Virtual Enterprise Security: Importance, Challenges, and Solutions

Morteza Mohammadi Zanjireh
Computer Engineering Department
Imam Khomeini International University

Ali Kargarnejad
Computer Engineering Department
Islamic Azad University of Tehran-South

M. A. Tayebi
Computer Science Department
Amirkabir University of Technology

Abstract: - Advances in Information and communication technology causes many changes in societies and human being life. One of these changes is formation of virtual enterprises concept in electronic markets. A virtual enterprise is a temporary alliance of autonomous and possibly geographically distributed organizations that pool their resources to meet short-term goals and exploit fast changing market trends. The important topic in a virtual enterprise life cycle is maintaining its security. Because if a virtual enterprise do not maintain its security, its lifeblood data and information will be accessed and used by other competitors and this means that virtual enterprise will defeat in electronic market. In this paper, we describe some security problems in virtual enterprise architecture. Also for each problem, we propose solutions for eliminating that security problem.

Key-Words: - virtual enterprise, electronic market, data access control, identification, authentication, authorization, partners communications, security.

1 Introduction

Recently we have observed the convergence of several threads of technology and business. One of these areas that become an attractive topic between computer scientist and business persons is virtual enterprise (VE). This is a particular form of business corporation that is built from organizationally and geographically distributed units.

A VE is a community of business entities that collaborate on the manufacturing of new products. The collaboration is often for a specific product only and after achieving foreseen goals the VE may taken apart. Indeed, VEs exist for a limited amount of time.[1] Each member of a VE often owns a complementary skill, which is supported essential for the target product. The partners collaborate among themselves [2] and they are goal-oriented communication-based that share their costs, benefits and risks. Therefore, a VE is composed of entities that come together as a team to achieve a special goal.

There is no clear definition of the VE, but there is a general agreement among the different definitions that are proposed currently. For example, the NIIIP project [3] defines the VE to be "a temporary consortium or alliance of companies formed to share costs and skills and exploit fast-changing market opportunities".

From a business perspective, building a VE involves contracts, cross-organizational management and statutory obligations. From a technical prospective it involves confronting problems such as heterogeneity, distribution, privacy and security.

Nowadays security is the major challenge in computer and network based systems. Because of that, also VEs are involved with this problem. The greatest challenge facing VEs is maintaining the security of itself. So for having an efficient VE, we should solve the security problems at first. Maintaining the security and protecting data in VEs is important for two reasons. First, data often represents a large amount of money due to labor intensive tasks. Losing data means losing money. Second, data often represents knowledge and provides companies with a competitive edge.

This paper builds on security problems of VE enterprises and proposed solutions for having secure VEs in the real world. The goal of this paper is focusing on security problem of VEs. As a matter of fact in this paper we want to define different dimensions of security problem in a VE such as data access control and communication in VE and then discuss about methods and technologies that can be used for solving these problems. Describing VEs' security importance, challenges and solutions can help us to design a more efficient security agent for VEs and because of that we should recognize and analyze the security problem in VEs to be able to create an efficient security agent for VEs. In this paper we talk about VE concept in section 2 to understanding VE structure exactly. Then we illustrate the problems that a VE may meet them in its life cycle and some solutions for eliminating these problems in section 3.

2 The Concept of Virtual Enterprise

The research area in VE become a growing one, which any day that is coming, we can see a new advance in this area. So, we should have an exact definition of the concept for speaking about the security problems of VE and its solutions.

VE is a network of enterprises that constitute a temporary alliance, in order to share their costs, skills, and resources, in supporting the necessary activities towards the exploitation of fast-changing opportunities for product or service requests and competitiveness in a global market.[4]

Each enterprise that participates in VE called a partner of VE. The partners work together to obtain a set of goals, so VE is a team of partners that have common goals and are committed to fulfilling some goals. The VE does not exist in the physical environment but only on an electronic network.

The company that establishes a VE and then forms it is called VE initiator. This partner will have a major role in the lifecycle of VE. All of communications and collaborations of VE partners may occur around this entity. Also this entity will manage partners' activities to achieve VE goals. The VE initiator will select the appropriate autonomous partners from which that are interested in participation according to their goals, intentions, and capabilities. The main task of VE that should be accomplished partitioned into several subtasks, according to various capabilities and skills of autonomous partners. These partners are called the virtual groups.

VE partners' activities are depended to each other. This dependency may observe in different dimensions in a VE lifecycle such as task dependency, resource dependency and goal dependency. In a goal dependency, a partner depends on another to make a condition come true; in a task dependency, a partner depends on another to perform an activity; In a resource dependency, a partner depends on another for the availability of an entity.[5]

Because of this dependency in partners' activities, they should have rigid communications to fulfilling their needs such as task coordination and information interchange between themselves. Internet technology and the evolving standards for interoperability are important technologies that support the communication in a VE operation. Although communications can occur on other networks, but most of VEs use internet for their communications. Partners use internet for create relationship and communicate with other, project data interchange to achieve VE final goal. Because VE partners are from different locations and they do not aggregate in one physical place, so network structure will have important role in VEs creation and operation. We show VE activities in a simple model in Fig 1. In this model is supposed that VE has four partners and they communicate and collaborate with each other across internet network.

Although this model is so simple and many dimensions of VE is not considered, but we can see the most principal features and the activities that are done in a VE. Also we can distinguish some security problems in this model. We will describe these problems in the next section.

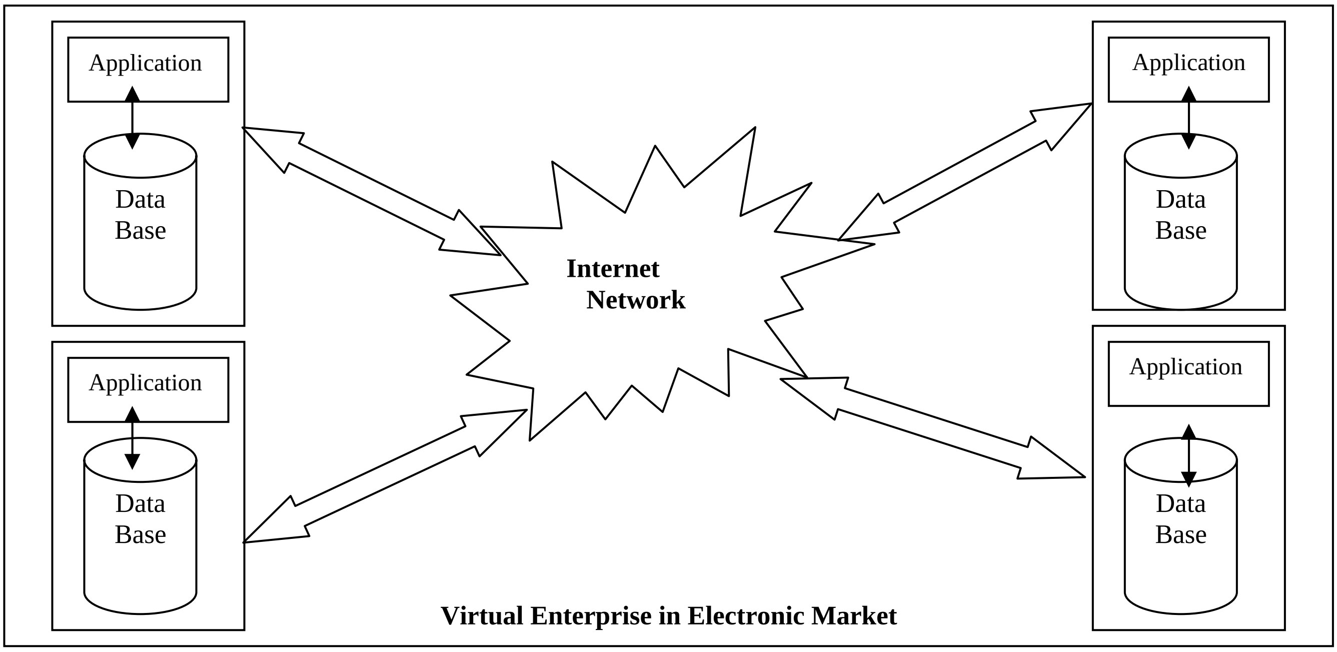

Fig 1. VE activities model

3 VE Security Problem

In last section, we described a model that shows how a VE works. In this model we can understand how partners of a VE can work together to achieving some goals. If we look abstractly and theoretically to this model, it does not have any problem for being active in an electronic market. But this is not true when we come to practical and actual phase. We may meet different problems such as infrastructure, administrative and security problems. The enterprises in a VE require both secure and flexible collaboration between unrelated information systems.[6] So discussion about the security problems, defining different dimensions of this problems and presenting some alternatives for them are essential topics for having more effective VE.

Nowadays Information systems security becomes an important topic. Because in recent decades information systems have grown so much and now play a big role in human being life. VEs also are a computer-based and network-based system. So we have such problem in this field too. It means that we should attend carefully to security aspects of VE. Security in VE in PerDiS consists of two parts: data access control and secure communication.[7] In this section, we will describe different security aspects in a VE life cycle.

3.1 Data Access Control

The tasks of VE participants are connected and their activities are depended to each other. Therefore, partners need to aware from other partners advances in their tasks that assigned to them and they need to have their progress report. This means that partners should access to other's assigned tasks progress information. In addition, we know that participants are not located in one place and they may exist in different places of world. Hence, partners should store essential information in databases and share it on network for using other partners. The control on what data to share within the VE and what to keep secret should stay with the participant to increase the level of confidence in and acceptance of the VE system. The participant should determine what kind of data and information system functions to expose to other. But we concerned with some subjects in data access. We will mention them below.

3.1.1 Identification

Identification is the process of distinguishing one user from all others. Over the network, many users can claim that they are valid person to access VE information. So, we should become confident that these claims are true. If we do not check this, invalid user can enter to VE databases and exploit data that he or she should not access to them. In Identification process, we distinguish valid user from invalid users. Then we can be certain that invalid users do not access to VE lifeblood information. In next section, we will describe some solutions for this topic.

3.1.1.1 User-ids

If a user wants to use VE resources, it should be identified. For his or her identification, he needs to use a user-ID. User-IDs and associated passwords for authentication are low-priced and greatly integrated into today's systems.

3.1.1.2 Proprietary Tokens

Tokens are physical cards similar to credit cards that work in conjunction with a user-ID to identify a user to the system. They combine something a person knows, such as a password with something they own, a token card. Token cards commonly generate either dynamic passwords or a response in a challenge-response communication between the user and the system. Tokens are commonly used for secure remote access where high levels of security are required.

3.1.1.4 Face Geometry

Face geometry uses a standard video camera to capture facial images. The system extracts features that do not easily change, such as the geometry of the eyes and nose, from the images. The template created is matched against real-time images. People do change, and facial hair, positioning and glasses can affect accuracy. Face geometry is less accurate than fingerprint biometrics.

3.1.1.5 Fingerprint Biometrics

Fingerprints have traditionally been used as an identification tool in law enforcement. Fingerprint recognition systems convert a scanned image of a fingerprint into a mathematical representation of the features. The main strengths of fingerprint recognition are its long history, the variability in fingerprints, and ease of use, cost and accuracy. Additionally it has the potential to be integrated into inexpensive devices such as smart cards and keyboards. A disadvantage may be its social acceptability due to its association with illegal activities.

3.1.1.6 Voice Biometrics

Voice biometrics is based on distinguishing the sound of a human voice based on the resonance of the human vocal tract. It is different from voice recognition, which is recognizing spoken commands or words. The system is trained by repeating a phrase that will be used as an access code. One shortcoming of voice biometrics is false rejects that deny a legitimate user access. This is due to medium to low accuracy rates and dependence on the type of equipment used. It may be suitable for outdoor situations and telephone access.

3.1.1.7 Signature Recognition

Signature verification depends on the rhythm, relative trajectories, speed, and number of pen touches. It measures the method of signing instead of the finished signature and, therefore is different from the comparison of a signature. A pen-based computer or digitizing pad is required for signature capture during enrollment and during verification. It has a relatively low level of accuracy. It may be acceptable where a history of signature use exists such as retail transactions and document authentication. It has limited uses where a large number of people must be identified in a limited time. It also has the disadvantage of requiring the individual to want to be identified. This limits its use in applications such as welfare or social benefits identification.

3.1.2 Authentication

Authentication is the process of confirming the identity of a user. Authentication answers the question: “Are you who you say you are?” It is the means of establishing and enforcing a user’s rights and privileges to access specific resources.

Partners’ data shared on internet network. So different internet users can access and use this Information. Surely, some of this information is vital for VE and it should be protected from other people access. Because competitors in electronic market can defeat the VE by achieving this information. Therefore, the identity of persons who access to VE partners’ data should be verified to ensure the user is who he or she claims to be. It means that, it should be controlled that specific persons who VE defines, can access to information. It is clear that in cooperation duration in a VE where different companies in VE cooperate, they will usually not be willing to give the other team broad access to their data. We want to describe some techniques that used for having successful authentication in next section.

3.1.2.1 Cryptography

Cryptography is a technology used to protect the confidentiality of information. It forms the basis for ensuring the integrity of information and authentication of users. Cryptography uses algorithms to scramble and unscramble information such that only the holder of a cryptographic ‘key’ can encrypt or decrypt the information. A cryptographic ‘key’ is a string of alphanumeric characters used along with the information as input into a cryptographic algorithm.

3.1.2.2 Public Key / Private Key Technology

Authentication which requires the unique identification of a user is often based on Public/Private Key cryptography. This form of cryptography uses two related keys. Information encrypted with one key can only be decrypted with the other key. The ‘Public’ Key is made openly available in a repository to anyone who wants to communicate with the user in a secure manner. The ‘Private’ Key is kept only by the owner and is never divulged. Since only the Owner has the private key, its use is considered sufficient to uniquely authenticate the owner. A digital signature is an example of a private key being used to verify that the sender (originator of the information) is really who they say they are. One potential use of public key/private key is a taxpayer using their private key to authenticate themselves to a tax department. The tax department recovers the taxpayer ’s information by using the taxpayer’s public key. Since only the taxpayer’s public key can recover what was encrypted with the taxpayer’s private key, the tax department is assured it came from this particular taxpayer.

3.1.2.3 Message Digest

Message digests are used to ensure the integrity of information. Integrity means that information cannot be altered without detection. Information is put through a mathematical ‘hash’ function. This function reduces the information to a small numeric value called a message digest. Even the slightest change to the information would generate a different message digest. To verify information has not been modified, a user applies the same hash function on the suspected information to generate a message digest. If the resulting message digest matches the original message digest, the information has not been changed. One important use of message digests is in digital signatures.

3.1.2.4 Digital Signature

Digital signatures are the equivalent of a handwritten signature in that they tie an Individual to a document. The first step in digitally signing an electronic document is to generate a message digest of the document. The signer encrypts this message digest using the signer’s unique private key. The document and encrypted message digest are sent to one or more recipients. Verifying a digital signature is the reverse process. The recipient generates a message digest from the document. By using the signer’s public key, the recipient can recover the original message digest from the encrypted one. This proves it must have come from the signer since only they have the private key. If the recovered and the generated message digests are equal, the document has not been modified and the sender cannot deny their digital signature. The digital signature, therefore, provides non-repudiation, which means that the sender cannot falsely deny having sent the message.

3.1.3 Authorization

Obviously, VE permit different persons to Access its data with different degrees. In authorization stage VE security System allows the users access in varied degrees to various resources based on the preassigned privileges associated with users' tasks and roles. This means that VE specifies access rights for a user having a specific role in a specific task. In this section we describe methods that can be used in authorization section of a security system for a VE.

3.1.3.1 Cryptography

Documents, communications, and data travel inside and outside the enterprise in electronic form. Electronic information is easy to read, modify or replace without detection. However, in many situations, the confidentiality of the information in transit must be maintained, e.g., taxpayer data, credit card and bank account numbers, and child abuse cases. Information transported across the State’s TCP/IP networks and across the public Internet is passed in clear text. Malicious individuals can intercept, view and modify this information using easily obtained tools. As described in the authentication section above, cryptography is a means to scramble information such that only authorized entities (people or processes) have access to the information. A combination of public key cryptography and secret key cryptography can be used to implement authenticated and protected communication for secure access control. Most bulk encryption of information involves the use of secret key cryptography.

3.2 Communications

Due to geographical distribution in VE Partners locations, Communications among VE partners are essential and they are forced to exchange information with each other. As the matter of fact without communication, each partner will become a separate entity, which works for itself and this is inconsistent with VE definition. Therefore, partners need to communicate with one another. To achieve the agile manufacturing VE visions, ubiquitous communication and information are the entral, critical, and fundamental parts of the technical elements.

In global VE, with no doubt, communication platforms do play a much more important role. Some techniques like Email or video conferencing facilities allow for globally distributed cooperative working and for a good cooperation, access to others and information are crucial. As we discussed in section 2, the internet network infrastructure usually used for connecting partners of VE from Different places. As the network communications are transported over a public infrastructure, everyone, except for the entities of the VE, must be prevented from understanding the communications contents of VE entities. VE should prevent unauthorized access to data and information transported across networks between partners.

The balance between awareness and privacy may be very delicate: While a VE team member might want to see what someone else has done the other person might not want to give this information away. Here, the groupware system must be able to handle different adjustments of awareness and privacy to allow for the support of an adequate level of trust between different teams and team members in a VE. This means that, although partners should have the capability of awareness of each other work progress, but VE software system should not permit other entities to access to this information. Indeed the counter part of awareness in the discussion of computer supported cooperative work is privacy. Similar to the ways people protect their privacy in paper based work settings there need to be ways for computer supported team members to protect their privacy. In the next sections we will illustrate some technologies that can be used for have secure communication in VE activities.

3.2.1 Firewalls

Firewalls are a common term for physical devices, software and network architectures designed to block or filter access between a private network and a public network such as the Internet. They can also be used to provide access control between separate internal networks. Firewalls enforce the enterprise’s security policy at determined perimeters, e.g., access point to the public Internet. To be effective, each must provide the single point of access to and from an untrusted network. Firewall technology is rapidly evolving. There are two basic types of firewalls, Packet Filtering and Application Gateways (proxy servers). The network architecture and location of firewalls relative to internal networks is an important consideration in securing internal networks. Packet Filtering firewalls filter access at the packet level. By examining the contents of packets, they permit or deny access based on a defined access control policy. Packet filtering firewalls operate alow the application and typically do not have access to information particular to an application. Application level firewalls or proxy servers protect internal networks by not permitting direct access from the internal network to untrusted networks such as the public Internet. Internal users connect to the 'proxy' which then acts on their behalf, completing the connection to the requested external service.

3.2.2 Virtual Private Networks (VPNs)

Virtual private networks are ways of connecting two networks over insecure networks such as the public Internet. A VPN establishes a secure link by using a version of the IPsec security protocol. These links are typically implemented between firewalls. VPNs today often use proprietary record structures and have inter-operability problems. A secure communications link between the networks does not ensure that communications beyond that link are secure. Some VPNs use a variety of non-IPsec protocols. These include PPTP, L2TP and L2F and proprietary protocols. These protocols offer similar services but are better suited to remote access applications and non-IP traffic across the public Internet. These protocols have their uses but are not covered in this document.

4 Conclusions

Security of VEs is so significant for having a productive economical entity. The most important challenges in VEs security topic are data access control and VE participants' communications over internet network. If we do not attend to these topics carefully in VE creation and operation, we will not have an effective VE. There are some technologies that we can use to have a secure VE in electronic market. In different phases of VE life cycle, VE initiator and creator should use these technologies to eliminate security problems.

5 References

[1] Fischer.K., Muller.J. P, Heimig.I, Scheer.A., Intelligent Agents in Virtual Enterprises, *Proc. Of the First International Conference and Exhibition on the Practical Applications of Intelligent Agents and Multi-Agent Technology*, 1996.

[2] Childe, S. J., The Extended Enterprise – a Concept of Co-operation, *Production Planning & Control, Vol. 9, No. 3, p. 320-327*, 1998.

[3] The NIIIP Reference Architecture, *www.niiip.org*, 1996.

[4]Afsarmanesh.H,arita.C.,Hertzberger.L.O,Santos-Silva.V., Management of distributed information in virtual enterprises–the prudent approach, *4th International Conference on Concurrent Enterprising*, 1997.

[5] Eric.Yu, Modelling Strategic Relationships for Process Reengineering, *Ph.D. thesis. Dept. of Computer Science, University of Toronto*, 1995.

[6] Coetzee M., Elofff J. H. P., Virtual Enterprise Access control Requirements, *Proc. of the annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology*, 2003.

[7] Coulouris G., Dollimore J., Roberts M., *SecurityServices Design. PerDiS deliverable PDS-R-97.URL.http://www.perdis.esprit.ecorg/deliverables/docs/T.D.1.1/A/T.D.1.1- A.htm*,1997.