Design of a Secure B2B Environment

Ivica B. Stanković[1], Aleksandar R. Mihajlović[2], Radomir A. Mihajlović[3]

[1] Faculty for education of the executives, Belgrade, Serbia,
ivica.stankovic@fpsp.edu.rs
[2]Technische Universität München, Munich, Germany, aleks.mihajlo@gmail.com
[3]Faculty for education of the executives, Belgrade, Serbia,
radomir.mihajlovic@fpsp.edu.rs

ABSTRACT: *This paper presents application of the topological physical space and software logical layered approaches to design of distributed business to business (B2B) systems. Being a tutorial in nature, this paper is stressing explicitly strict, almost formal, technical terminology, which has been loosely used in relevant technical literature. In the introductory part we discuss general e-business sytem design issues, focusing on B2B systems with built in security components necessary for secure business transactions. Special attention is devoted to the integration of individual systems of B2B business partners without any additional modification or redesign of the original existing local business automation software versions. We insist on B2B designs without any existing software alterations caused by security problems. With such a design approach, security problems become totally transparent to the original designers of the business partner's local systems and future users of B2B systems Special attention is devoted to the problems of possible drastic asymmetry of B2B business partners, where one partner could be too small and the other too large, resulting in degeneration of the B2B to customer to business or C2B system. Finally, we present design alternatives with different distributions of cryptographic modules in space, across the network topology and logically, along the stack of software layers and protocols.*

Keywords: *E-commerce, e-business, business transactions, B2B, C2B, system topology, system logical architecture, encryption, decryption, security tunnel, protection granularity.*

1. INTRODUCTION

One of the technological developments that literally changed the world in which we live is the emergence of telecommunications, digital computers and the Internet. On the top of these technologies we are witnessing the development of the super technology of modern information and communication technologies or ICT, which interconnects people, organizations and machines across the globe. However, as the history teaches us that technology is changing the world for the better, it tells us that new technologies are bringing new problems too. Common problems seen are mismatch and incompatibility of products of different origin and the misuse of technology.

Problem of incompatibility of technological hardware and software products from different sources is handled by introduction of standards. Standards enable a device, program, process, task or project, to be added to existing technology without a risk of a conflict or need for redesign and adjustment to the new context. With the globalization of the Internet, standardization of hardware and software to be used on this super sized public infrastructure has reached global proportions too.

The most detrimental misuse of technology that deserves serious standardization consideration is related to security and immunity to the misuse of technology. To illustrate the importance of addressing security of public infrastructure with total exposure to users and misusers, we may look at the Internet abuse reports which are reaching levels of over five orders of magnitude per year [1]. Networked computer security is evidently a growing problem. A central information hub, the Computer Emergency Response Team or CERT, regularly reports security violation incidents and new application, systems and network vulnerabilities. Both, security incidents and reported vulnerabilities have been doubled each year since 1997. In addition, the number of business and private web page defacements per year has roughly doubled each year too. Since 2000, attacks on larger web servers has grown to more than 20 per day, [1] [2].

Since the integrity and security of business transactions, is one of the most important issues, we place emphasis on the protection of these transactions using cryptographic technology. Through a set of steps and examples, we present structured principles of design of secure business systems that integrate multiple business entities across inexpensive Internet infrastructure.

2. BRIEF HISTORICAL OVERVIEW

Explosive growth of the Internet as the global system of networked hardware host computers and software modules of distributed applications has started with the US government Department of Defense (DOD) ARPANET project in the year 1968, [3]. In order to engage a larger number of talented people on the development of the super complex system, the military project ARPANET network was gradually turned into a public network project which we now know as the Internet. Initially the ARPANET project was transferred to the leading US universities. The ground breaking development of the public Internet took place at Berkeley, MIT, and Stanford universities. The first exchange of digital messages between research applications running at Berkeley and Stanford University, over the ARPANET, has marked the beginning of the public use of the Internet. This first instance of opening of the future Internet, has announced possible networks malicious use or misuse that we now refer to as hacking.

In spite of early public opening, transition of ARPANE to Internet took very long period of time. Price of computers and telecommunications services were the main reason why the massive use of ARPANET, was more than 25 years delayed. In order to have Internet be part of everyone's daily life, global market inertia had to be countered with the gradual developments of affordable hardware and software technologies, (e.g., high-speed personal computers, more powerful operating systems and user friendly, easy to master and use, applications.) It is worth noting that slow development and hard market progress of personal computers (PCs), as Internet user interface devices, was the primary reason why wide public adoption of Internet lagged behind the ARPANET early development for over 25 years. For instance, following the initial introduction of simple PCs in the early 1980s, the first powerful PCs with large enough memory to accommodate Internet software and user friendly Graphical User Interface (GUI), emerged 10 years later, in the early 1990s. The first multi-tasking and multi-threading popular PC operating system, Windows NT 3.1, was shipped 1993. With confidence, we may say that Internet massive public use has started about the same time.

PC as Internet user interface device was the key element of Internet development and globalization of use. The reasons of slow PC hardware development are primarily economic in

nature. This implicate fact has been explicitly recognized by the ingenious market master, Bill Gates. He was clearly aware of the fact shown in Figure 1. Namely, Figure 1 illustrates quadratic dependence between the computing speed and the cost of development of faster computing devices. To justify the investment in new device and software development, such costs have to be divided over an as large as possible market [4]. The Internet and Bill Gates have enabled exactly that mechanism in the best possible manner. By selling, i.e., doing commerce electronically over the Internet, sharing of newly developed product costs becomes much faster and price decline trend much steeper over a much shorter period of time. E-business has powered technological progress and vice versa. It would be impossible for Microsoft to generate over 70 billion dollars of sales in 2012, without the Internet electronic or e-business means, [5].

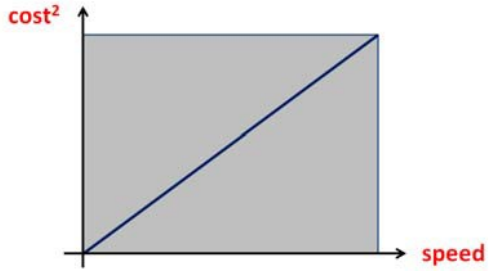

Figure 1: The dependence of the cost and the speed of new computer development.

3. INTERNET PROTOCOLS AND INTERFACES

Modern Internet, as global network of hardware devices, software applications, individual people and organizations has grown into the structured layered super system capable of providing world wide services at any recognized layer of generality.

The Internet as global network is based on system software, i.e. the protocols known as TCP/IP. In order to bring order into the rapidly developing area of distributed computing software and computer communications, in the early 1980s, International Standard Organization, or ISO, has proposed a standard named **O**pen **S**ystems **I**nterconnection known as ISO-OSI model of distributed software architecture, [6]. As shown in Figure 2.b) TCP/IP systems and application software are logically stacked up similarly to the ISO-OSI model of Figure 2.a). We may consider TCP/IP logical model as practical and widely applied and ISO-OSI model as theoretical. The majority of distributed applications running on the Internet are engineered according to TCP/IP model, where application layer software incorporates the top three layers of the ISO-OSI model. According to the TCP/IP model application software modules directly use services of the application message transport layer.

Figure 2: a) Layers of the ISO-OSI model. b) TCP/IP Internet protocol layered model.

TCP/IP compatible implementations offer two types of transport, TCP to be used with error intolerant applications such as e-commerce, and UDP to be used with delay intolleant applications such as multimedia data distribution or IP telephony. To better utilize the underlined network of links that are spanning the Internet, all legthy application messages are segmented by the transport software into Maximal Transport Units MTUs or packets of roughly up to 1.5kB.

It is important to note that all technical solutions implemented on the layer immediately below the transport layer are classified as network solutions. Standardized TCP/IP network layer of services is implemented in two versions, versions IP v.4 and IP v.6. Topologically, in the physical space, the Internet is maintained on the network layer by the massive number of devices known as routers, which are interconnected with their immediate neighborhoods by hardware-software entities known as a links. Figure 3 illustrates an internetwork of four business networks connected to the Internet via routers. Even home based networks, single host networks are attached to Internet via routers. With routers acting as internetworking devices, one may define the Internet as a global network of routers.

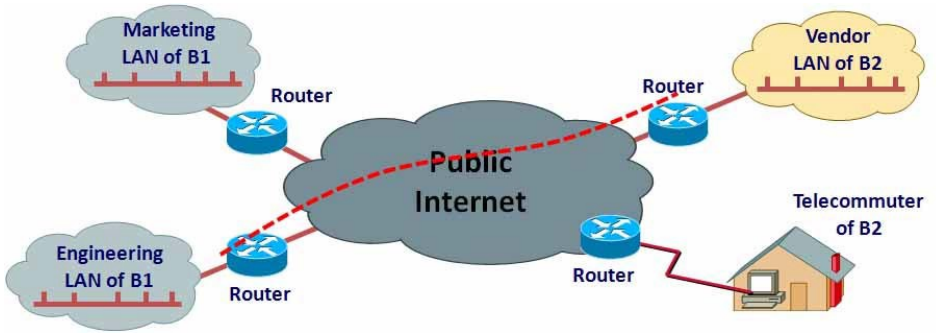

Figure 3: TCP/IP powered network is a packet network that transmits segmented application messages no larger than MTU.

As shown in Figure 3, the topological business network layout with two business partners B1 and B2, have their local networks interconnected across inexpensive public Internet infrastructure. To benefit from the low cost Internet communication services, businesses and all users in general, must have routers as packet switching or packet data traffic processing devices, working also as private network delimiting or border perimeter definition devices. Each private local network may contain multiple internal routers delimiting internal local sub-networks, but must contain at least one border or gateway router facing Internet.

Before sending or after receiving application messages, in the application layer, in the top layer of Figure 2, wide variety of distributed applications processes messages differently. Software in charge of direct communication with the transport layer services, and in charge of pre-processing messages so that higher application layers have less work to do and may be simpler to develop, is known as application message protocol. One of such message protocols that have been recognized as the easiest to use and the fastest in packing and unpacking messages is known as Hyper Text Transfer Protocol (HTTP.) HTTP protocol is the most widely used application sub-layer or sub-protocol. As a message protocol, HTTP provides services to standardized class of distributed applications that we all now know as the World Wide Web, WWW, W3 or simply the Web. We are stressing here that the Web is pure software entity, made up of globally distributed modules of standardized client and server software modules using HTTP to interface with the transport layer of TCP/IP services. On the lower level of the application layer, Web application software end-point-modules are interfaced with the Internet TCP/IP services via HTTP.

To highlight the simplicity of developing Web software using HTTP, on the higher level of the application layer, we mention here that developers have to use simple languages such as Hyper Text Markup Language (HTML), and JavaScript. HTML and JavaScript are standardized Web application development languages [7].

On the top of the entire family of standardized software layers or protocols, (e.g., TCP/IP with TCP and UDP message transport services, HTTP as message pre and post processing protocol, HTML and JavaScript as Web application simple programming languages, etc.), ignoring all complexities of standardized protocols, developers may focus on the application relevant complexities, i.e., on business processes and their software support. Most of the business software using Internet is of a Web type, i.e., uses Internet through the Web. The Web has immensely simplified use of the super complex Internet communication infrastructure. Using the Web browser as a general programmable Web client module, the user can approach remote data source by simply clicking a button on the mouse. There is no simpler activity that user is capable of generating to initiate complex communication session. This tremendous ease of use of the Web applications is the driving force behind the wide spread and acceptance of the Web. Hypertext concept on the higher end of the Web application layer and standardized Uniform Resource Locator (URL) with HTTP as the lower application standard sub-layer, define the Web as the most user friendly interface to the complex Internet communication infrastructure.

4. USING THE INTERNET FOR E-BUSINESS

Using computers and teletype terminals in a form of Business to Business or B2B system appears in the early 1970's. In an attempt or maximize flight occupancy and sales profits, airline carriers were among first to embrace computer supported tracking flights and seat availability, and sharing data between their sales offices or partner airline companies, [8]. From the early 1970s e-business has taken exponentially rising path. Just to stress the dimensions of e-business development it is enough to look at the amounts of business done on the Internet. For instance, total e-commerce sales in United States for 2012 were estimated at $225.5 billion. Total retail sales in 2012 increased 5.0 percent and e-sales 15.8 percent from 2011. E-commerce sales in 2011 an 2012 accounted for 4.7 and 5.2 percent of total sales, respectfully. The trend of escalating e-commerce is evident.

With the advent of the Web as one general application running on Internet, messaging over the Internet has become simple. That ease of communications and the Web programming simplicity is effectively employed, as one higher level platform, as one intelligent communications infrastructure, by distributed business applications.

By definition all business applications dealing with promoting and realizing exchange of goods and services, i.e., implementing trade transactions, can be classified as e-commerce applications. Electronic business or e-business represents a set of business activities that are enabled by ICT, (especially the Internet.) Business activities in question include:

- Optimization of business processes, (e.g., production, marketing, sale, distribution, sales, billing, deliveries, and inventory update),
- Improving relationships with customer population and business partners, (i.e., customers, employees, suppliers, distributors), and
- Enhancing activities with business support partners, (e.g., banks, investors, law agencies, accounting agencies, and government agencies.)

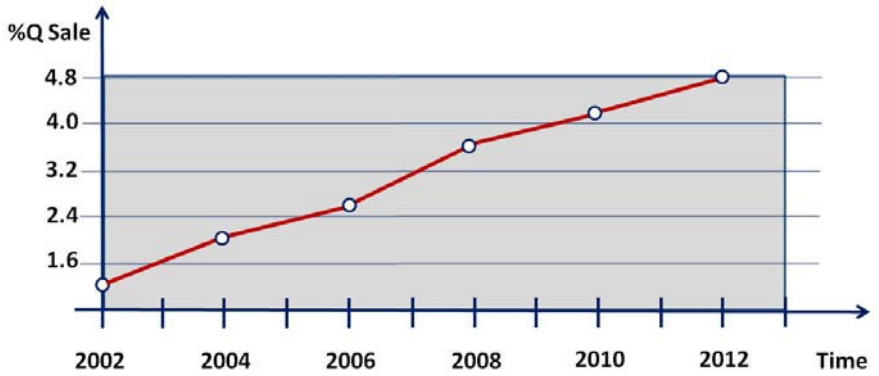

Figure 4: Estimated quarterly US e-commerce sales as a percent of total quarterly retail sales, [9].

Popular term of e-commerce represents e-business activities narrowly focused on sales. E-commerce is one subset of e-business. By definition, e-commerce as a branch of e-business is the process of purchase, sale and exchange of goods, services and information via computer networks including the Internet.

Elementary business process requires a minimum of two business entities. According tho the basic categorization of e-business, depending on participants and the relationships, we may have the following e-business relationships:

- Business to Business (B2B)
- Business to Consumer (B2C)
- Consumer to Business (C2B)
- Consumer to Consumer (C2C)
- Business to Employee (B2E)
- Employee to Business (E2B)

When employing a chain of multiple transactions, business system may include more than two business entities. With regard to the business partner cardinality, general types of such business systems may be classified as:

- Business to Business to Consumer (B2B2C)
- Consumer to Business to Consumer (C2B2C)
- Peer to Peer (P2P)

This paper discusses the design of e-business system primarily with binary cardinality.

5. B2B ELECTRONIC BUSINESS SYSTEMS AND PROBLEMS

At the very beginning of e-business dating back to the early 1970's [8] [10], when business organization started electronic linking of computer systems over the private telecommunication lines, propriatry custom developed software was used without any standardization. With the expansion of public use of Internet, with the lower cost and higher power computers, communication lines and software packages, a series of standardized solutions emerged. Expansion of markets implied necessity and progress of standardization, and standardization, in a feedback loop further propelled market expansion [11]. Among the first companies to embrace the Internet as a communication infrastructure, to build and perfect B2B software super-structure was shipping giant Fedex Corp. Originally called FDX Corp., formed in January 1998 and later renamed FeDex Corp. organized their express delivery services around the network of computers and software that has integrated FeDex shipment management team with FeDex transportation service partners [12].

The idea of computer powered business partnerships was initially proposed by Frederick W. Smith, FeDex founder, in 1965. As Yale University undergraduate student, he wrote a term paper about the computerized passenger and cargo route systems optimization. Preliminary implementation of his original idea has started in August of 1971 When Smith bought controlling interest in Arkansas Aviation Sales Co., located in Little Rock, Ark. While operating his new firm, Smith identified the tremendous difficulty in getting packages and other airfreight delivered within one to two days. This dilemma motivated him to do the necessary research and development for redesign of the inefficient distribution system. Thus, the idea for B2B Federal Express giant was born. FeDex is a company that revolutionized global business practices, as the very first organization to effectively employ B2B technology over the Internet, and so redefines speed and reliability of customer services. Without a B2B and C2B e-business systems, it would be impossible for FeDex to handle close to 20 million shipments per year, [13]. FedEx Corporate Services, Inc., represents today one of the largest B2B systems, aligning, vendors, customer contact centers, worldwide revenue operations, claims offices, tracing packages, etc., acting as a professional services company, [12].

Two more companies which have contributed very much to the development of B2B and C2B systems development is Amazon and Dell Inc., with annual sales reported for fiscal 2011year of close to 50 and 60 billion dollars, respectfully. [14] [15].

In 1994 Dell, a Texas based manufacturer and distributer of personal computing products launched Dell.com e-business site. By the end of 1997 Dell was the first company to record a million dollars in online sales. The company's unique strategy of selling goods over the Web with no retail outlets and no middlemen has been imitated by a great number of e-commerce

businesses. The key factor of Dell's e-business success is that Dell.com enables customers to browse, choose and assemble PC components piece by piece based on their budget, requirements and free will. While maintaining zero inventory, reaching sales of over 60 billion dollars per year would be impossible without gigantic B2B and C2B system, [15]. Dell systems were integrated with suppliers and customers, maintaining optimal inventory holding costs at nearly the theoretical minimum. By using ICT and e-business, Dell achieved a higher income than classical operators such as McDonald's with more than 33,000 restaurants and 1.7 million employees.

E-business systems of B2B type, uses Internet to integrate systems of minimum two business organizations, providing automated exchange of business data between different legal entities. Lessons learned are that B2B is of mutual benefit to all participants. The use of public Internet at a lower level, and the Web at a higher software level, brings to B2B systems following advantages:

- Reduction of communications costs
- Better integration of the supply chain
- On-line acquisition of the goods from the supplier partners
- The simplification and greater transparency of transaction operations
- Easier access to new markets and connection with new partners
- Expansion of existing and introduction of new transaction processing methods

As it is the case with all engineering projects, migration from legacy business methods to B2B e-business methods introduces certain difficulties and problems. Designers of B2B systems have to deal with the following issues:

- Re-engineering of existing manual business processes requires significant costs and human resource.
- The use of electronic methods brings certain legal problems associated with insurance of transactions and goods, and
- The use of public Internet communications infrastructure opens business transactions to malicious attacks and various security problems.

Successful B2B system typically includes an optimized and integrated business process, of at least two business organizations, where among optimal integration solutions one must count in the solid security of all transactions handled over public Internet.

6. DESIGNING A SAFE ENVIROMENT FOR B2B OPERATION

B2B system designers are faced with a spectrum of design dimensions. The first dimension to deal with is the legal dimension. Before dealing with technical problems, all legal issues must be resolved.

When the team of B2B partners with previously automated business procedures, decides to proceed with the integration, the following issues must be resolved:

- Mutual agreement between business partners must be made, in terms of data structures related to the forms and templates for ordering, invoicing, shipping, delivery notifications, the method of payment, etc. Standardization is welcome in all situations when multiple parties have to agree on format of data and documents. One of the first standardized

solutions relevant to this issue is Electronic Data Interchange (EDI) standard, [16]. EDI standard specifies the format of application messages between trading partners connected electronically. The Accredited Standards Committee X12 (ASC X12), chartered by the American National Standards Institute (ANSI) in 1979, maintains the X12 EDI and Context Inspired Component Architecture (CICA) standards with XML message standard schemas which drive e-business processes globally [17]. The name "X12" is a sequential code assigned by ANSI at the time of accreditation. ASC X12 covers more than 315 X12-based EDI standards and a growing collection of X12 XML schemas for health care, insurance, government, transportation, finance, etc., transaction data formats. High level business protocols like EDI are the job of expert business process designers. ASC X12's membership includes over 3,000 standards experts representing over 600 companies from multiple business domains [18]. All mismatched business protocol details between the B2B partners must be precisely aligned at the very beginning of B2B system. EDI tremendously simplifies this alignment job.

- Communication and Internet readiness is essential. EDI as the very first and comprehensive B2B relevant standard was originally used over the private and leased communication lines with exotic message and transport protocols over single link connections. Infrastructure used was not Internet compatible. Introduction of Internet has brought new and easy to adopt communication standards. Before starting with B2B planning, each business partner is expected to already have established private Internet compatible intranet, (i.e., local TCP/IP compatible networks.) Almost all new B2B systems start with well established intranets connected via standardized routers to the Internet.
- Internal business process automation systems have to be in place. Almost all B2B partners start planning for the B2B integration with already working business automation software in place, with office personnel well trained and used to the existing ways of processing business transactions.
- Security problems must be recognized and proper design solutions must be pre planned. All necessary plans and conditions for securing transactions across the Internet must be ready for implementation.

On the subject of the second B2B design point, partner's B2B inter network, must be TCP/IP compatible intranets (e.g., B1 intranet and B2 intranet shown in Figure 5), using standard routers (e.g., Router1 and Router2), to define intranet boundaries and enable traffic filtering to and from the Internet. Figure 5 illustrates an example of the basic topology of one B2B internetwork system without security measures applied.

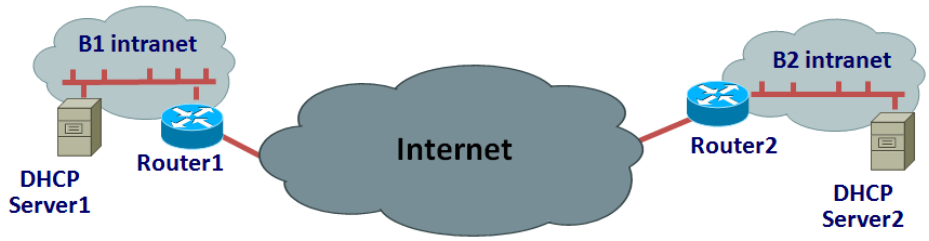

Figure 5: Network topology with two B2B business partners intranets with local DHCP servers [19].

The fact that partners have working intranets guarantees, by definition of intranets, that each individual host computer (network node) in their operating systems (OS), regardless of whether it is Winodws, Unix, MacOS, Solaris, or Linux, has TCP/IP software layers installed, loaded and properly configured. Figure 6 shows an example of system configuration utility that enables systems administrators of Windows OS to configure loaded TCP/IP service parameters. Most of the host computers have TCP/IP service automatically configured via Direct Host Configuration Protocol (DHCP) local network service, (e.g., Figure 5 shows intranets of two partners with two local DHCP servers.)

One of the elementary B2B partner networks design rules implies the necessity of planning a DHCP automatic TCP/IP parameter distribution. By using a DHCP server, as a part of local intranet infrastructure, designers may guarantee certain discipline and order in the distribution of the relevant systems parameters such as:

- IP address of the host computer,
- IP address mask defining local network IP address
- IP address of the default router, and
- One or more of IP addresses of Domain Name System (DNS) servers to be used for the URL user friendly application layer address conversion into the Internet address number.

Manual TCP/IP configuration is used only on the small business partner's networks. In case of larger networks, DHCP is preferable choice. Client host transition from the manual TCP/IP configuration to automatic via DHC is very simple, (e.g., by simply checking "Obtain IP address automatically" on the form in Figure 6.)

In the framework of the B2B design project, particular attention has to be devoted to the last point in the above list of major design issue. Namely, the importance of security sub sytem is proportional to the volume and the value of business transaction data traffic from one partner to another.

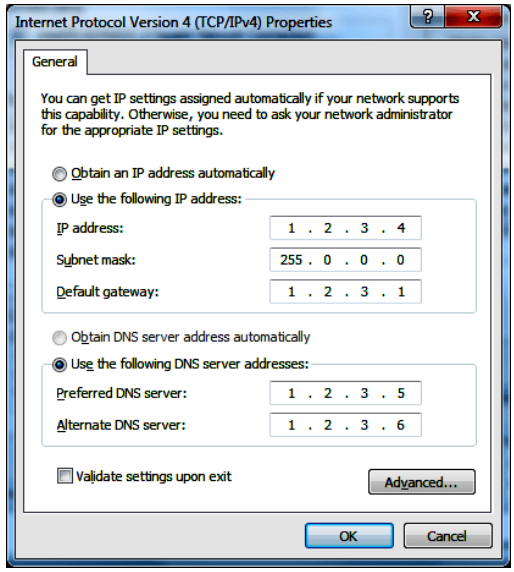

Figure 6: Example of the screen form of the TCP/IP manual configuration utility under Windows 7 OS.

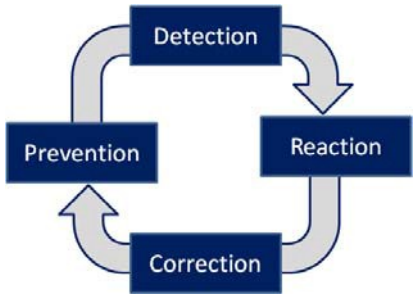

Figure 7: The security process cycle.

Security does not assume only the implementation of security technologies, but also a process that must be implemented on the user level throughout the business organization. Implementation must define security relevant system design project segments and future continuous daily operations (e.g., administration and timely updates.) Planned maintenance activities related to security can be divided into the following four repetitive stages:

- Prevention stage anticipates and prevents known type of security violations.
- Detection stage detects and identifies security violation in progress or imminent threat.
- Response stage uses detection results to decide upon the type of response and proceeds with neutralizing attack in progress or imminent threat.
- Repair stage includes activities of reinstatement of the original operational system state, and adaptive (learning) upgrade of all previous stages.

Figure 7 shows four main stages of the cycle of the security process. The security subsystem is not static in nature, and once designed and implemented, it is not finalized. If necessary, the process must be modified and reworked. Basic B2B security system design must have possible opening to later refinement.

The initial design of B2B security system focuses on the prevention of malicious attacks on business transactions. Defense strategy with e-business is to enable primarily prevention, than detection and response.

7. B2B TRANSACTION PROTECTION

To avoid business transaction data being open during a commercial message exchange over the public Internet infrastructure, encryption methods can be used to transform public data paths through the Internet into virtually private roads, which can be called safety tunnels. Such application of cryptographic, here referred to as crypto technologies, results in B2B alteration into a Virtual Private Networks or VPN. Upon application of encryption, B2B internetwork with Internet portion being public in nature, becomes virtually private.

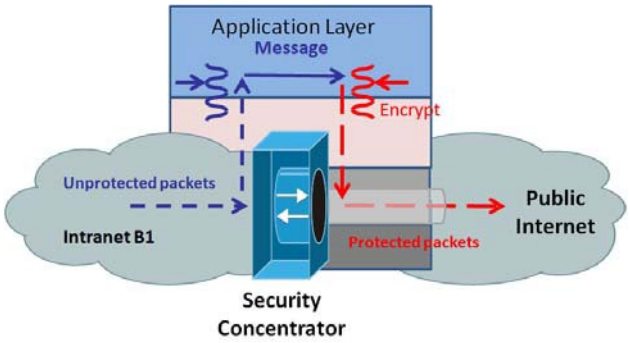

Figure 8: Security encryption application in one of the logical layers [19].

Figure 8 shows the flow of data traffic through the layers of encryption processing software running on the security data traffic processor at the point of entry into the Internet. The view shown may be classified as the logical software architecture layered view, and the device implementing such a view may be labeled as traffic security concentrator [20]. Concentrator of Figure 9, selectively collects all unprotected traffic packets of B2B messages, unpacks them, encrypts them, packs them again and forwards them in the Internet direction. On the other end of the security tunnel complementary concentrator performs the reverse processing before forwarding unprotected data traffic in the direction of the partner's intranet. Concentrator may be distinct device or can be implemented as software installed in the end point host computers, (See Figure 9.).

Pair of encryption and decryption processes form software object logically appearing as "dark" tunnel which transform traffic data content from readable or clear into protected, unreadable or opaque. In the following sections we use the concept of security tunnel when considering

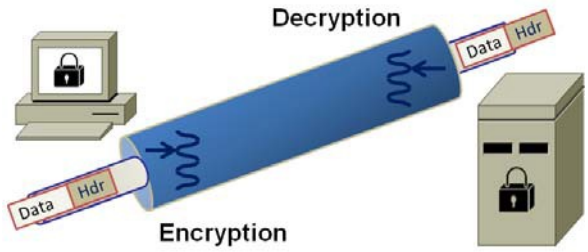

Figure 9: Security tunnel with the encryption on the entrance and decryption on the exit of the secure tunnel between two designated host computers, [19].

the topology and distribution of points of encryption and decryption in B2B network topology and logical architecture. In this paper we consider all topological solutions. The choice of selected solution depends on the degree of mutual dependence between the business partners in the overall B2B system.

8. TOPOLOGICAL DESIGN FOR SECURE B2B ENVIROMENT

When it comes to the distribution of topological points of encryption and decryption mechanisms in the B2B system, designers can consider level of refinements of traffic protection. The choice of a particular option depends upon the needs of all B2B users and those users of intranets that do not participate in B2B activities.

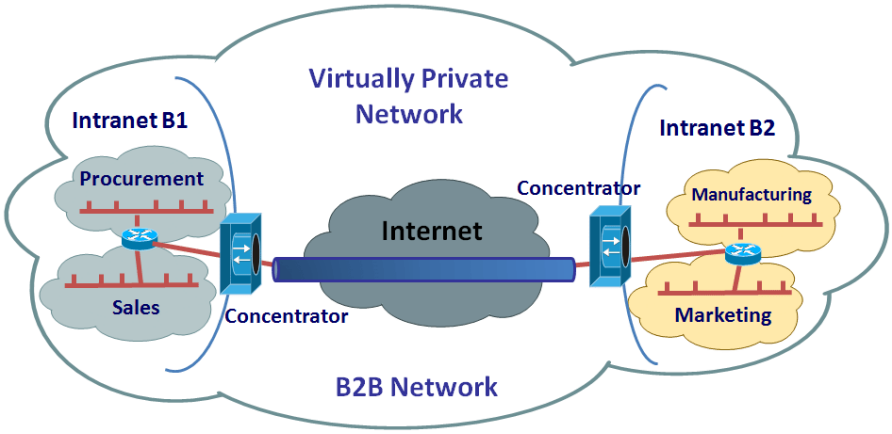

Figure 10: B2B design of encryption tunnel from the main border router of a business partner B1 to the main border router of the business partner B2.

Figure 10 presents the most general design proposal of encryption/decryption traffic protection refinement. Two concentrators positioned next to each partner's intranet perimeter routers are able to protect all business sessions in the data traffic streams, from any node to any node of partner's intranets. This solution simply integrates two intranets into one VPN, where private refers to the fact that traffic between intranets through the public Internet will not be available for interpretation by any other user of Internet except the business partners. Design solution with topological positioning of concentrators shown in Figure 10 is good choice when partner's intranets are of similar size. This option enables users to work securely at any of the intranet's nodes, and move freely from one host computer to another.

In situations of partner intranets asymmetry or when partner's intranets are very large in size, only sub-networks of each intranet are to be protected by concentrator delimited secure tunnels. In these situations we have segmented confidentiality, i.e., privacy. For instance, Figure 11 shows two large partner intranets, with only Procurement sub-network of Intranet B1 securely connected into the VPN with Sales sub-network of Intranet B2. Security tunnel exists between edges of smaller sub-networks within larger partner's intranets.

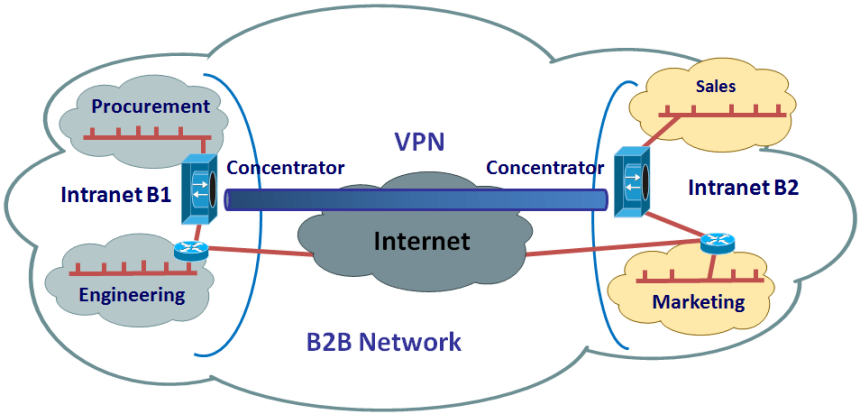

Figure 11: B2B with a couple of intranets of large Enterprise organizations segmented to smaller sub-networks integrated into the B2B VPN.

In case of huge organizations, to which we refer as Enterprise, with over 1,000 network nodes per intranet, segregation of the original intranets into the sub-networks to be integrated into the B2B VPN is necessary.

When designers face extreme B2B partner intranet asymmetry, e.g., with one large size partner and one or smaller partners or individuals, segregation of partner's intranets may be performed down to the individual network node. Example of the B2B topology shown in Figure 12 illustrates one such case, where just one host on the Intranet B1 is securely connected via VPN tunnel to the Sales sub-network of the Intranet B2. This case of very fine traffic stream protection degenerates B2B to C2B system.

A refined approach to the distribution of security tunnel end points in B2B systems demands positioning of the tunnel end points at the host computer physical network port or inside of a node, above the transport service layer, at the port of the application modules in charge of e-business transaction processing. As shown in the logical protocol stack diagram in Figure 14.b, popular Secure Socket Layer (SSL) [21] or Transport Layer Security (TLS) software may be used to implement security tunnel between two application modules [22]. In case of the most refined approach of tunneling data traffic between the modules of the distributed application, original application software has to be reprogrammed, i.e., the security problems become developer's problems. In case of C2B or C2C e-business applications this may be a choice. Application module-to-module security tunnel protects only given application traffic, while, host-to-host tunnel (e.g., Host1 yo Host2 tunnel in Figure 13), protects all traffic between two hosts regardless of the application being used.

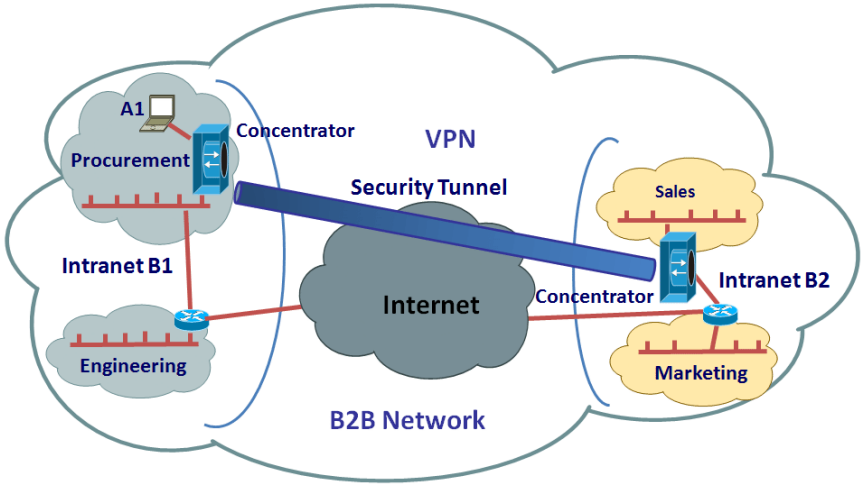

Figure 12: Design with fine traffic protection-granularity on Intranet B1, and coarse protection-granularity on the Intranet B2 of the B2B VPN.

In summary, security tunnel end points between B2B partner intranets can be located at any two points on the following list:

- In the network layer on the edge of the partner's intranet, at the location of the edge router, (Coarse traffic protection granularity solution)
- In the network layer at the entrance to the relevant partner's intranet subnetwork, at the location of the internal intranet's router, (Medium coarse solution)
- In the network layer at the point of the relevant host physical line access, (Fine granularity of data traffic protection), and
- In the application and above the transport layer, at the entrance to the specific application module, (Very fine granularity of the data traffic protection).

All of the network layer choices are system design options and do not require any application software reengineering. As such all security tunnel implementations in the network layer are problem of network engineers and systems administrators. The best solution of this type is widely used IPsec protocol [23] (See Figure 14.a.) As the network layer solution, IPsec can be implemented at any of the first three points in the above discussed topological list of points of the integrated B2B system.

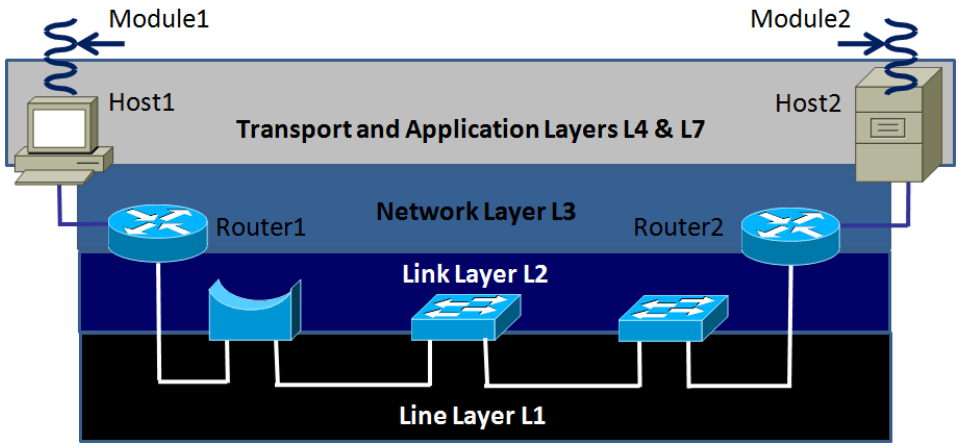

Figure 13: Logical stack of protocol layers and possible locations of B2B security tunnel end points, (Module1, Host1, Router1, Router2, Host2 and Module2.)

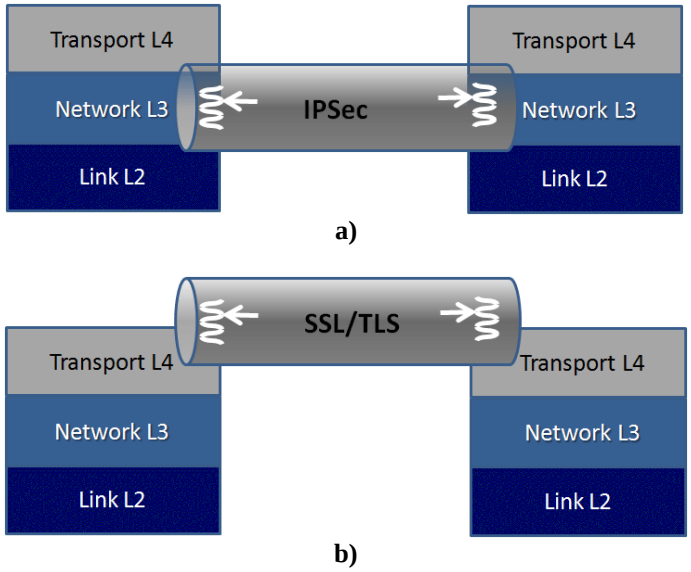

Figure 14: a) IPsec network security implementation may be implemented with various protection granularity. b) SSL/TLS application layer security implementation with very fine granularity.

The concept of the security tunnel is based on the application of the pair of programs executing encryption and description algorithms. Sensitive data “traveling” through the security tunnel are encrypted. Coordination or crypto-synchronization, of the two tunnel programs is typically controlled by the third program (or set of third party programs) in charge of safe encryption key management and distribution. The presence of the third party with security tunnels makes all secure session hijacking attacks virtually impossible.Discussion of security

protocols used to manage security tunnels of B2B systems is beyond the scope of this paper. Dorsawamy and Harkins present this quite involved subject in a very elegant manner in [Dorsawamy 2003].

At the end, we must mention that security tunnels may be implemented in the layers below the network layer too. Tunnels in the link layer or L2, shown in Figure 13, can protect only one individual link along the route of links between the B2B internetwork end points, and as such are not interesting for B2B applications across Internet. Commonly, B2B end points are connected by the long route as a chain of multiple links. Designing and implementing chains of individual link based security tunnels in the B2B system would be to complex, too costly and in most cases unfeasible.

Security tunnels implemented in the lowest physical layer L1, by securing physical communication lines via electronic signal encryption modulations is acceptable only in military applications and as very costly, such tunnels are of no interest for commercial applications of B2B systems.

9. CONCLUSION

This paper project is aimed at the problem of practical B2B system design with particular reference to the unavoidable issue of security. The benefit of low cost and good performance of the modern Internet to business applications comes at the expense of having to deal with possibilities of malicious attacks on business transactions.

In our approach to secure B2B system design we distinguish three general design segments: business, application, and security design segments. Cryptography is the indispensable foundation of the last design segment and of any secure solution. Following the deductive argument, like the one demonstrated in [24], our analysis of possible methods of application and distribution of the so called crypto technology across the B2B system, proposes distribution that can be rough or coarse (from network to network), or refined (from application to application).

In section 3 we emphasize that many Web users identify Web with Internet, which technically is not the case. We make it clear that the Web is a general type of distributed application, powered by Web message processing protocol knonw as HTTP. B2B systems run on the Web, while Web runs on Internet as a communication infrastructure.

BIBLIOGRAPHY:

[1] FireEye Advanced Threat Report – 1H 2012, FireEye 2012 reprot, http://www.fireeye.com/resources/pdfs/fireeye-advanced-threat-report-1h2012.pdf
[2] ICS-CERT Incident Response Summary Report 2009-2011, US Department of Homeland Security, 07/11/12.
[3] ARPANET Information Brochure 535, Defense Communications Agency, February 2, 1979
[4] Ellen Dulberger, Sources of Price Decline in Computer Processors : Selected Electronic Components; Murry Foss, Marylin Manser, and Allan Young, editors, Price Measurements and Their Uses, University of Chicago Press, : January 1993, p.103 - 124
[5] Microsoft Corp. 2012 Annual Report – Financial Highlights, Microsoft.com, 2013

[6] H. Zimmerman, OSI Reference Model -- The ISO Model of Architecture for Open Systems Interconnection, IEEE Transactions on Communications, 28(4), April, 1980, pp. 425-432.
[7] Steven M. Schafer, Web Standards Programmer's Reference: HTML, CSS, JavaScript, Perl, Python, and PHP, Wiley Publishing, Inc., 2005.
[8] Copeland, D., McKenny, J. Airline reservation systems: Lessons from history. MIS Quarterly, September, 1988, pp.362- 364.
[9] Quarterly Retail E-commerce Sales , 4th, Quarter 2012, U.S. Census Bureau News, U.S. Department of Commerce, Washingron, D.C., 20233, Friday, February 15, 2013,
[10] David Lucking-Reiley and Daniel F. Spulber, Business-to-Business Electronic Commerce, Journal of Economic Perspectives—Volume 15, Number 1—Winter 2001—Pages 55–68
[11] Rolf T. Wigand, Electronic Commerce and Reduced Transaction Costs; Electronic Markets, Newsletter of the Competence Centre Electronic Markets, No. 16-17, 1 November 1995, pp.2-5
[12] History of FedEx Operating Companies, Aout Fedex, 2012
[13] E-Commerce Shipments to Drive Record FedEx Holiday Volume, FedEx Newsroom, October 24 2011
[14] Amazon 2011 Financial Anual report, Amazon.com. 2012.
[15] Fiscal Year 2011 in Review, Dell Corp., 2012.
[16] EDI Standard Exchange Format - Version 1.6, ED-4-0101, Foresight Corporation, January 2001.
[17] CICA: The Future of Standards Development, Accredited Standards Committee X12 Context Inspired Component Architecture Using CICA Architecture for Building XML Messages, ASC X12, 2013,
[18] The Creation of ASC X12; Today's Foundation of Business-to-Business Electronic Exchanges, The Associated Standards Committee ASC X12, 2013
[19] Radomir A. Mihajlovic, Computer Network Perimeter Protection, New York Institute of Technology, 2009.
[20] Security Requirements for Cryptographic Mocules, FIPS PUB 140-1
FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, January 11, 1994.
[21] D. Wagner and B. Schneier, Analysis of the SSL 3.0 protocol, The Second USENIX Workshop on Electronic Commerce Proceedings, pp. 29–40, 1996.
[22] C. Michael Chernick, Charles Edington III, Matthew J. Fanto, Rob Rosenthal, Guidelines for the Selection and Use of Transport Layer Security (TLS)
Implementations, Computer Security - NIST Special Publication 800-52, June 2005
[23] Naganand Doraswamy, Dan Harkins, IPSec, Prentice Hall; 2 edition, March 23, 2003.
[24] Borivoj I. Subotić, Viša matematika pomaže elementarnoj, strana 141-146, zbornik radova broj 4 godina 3, Fakultet za ekonomiju i inženjerski menadžment u Novom Sadu, Novi Sad 2010.