INFORMATION SECURITY STANDARDS FOR E-BUSINESSES

[1]Muhammad M. Satti

[2] Brian J. Garner

[3] Mahmood H. Nagrial

[1]Macqaurie Corporate Telecommunications Pty, Sydney 2000 NSW Australia, msatti@macquarie.net.au
[2]School of Computing and Mathematics Deakin University Geelong Vic. 3217 Australia, brian@deakin.edu.au
[3]School of Electrical, University of Western Sydney Nepean 2747 NSW Australia, m.nagrial@uws.edu.au

ABSTRACT

The process of buying, selling or interacting with customers via Internet, Tele-sale, Smart card or other computer network is referred to as Electronics Commerce. Whereas online trade has been touting its flexibility, convenience and cost savings, the newest entrant is wireless e-commerce. This form of business offers many attractions; including 24 hours seven days' open shop–business, vastly reduced fixed cost, and increased profitability. Amazon.com is an example of a successful venture, in e-business. Internet Service providers (ISP/ASP) have a significant influence on the feasibility, security and cost competitiveness of an e-business venture. In the ISP model of services, multiple users and their databases are normally offered on a single hardware, platform sharing the same IP address and Domain name. Clients will require a mechanism, which allows them to update their Web contents and databases frequently even many times daily without intervention of local system Administrator (ISP Admin). The paper overviews few steps to enable corporate clients to update their web content more securely.

Keywords-E-Commerce, E-business, Information Security, ISP/ASP, Satti, Nagrial, Garner,

I. INTRODUCTION

With the technological development, Electronic Commerce (E-Commerce) is becoming an important milestone in Information Technology (IT) revolution. The technologies that make the World Wide Web and e-commerce possible have some potentially negative components. To make e-commerce more cost effective by using e-cradle from Internet Service Providers and Applications Service Providers (ISP's/ASPs) , there has to be a security trade-off as defined above, that single hardware hosts multiple sites. The privacy issues are also of major concern for many users. There are means to collect consumer information easily with digital tools but the security is equally important in a digital transaction. It is revealed that companies conducting either business to business (B2B) or business to customer (B2C) e-commerce experience significantly higher rates of many such security breaches, incidents are recorded in ISP shared services, where multiple businesses are running by single hardware. Further, ISP's are not aware of most security tools and standard [1]. E-Commerce is fundamentally World Wide Web based buying and selling of goods and services. Most people see it as the ultimate form of removing the Intermediary or go-between. Most E- Commerce services are delivered by ISP's. The Internet service provider has a significant influence on the feasibility and cost competitiveness of an e-business venture. Large ISP's that provide business services claim to be security conscious, but in reality it may not be true. The Co-location hosting, in the ISP's environment, allowed users to come in unencrypted. An ordinary hacker is easily able to hijack the connection.

***Knowledge is power*:** It is the hacker's creed. If a company stores any valuable information on web server and those servers are housed at an ISP's data center, one should pay close attention to the ISP's security policy. Even if the information on a web server is of little value, the customer should worry about a deliberate denial of service (DoS) by hacker's [2].

II. COMMON ISSUES

A growing number of companies are placing some or all of their E-Commerce support needs into the hands of corporate service providers (ISP / ASP) or one-stop, no-hassled web hosting, dedicated hosting or share hosting services centers. The server farms that sit inside the walls of web hosting services are among the most tempting targets for nosy hackers, who might tap away until they find a crack, most commonly a mis-configured firewalls or routers [3]. The most vulnerable arrangement is a server farm in which servers are shared by a number of companies, and each have their own File Transfer Protocol (FTP) account on the same server to update the web contents and database. FTP was written as a quick tool to

transfer files across a small network and security was not of that much importance at that time. The way most ISP's become economical by installing a quad processor with giga-byte of RAM and allocating multiple customers on it. When a hacker breaks into one machine, he will breach the security of all those customers. The ISP's business is based on generally cheaper, switching infrastructure. The switches which offers filtering (layer 3, 4 and layer 7), strict access controls between machines and connections are better and more secure, but at a cost of US$20,000 to US$30,000 compared to normal non-filtering switches at about $1,000. Most ISP's have firewalls but nothing else. Firewalls are further categorized using the IT Security Evaluation Criteria (ITSEC) leading to an **'E"** level of assurance. The ITSEC rates the correctness, effectiveness and strength as meeting the stated requirement for a level between E0 and E6. Level E0 represents an inadequate level of assurance, while E6 products are the most trusted [4]. The information security laws are enforced in some countries including Australia. These laws imposed restrictions on all third party service providers to use at least E1 grade firewall for general trading and E3 level for government web and data hosting, whereas for credit card information and financial transaction, payment gateways must have E6 level firewall to protect security domain. ISP's are vague about attacks they have experienced. In spite of this false sense of security, ISP's customers do worry about more visible problems, such as malicious destruction of web pages or even web page content being replaced with sexual, racist, or otherwise unpalatable content. Regrettably, the triumph of the Internet design for global information access and sharing is at risk of being tarnished as a ubiquitous open trading environment by unscrupulous and vindictive attack [5]. Information security is thus the overarching concern of Internet businesses and users!

Due to poor infrastructure design and hidden security holes, over the last two years hundreds of web pages were changed; several of which resulted in embarrassing press reports. These stories led the Ebusinesses to earn a bad reputation and customers hesitating to buy commodities by credit card. Most of them thought that their credit credentials were not in safe hands, which put the E-Commerce business into decline. Internet security was one of the major factors of E-Commerce failure in the USA and across the globe. In the year 2000, hundreds of IT related companies have closing and e-economy slumped to its lowest rate ever, since its inception. The proposed work is *"Secure data Center"* to host web sites of delivering e-commerce trading, which is most cost effective and more secure. This model will address the ISP's snags, system weaknesses and fulfill the e-business needs. The biggest challenge is in the fundamental transformation of the way things get done in the world. That's because networks are great levelers. They dissolve barriers to entry and neutralize traditional assets like physical stores and branches. Networks dissolve the boundaries within and between companies, countries, continents and time zones. It's not hyperbole to say that the "Data Center" is quickly emerging as the largest, most dynamic, restless, and sleepless marketplace of goods, services and ideas the world has ever seen.

III. SYSTEM ARCHITECTURE

The model data center is unique in design; where remote access, security, intruder detection system and other state-of-the-art equipment is in place.

E-Clients

In the Internet, data center reference architecture, the clients issue requests to a service name, which represents the application being delivered to the client. The end-user system and the client software have no knowledge about the inner working of the system that delivers the service. The end user typically types in the URL, for example, http://www.itbutler.com.au, and then either clicks on hyperlinks or completes forms on Web pages to navigate deeper into the site.

Gateway Routers

Gateway routers connect the infrastructure to the data center (ISP) networks. For high-end Ebusiness environments, full redundancy is considered in the proposed model. The full redundancy requires at least two Gateway routers, with each router connected to a different back end carrier provider commonly called Back End Service Provider (BSP). This implementation provides fault tolerance and traffic-aggregation.

The routers should run Border Gateway Protocol (BGP) to ensure proper and fast routing. Most routers are capable of enforcing traffic policies, which should be used to create a security perimeter network (also known as, for demilitarized zone (DMZ, and Inside 100% screened sub-net) and additional levels of security for the internal network.

Load Balancing

Network Load Balancing can be successfully used to load balance front-end web-tier systems and is used in the Internet data center reference architecture to provide both resilience and scalability in conjunction with Round Robin DNS (RRDNS). It is strongly recommended to have three DNS, (Primary, Secondary and External Secondary), where the external secondary must be placed at a different location.

Services Systems

Services systems are the collection of servers that provide the core Web services, Database services and E-Commerce solutions such as HTTP/HTTPS, LDAP, RADIUS and Secure Copy Protocol SCP to Web clients/systems. Developers usually group these services systems into sets of identical systems called clones. The clones run the same software and have access to the same Web content, HTML files, ASPs, Java scripts, Cold Fusion and other middleware and so forth, either through content replication or from a readily available file share [6]. By load balancing the requests across a set of clones and by detecting and separating a failed clone from the other working clones, you can achieve high degrees of scalability and availability.
For E-Business, both scalability and availability is a critical success factor (CSF) to consider in architecture design.

Intelligent Switches

The design can be implemented with multiple physical devices or only two large multi-layer switches. The reference architecture configuration uses two large, multi-layer switches to maintain simplicity, manageability, and low cost. The switches are partitioned as multiple logical Layer 3 devices. The Virtual Local Area Networks (VLANs) are created and spanned over both switches to provide hardware fault tolerance. This has extended capability to isolate corporate customers from each other on the same switch but with explicit ACL to each VLAN. This also minimizes the eavesdropping across the neighboring VLAN customer. The servers are configured with two-teamed network adapters and connected to the same VLAN on each physical switch. The traffic between VLANs is routed using the internal router and controlled using access-control lists ACLs[7].

Firewalls

A firewall is a mechanism for controlling the flow of data between two parts of a network that are at different levels of trust. The firewall inspects traffic between the front-end (Web tier) system and middle and back-end systems. Different firewall policies are implemented to control traffic between the tiers. The firewall often becomes a single point of failure and a traffic bottleneck. To avoid these limitations, the reference architecture implements two fast, reliable firewalls in a fail-over configuration. The last rule-set is always set *DENY ALL* if not permitted. For E-Commerce cradle, generally E3 and higher grade of firewall are recommend, however, for general Web hosting E1 to E3 firewalls can be used [4].

Middle-Tier Systems

This tier is used to host domain controllers running the Windows 2000 operating system with Windows 2000 Active Directory™ service and Domain Name Service (DNS). Depending on the application design, the middle tier can also be used to host servers running components and business objects (for example, Microsoft BizTalk™ Server 2000 or Message Queuing). If the application is designed to support three tiers, the middle tier can host application logic and services. Most applications are designed logically as three-tier systems, but they can also perform if they are installed on two physical tiers. In this case, the middle tier can be collapsed to a back-end tier and the business objects run on the front-end systems.

Back End Systems

Back-end systems are the data stores that maintain the application data or enable connectivity to other systems, which maintain data resources. Data could be stored in flat files or in database systems such as Microsoft SQL Server™ 2000, Oracle, DB2 and MYSQL back-end systems. The database systems are more challenging to scale and make highly available, primarily due to the data and state they must maintain [8].
If a system cannot be scaled further, it is necessary to partition the data and use multiple servers. Continuous scalability is, therefore, achieved through data partitioning and a data-dependent routing layer or a stateful load-balancing system, which maps the logical data onto the correct physical partition. For increased availability, a cluster supports each partition. These clusters typically consist of two nodes with access to common, replicated, or protected Redundant Array of Independent Disks (RAID) storage. When the service on one node fails, the other node takes over the partition and offers the service. Another feature of backend is very important in data center design is swift and safe mechanism to update database servers.

Intrusion Detection Systems

Intrusion detection is defined as the problem of identifying individuals who are using a computer system without authorization and those who have legitimate access to the system but are abusing their privilege. In this paper the term intrusion means both external and internal intrusions. The recommended system for the corporate environment is "Enterprise Managed Intrusion Detection System" where multi sensor IDS systems allow pickup of traffic from all ingress communication tracks and analysis locally and report

to central management servers for further analysis and display on network operator consoles.
IDS Intrusion detection systems are the burglar alarms (or rather intrusion alarm) of the computer security systems. The aim is to defend a system by using a combination of an alarm that sounds whenever the site's security has been compromised. The security staff and incident response team respond to the alarm and take the appropriate action for instance by ousting the intruder, calling on the proper external authorities and so on [5].

Remote Access Connection

An e-business network can be created as an extension of an existing corporate network or it can be a completely separate physical network and system
Infrastructure, located at a carrier collocation facility. In a case where the new e-business infrastructure is created as an extension within an existing corporate network, the simple and secure way to connect the corporate network and e-business system is to build a dedicated VLAN on the core e-business infrastructure switch and restrict traffic by applying ACLs on the router and Switch (Layer 3), where all servers are connected. For more secure scenarios, it should be considered by putting a firewall between the Data Center Network and the Corp VLAN e-business infrastructure, as it is called "*backdoor"* protection [7-9].

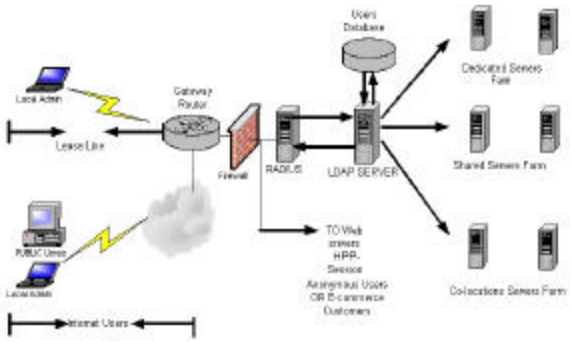

Figure 1: Remote Access Infrastructure diagram

In an e-business implementation where the supporting infrastructure is co-located at a remote facility there are two options for connecting to the corporate environment. The first option is to install a dedicated, private, point-to-point connection between the two sites. This alternative should be considered in scenarios where large amounts of data are expected to be transferred between the two sites. Redundant links should also be installed for resilience. The second option is to implement a secure communication path by using a Virtual Private Network (VPN) between the e-business network and the corporate network connecting both LANs. The connection between the two VPN servers provides end-to-end security over the Internet by encapsulating and encrypting traffic between two sites. IPSec over L2TP is the preferred way of connecting to the reference architecture infrastructure. In this scenario, a certificate authority server is installed for issuing certificates to the servers to ensure that the identities of the VPN servers do not change [10].

Remote access management is a paramount factor in Data Center security, since hosting private E-Businesses, where daily updates, or even many times in day updates of web Contents and database is needed. Without secure remote access, one cannot achieve the level of security, when many privileged users log in to a production server, serving web pages. The external and internal intrusion can only be detected, if the user login credential are in centrally controlled and managed enterprise-wide. The best choice will be the LDAP running on Unix server.
Radius is an Internet protocol that Lucent Technologies proposed in 1996. RADIUS contains three-user management pieces- Authentication –Authorization – and Accounting that referred to as AAA. RADIUS server on Unix is again the best choice and I would like to utilize all of these engineering features in this design.

IV. PKI KEY MANAGEMENT

This model is incorporated with digital certificate along with Key management. If an enterprise offers on-line business and remote users are using their login for financial transactions, or dealing with critical database, highly protected (HP) infrastructure is recommended.

However if the users are just a corporate users and dealing with business not required high level of protection than a digital certificate can be taken off from the above model but Key management will remain as in protected security zone.
In order to provide a uniform framework for key distribution and to manage key groups reflecting need-to-know categories, it is recommended to implement PKI (*Public Key Infrastructur*e) style key generation and authorization as a centralized function.
The basic structure of any PKI requires at least 2 functional blocks. Firstly, certificates must be created and destroyed (revoked) somewhere within the system, and secondly, certificates must be stored and made available to the clients [9]. The Certification Authority (CA) provides all the

required services of the former, and the Certificate Server (CS) the latter.

Since trust in a PKI system resides within the certificates themselves, the CA must be a trusted entity, but no such requirement need be placed on the CS. The CS receives Certificates and CRLs from the CA and stores these items in the corresponding database. The database server should be in highly protected portal. The CS provides several other interfaces to clients within the local domain as well as an inter-domain interface. Clients may contact the CS requesting certificates by subject name or serial number; they may also request CRLS from the CRS interface. Inter-domain clients may access the same facilities through the local CS. The CS may reside in corporate zone; need not be trusted as it merely stores certificates in which the trust is inherent.

Desirable Characteristics

Ideally, following are the characteristics needed to be included in the Data Centre design and in proposal for infrastructure,

i. Access Control List (ACL) on (Fire-walling) gateway router
ii. ACL on switching networks
iii. Firewalls at front and backdoor Multiple Sensor IDS system
iv. Anomaly detection system (for internal audit)
v. Radius server, for all remote dialup for web content. LDAP authentication for all users and remote access accounts
vi. DMZ and inside security zones rule sets on firewalls
vii. Enterprise Managed backup system
viii. Redundant power supplies (UPSs, Diesel Generators)
ix. State-of-arts environmental sensors (Surveillance cameras, humidity, fire, water leakage, moisture, Temperature sensors)
x. Strong air-conditioning systems Physical, Electronic Security appliances (Security Guard, Bio- metric hand scanners).

V.CONCLUSION

The issue of trust in e-commerce is fundamental to its eventual success. If consumers cannot trust that personal information is safe and secure, the Internet will never reach its economical potential. Based on best method principles in conjunction with independent auditing can bring back the confidence of customers of E-Trading. Computer based crimes are on the increase; in the past few years the Federal Bureau of Investigation (FBI) in the USA has recorded an increase of over 25% in computer crimes. In one case, an intruder was able to break into an Internet Service Provider's network, connect a sniffer and collect numerous ID's and passwords. When this intruder was finally apprehended, the FBI retrieved 86,270 credit card numbers from 1,217 different financial institutions [3].

The Internet and the World Wide Web offer enormous potential but measures need to be developed now to prevent abuse from occurring in this environment. These issues need swift resolution now in a co-operative climate between industry and government working together. If action is postponed, both the industry and consumers will have to deal with consequences of reactionary regulation in the very near future. This study unveiled some common weaknesses of an ISP / ASP services and suggested better design to overcome the issues. This paper would be helpful to professional engineers and researchers equally.

VI. REFERENCES

[1]. Yasin, R. " Security breaches surge over past two years FBI report " (1998).

[2]. Radcliff, D, " IS your ISP's Secure", March (1998)

[3]. Crume, J. "Inside Internet Security" (1999)

[4]. Directorate of defense signal Australia "Gateway Certification Guide" (1999)

[5]. Satti .M " Enterprise Managed IDS system" IEEE INMIC 2001 Lahore.

[6]. Et .B "Analyzing E Commerce on Internet" 2000
[7]. Wilson,T. "Profit Embolden Hackers " (2000)

[8]. Lewis, J." Data warehouse E Commerce (1999)

[9]. Graff,.CJ. "Cryptography and E-Commerce" (2000)

[10]. Jannathan, L " E-Commerce metrics models (1999)