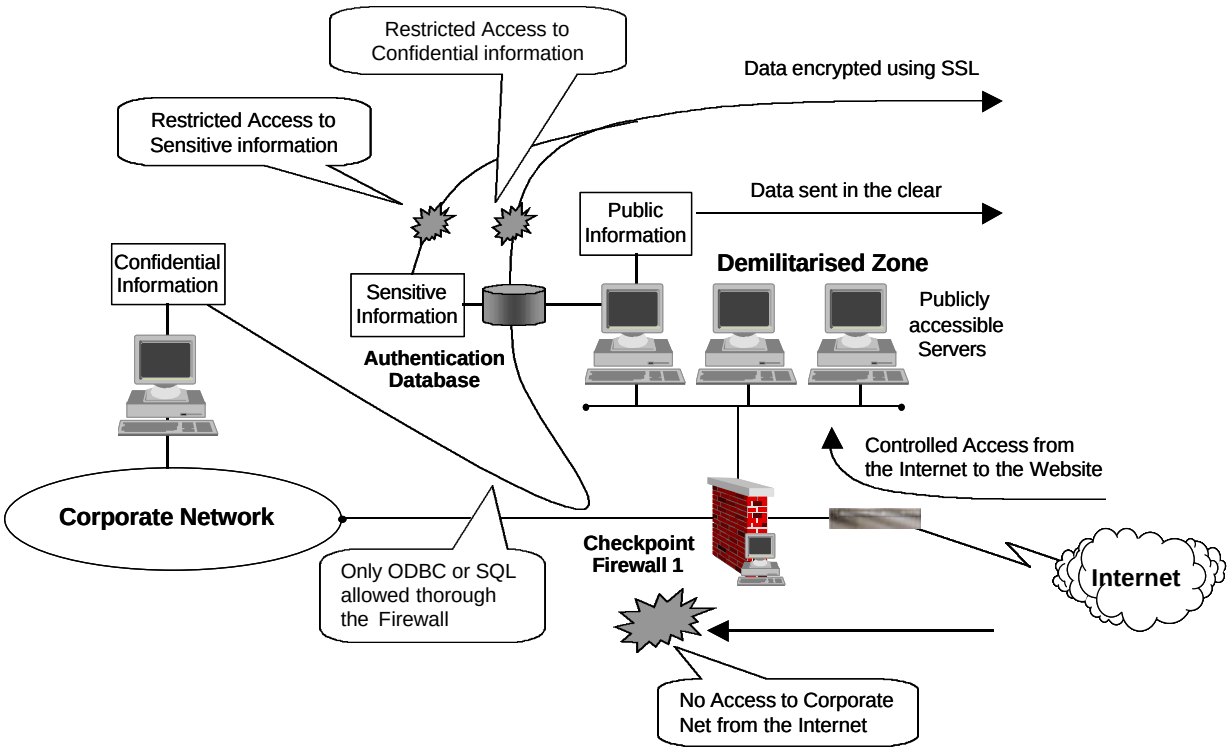

Figure 4: Commonly deployed solution, allowing access to corporate databases

The architecture attempts to protect information and services on the corporate network by allowing controlled access for SQL or ODBC protocols from the website through the firewall to applications running on the corporate network behind the firewall.

Upon further analysis however, we notice that it makes several security compromises. In particular there are two issues that are highlighted:

1. The Access Control Database (userid's & passwords) is stored on the web server allowing the possible exposure of this information, should the server ever be compromised.

2. The nature of confidential information stored on backend databases behind the firewall is such that it is not feasible to implement user level access control in the database (particularly if there is a large number of users accessing the site). This usually means that the SQL application running on the web server, accessing the SQL database will need to be aware of the administrator user id and password. Thus exists the possibility of exposing this information if the web site is compromised and allowing the intruder complete access to the database on the corporate network.

Secure Architecture utilising Messaging

It is possible to design an Internet-based application that is not susceptible to the weakness of the architectures described above. In order to achieve this it is necessary to separate any application logic, including connectivity to core systems and application, from the website.

A messaging system, is used to isolate the web server from the application logic on the corporate network. This is implemented on a dedicated Application Server, which performs many of the functions that have traditionally been found in middleware systems. In the end, the aim is to get the access control database and the application logic off the web server where it is open to possible compromise.

An example of this architecture is shown below:

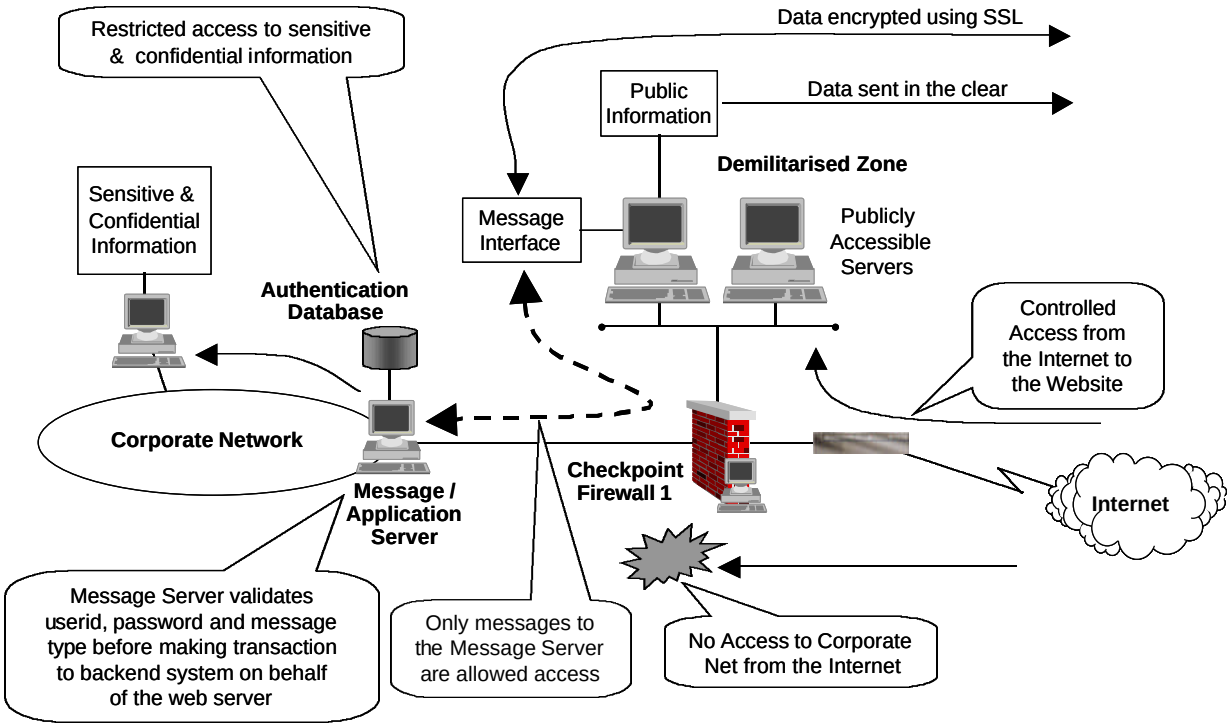

Figure 5: Secure architecture utilising messaging

The use of an application server in a web-based architecture has several other advantages.

1. It allows the business logic of the application to be centralised on the application server.
2. Because the business logic is activated by real-time messages sent from the web server, it can also be activated by any other system in the corporate network, allowing the same business logic to be shared across multiple applications.

The application servers will usually incorporate, a front end transaction server, allowing a single message to extract information from multiple systems and present the results as a single transaction response to the web server. An example of this environment would be a bank customer querying their account status, where customer account information is stored on separate systems for each account held. The cheque account is stored on a mainframe, their credit card details on a Unix host and the home loan information is maintained in a SQL database running on an NT system. The application/transaction server queries each system, and the results are summarised and returned to the application.

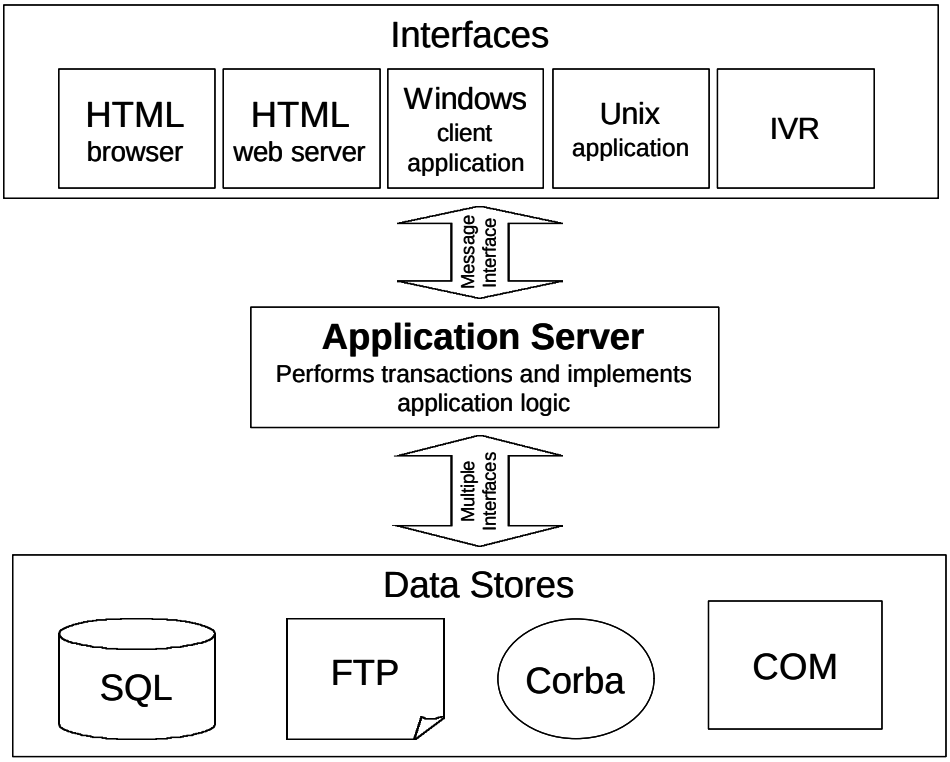

Figure 6: Leveraging the application server

The messages sent to and received from the application server are generally small. This means that they can be effectively passed over a slow Internet link, allowing the primary web server to be hosted at a remote location such as an ISP, without compromising the security of the organisation's data and still ensuring an appropriate response time.

In order to ensure the security of the application server, the messages sent to it should be simple and should only contain the minimum information required to facilitate the transaction. In order to identify the type of transaction requested, the message should contain an identifier which indicates to the application server the application logic required to perform the request, along with any input data required. The message may be as simple as Name/Value pairs sent in ASCII text and could look like the following

Messageid=101
Function=lookup
UserId=Smith
Passwd=XXXX
<eom>

The application server will recognise that "messageid=101" requires an SQL query on database and will run the appropriate query to extract the required data from their account. Before running the query it will check the userid & password in the authentication system to ensure that they are correct, and that the user has the required permission to run the query. If all is correct then the query is run. Note: that the user is not asked to supply an account number. The application server will extract the account number from the authentication/membership system. This means the user is only able to run queries against their own accounts, and cannot nominate another customers account.

In the event that the web server is compromised, there is no sensitive personal or confidential information located on the web server that can be exploited by the intruder. In the worst case they may discover the format of the messaging protocol used to communicate with the application server. Should this occur the intruder may be able to send messages to the application server, however the format of the message is defined, and they must know a customers valid userid & password to run the query. Therefore, no benefit is gained by breaking in to the site. (Although denial of service & malicious modification to the site are still risks).

The messages used to communicate with the application server are simple and do not provide any mechanism to run custom scripts that a web server would normally provide, and they also do not have the same administration & security configuration required for a web server. This means that the opportunity of exploiting a security or administrative error in the application server is significantly smaller than that of a web server.

5. Conclusion

Companies at the forefront of the eCommerce revolution are developing business strategies that incorporate advanced technologies to redefine industries to their advantage. Many of the fastest growing companies operate solely as an eBusiness. Many global enterprises are now recognising that the development of a sound eCommerce strategy is not just a prerequisite to remaining competitive – it is paramount to survival. As a result, every company is faced with the question of how to rapidly grow and extend their eBusiness, at the same time ensuring that all interactions are authenticated and can be audited.

We highlighted that dealing with this transformation, or making use of the revolution to one's competitive advantage, requires transcending the technology landscape. We developed a method of viewing Internet-enabled applications from the perspective of the services that the application offered and that six main services were essential to any successful Internet-enabled application. We also examined the premise that Internet-enabled applications must be underpinned by a formal examination using a set of six lifecycle services, which we call SAFECommerce. This allows for a secure foundation to be established and built upon.

We also examined architectures with an analysis of several methods for establishing an Internet presence. Each offers a solution to the problems uncovered by the analysis of a hypothetical organisation's attempting to become an eBusiness, with particular emphasis on the security implications of the different approaches.

It can be seen that the technology options for deploying applications in the Network Economy are as numerous as the business opportunities that exist. Effective planning for the Network Economy, requires an alternative perspective; a perspective that is formal and structured yet provides the necessary flexibility demanded by the organisation.