Security Modelling for Integrated Information Systems over the Internet

Jianming Yong
University of Southern Queensland

Security Modelling for Integrated Information Systems over the Internet

Jianming Yong
Department of Information Systems
Faculty of Business
University of Southern Queensland
Email: yongj@usq.edu.au

Abstract

This paper provides a proof of concept for a security modelling framework to manage the complexity of security access control in integrated systems that are emerging due to the connectivity of the Internet. We outline a series of matrices which provide a means to conceptually define and manage all of the various security relationships that arise in an integrated set of systems. The security framework for integrated systems consists of two tiers. Tier 1 is in charge of local systems. Tier 2 is in charge of overall security of an integrated system. Then an extended tier, Tier 3, is deduced. Tier 3 is in charge of all over the Internet. By implementing this extended three-tier security architecture, all relevant systems security is enforced.

Keywords: Information systems, Security Modelling, Access control, Internet, Security Matrices

1. Introduction

The impact of the Internet on the organisations in the modern economies is significant. The networked knowledge-based economy has meant that the organisations have opened their information systems up to the outside world to facilitate the exchange of information and business transaction processing in real time. Systems integration over the Internet is becoming increasingly important for industry specific applications such as supply chain management (SCM), customer relationship management (CRM), procurement and the need for business partners to access and exchange information between ERP (Enterprise Resource Planning) systems. Therefore it is not surprising that system integration (Hearst 1988; Bolcer and Taylor 1996; Hasselbring 2000; Ball, Ma et al. 2002), including data integration (Yong and Yang 2003), tool integration (Yong and Yang 2003), and process integration (Yong and Yang 2001), has become a hot research topic.

However, little practical research has been conducted on security issues raised by systems integration over the Internet. In particular, one aspect of systems security, ‘access control’, which is a relatively simple function to administer for a single system, becomes incredibly complex to administer when beginning to integrate systems over the Internet. As we all know that it is relatively easy to define secure access control for an individual computer or even a simple computer system. For example, a computer can easily be set up to control the access based on user’s name and password. For a simple system, users can be divided into different groups and different groups will have different access privileges. However for a complex integrated system, especially one connected by the Internet, it is not easy to manage its secure access control across a range of potentially dispersed systems. At the same time, because integrated systems are being used to conduct significant business activities over the Internet, security has become a priority.

The structure of this paper is as follows: In Section 2, 20 top Internet-based security vulnerabilities are introduced. In Section 3, traditional access control mechanisms are addressed. In Section 4, the new access requirements are addressed for integrated systems. In Section 5, detailed security matrices for access control are presented. In Section 6, a new security framework for access control is illustrated. In Section 7, an extended three-tier framework is deduced for all Internet-based systems. In Section 8, conclusions are drawn.

2. Top 20 Internet Security Vulnerabilities

It is common that most computers, which connect to the Internet, run either Microsoft Windows or Unix/Linux. It is important to know the vulnerabilities for Windows and Unix/Linux respectively. The next two subsections briefly introduce top ten vulnerabilities for Windows and top ten vulnerabilities for Unix/Linux separately. The details appear at SANS's top twenty vulnerabilities(SANS 2004)

2.1 Top Ten Unix/Linux Vulnerabilities

This section addresses the top ten vulnerabilities for Unix/ Linux systems.

1. DNS (Domain Name Service): DNS is a system which allows the conversion of hostnames (e.g. www.usq.edu.au) into the registered IP addresses. This vulnerability is mostly caused by a software package, Called BIND (Berkeley Internet Name Domain). The ubiquity and critical nature of BIND has made it a frequent target for attackers to launch a DoS (Denial of Service) attack or other malicious activities.
2. RPC (Remote Procedure Calls): RPCs allow programs on one computer to execute procedures on another computer by passing data and retrieving the results. Because these RPC services can execute with elevated privileges that lead to a vulnerability for an attacker to launch malicious activities in other computers.
3. Apache web server: An Apache server is used to provide the web service to all web browsers. All potential vulnerabilities (e.g. SQL, CGI, PHP, etc.) are exposed to the outside through the web server.
4. General Unix/Linux authentication accounts with no passwords or weak passwords: All the usages of Unix/Linux systems are related to passwords. Any accounts with on passwords or weak passwords will become a potential security hole for that system. Thus a good password policy needs to be implemented to minimize system vulnerabilities.
5. Clear text services: Because Unix/Linux systems use plain text to conduct network services; it allows everybody who is sniffing network to gain access to either communication contents and/or authentication credentials.
6. Sendmail: Sendmail is the program that sends, receives, and forwards most electronic mail processed on Unix/Linux systems. Sendmail is one of the most popular mail transfer agent and its widespread use on the Internet has made it a prime target of attackers.
7. SNMP (Simple Network Management Protocol): SNMP is used to monitor and configure almost all types of TCP/IP-enabled devices. SNMP communication consists of different types of exchange management messages, which leave significant vulnerabilities when these messages are handled.
8. SSH (Secure Shell): SSH is a popular service for securing logins, command execution, and file transfers across a network. It allows an attacker to exploit holes to obtain root access on a vulnerable computer.
9. Misconfiguration of enterprise services NIS/NFS: NIS and NFS are the network file system and network information service. They are two important services used in Unix networks. The security problems with NIS/NFS are related to buffer overflows, DoS and weak authentication.

10. Open SSL (Secure Sockets Layer): The Open-source OpenSSL library is a popular package to add cryptographic security to applications that communicate over the network. Because OpenSSL is used by most programs/applications for security concerns. Thus if OpenSSL has any vulnerabilities, the attackers will use them to attack the programs/applications which rely on OpenSSL.

2.2 Top Ten Windows Vulnerabilities

This section lists the top ten vulnerabilities for Windows.

1. IIS (Internet Information Services): IIS has similar functions as the Apache server of Unix/Linux. Through the web server, the attackers can launch different attacks, such as denial of service, exposure or compromise of sensitive files or data, execution of arbitrary commands, complete compromise of the server, etc.
2. MSSQL (Microsoft SQL Server): MSSQL contains several serious vulnerabilities that allow remote attackers to obtain sensitive information, alter database content, compromise SQL servers, and, in some configurations, compromise server hosts.
3. Windows authentication: this is more related to password vulnerabilities. Although Microsoft Windows does not store or transmit passwords in clear text – it uses a hash of password for authentication. The mathematical algorithms which are used by Windows can be cracked down by attackers through brute-force or social engineering. Then it becomes a security hole.
4. IE (Internet Explorer): Microsoft IE is the default we browser installed on Microsoft Windows platforms. All existing versions of IE have critical vulnerabilities if they are not kept up-to-date with current patches. The attackers can use IE to takeover the vulnerable system.
5. Windows remote access services: Like NETBIOS network shares, anonymous logon null sessions, remote registry access, and remote procedure calls, these items make up a large share of the more common network level exploits on windows. The attackers can use these items to obtain access to vulnerable computers.
6. MDAC (Microsoft Data Access Components): MDAC can bring vulnerabilities to Windows platform computer through database components to run malicious commands and code on attacked computers.
7. WSH (Windows Scripting Host): WSH is a Microsoft technology that serves to extend the functionality of Windows, supporting both JavaScript and Visual Basic Script. WSH will affect vulnerable computers via web components (e.g. IE) to control Windows operating systems.
8. Microsoft Outlook and Outlook Express: Outlook and Outlook Express will leave vulnerabilities over their mail server and client. This gives the attackers to spread e-mail viruses, worms, malicious code to compromise the local system.
9. P2P (Windows Peer-to-Peer files sharing): P2P file sharing system are used extensively by a rapidly growing user based. These applications are used to download and distribute different types of data (e.g. video, audio, graphics, and proprietary information). P2P communication consists of requests, replies, and file transfers, which bring relevant systems vulnerabilities.
10. SNMP: this vulnerability is the same as the Unix/Linux. After the vulnerabilities of SNMP are found, the attackers can use them to attach relevant network devices, computers, and their operating platforms.

3. Access Control in Systems Security

From previous section, the top twenty vulnerabilities have brought a big trouble to the Internet and its applications. Through a careful analysis, we found most of the top twenty vulnerabilities can be controlled by implementing an effective access control policy.

Traditionally Role-based Access Control (RBAC) is frequently used by many organisations to implement their security strategy. Bacon, Moody and Yao (2002) has described a model of RBAC by OASIS(Organisation for the Advancement of Structured Information Standards). OASIS published a role-based access control architecture for achieving secure interoperation of services in an open, distributed environment; the aim of OASIS is to allow autonomous management domains to specify their own access control policies and to interoperate subject to service level agreements. Services define roles and implement formally specified policy to control role activation and service use; users must present the required credentials, in an appropriate context, in order to activate a role or invoke a service. All privileges are derived from roles, which are activated for the duration of a session only. In addition, a role is deactivated immediately if any of the conditions of the membership rule associated with its activation becomes false. These conditions can test the context, thus ensuring active monitoring of security. To support the management of privileges, OASIS introduces appointment. Users in certain roles are authorized to issue other users with appointment certificates, which may be a prerequisite for activating one or more roles. The conditions for activating a role at a service may include appointment certificates as well as prerequisite roles and constrains on the context. An appointment certificate does not therefore convey privileges directly but can be used as a credential for role activation. Role-based access control, in associating privileges with roles, provides a means of expressing access control that is scalable to large numbers of principals.

Other access control methods include Temporal Role-based access control (TRBAC)(Bertino, Bettini et al. 2000), Team-based Access Control (TBAC) (Georgiadis, Mavridis et al. 2001), Generalized Role-based Access Control (GRBAC) (Covington, Moyer et al. 2000). TRBAC introduces periodic activation and deactivation, and role triggers for expressing temporal dependencies. Periodic activation and deactivation support time-limited authorization. TMAC is directly associated with a team, which is a group of users in specific roles, collaboratively working on a common task, the privileges that a user has are determined by his/her current team. GRBAC extends traditional RBAC by introducing object roles and environment roles in addition to subject roles. An object role represents a facet of the requested object. These roles are activated automatically by the system. The access control only can satisfy the classification of users and services statically. When integration of heterogeneous systems is required, how can the access control policies be achieved actively? This issue is discussed in later sections.

4. The New Access Control Requirements for Integrated Systems

Before integration of a set of potentially quite different systems in terms of users needs and security, the access control requirements for users that will need to access other individual systems within the set of integrated systems needs to be established. It is important to establish the desired level of access control for each system for individual users. Otherwise, in large set of integrated systems, the number of individual users could be exponentially quite large resulting in performance issues. An in-depth requirements analysis of user access needs in the integrated set of systems is required. This will allow the systems administrator to determine the access rights for each individual in the integrated system. An integrated system will consist of a large number of individual systems, which actually implement their own access control policies separately. After integration, some systems might need to access other systems for cooperation, which requires a mechanism to look after all individual systems as a whole to ensure the system security. Some research has addressed aspects of these requirements. Riet & Janssen (Riet, Janssen et al. 1998)identified database security from database systems to ERP systems,. Olivier (Olivier, Riet et al. 1998) addressed application-level security for workflow systems, and Soshi & Maekawa(Soshi and Maekawa 1997) dealt with security architecture for open distributed systems. They all discussed security issues from certain aspects of system integration, but they did not deal with the overall requirements from the perspective of system integration. In particular, none addressed access control for an integrated system. Following sections will address how that mechanism can be achieved and provide a proof of concept.

5. Security Modelling Matrices for Integrated Systems

Assume there are n systems, which will be integrated. We represent these systems as S1, S2, S3, …, Sn. S1has n_1 internal users, m_1 groups and p_1 privileges. S2 has n_2 internal users, m_2 groups and p_2 privileges. S3 has n_3 internal users, m_3 groups and p_3 privileges. Sn has nn internal users, g_n groups and p_n privileges. Now for the integrated system, the number of internal users is a sum of all respective systems' internal user number: $n_1+n_2+n_3+\ldots+n_n$.

What privileges should the integrated system have? It is obvious that all the privileges in the individual system should be included in the integrated system. Thus for the integrated system, privileges P will be defined as:

$$P= \bigcup Pi \quad 1<=i<=n \qquad \text{Pi represents the privileges of individual system i.}$$

Next design different groups for the integrated system. Each group will be assigned relative privileges from P. These groups will operate all the individual systems in the same way. If a user belongs to one of these groups, then the user can get all privileges, which that group has been given, to operate on all available resources within the integrated system. For example, suppose there is a group which is responsible for web services. Now assume there are several users in this group. This group will have all authorities to operate on any web servers within an integrated system. Now any user from this group can operate on any web server within the integrated system. From this example, we can know that these groups exist beyond an individual system.

In other words, there is a need to know how integrated system security policies effectively cooperate with all previous individual security policies. The following security model for system integration is proposed: Two-tier security architecture for a large integrated system to enhance its overall security.

5.1 Tier 2 Security of the Integrated Systems

Tier 2 is concerned with the integrated system which has an overall security view for all integrated systems. The relationships of security elements in the integrated system are as follows (Yong, Lane et al. 2003).

Relationship 1 (R1), for users and systems, express this relationship as R1(U×S). U is a set of all the users, U1,U2, …, Un, in the integrated system. S is a set of individual autonomous systems, S1, S2, S3, …, Sn. Ui is a set of users in autonomous Si, while 1<=i<=n.

Relationship 2 (R1), for groups and systems, express this relationship as R2 (G×S). G is a set of all the groups,G1, G2, G3, …, Gn, in the integration system. S is a set of individual autonomous systems, S1, S2, S3, …, Sn. Gi is a set of groups in system Si, while 1<=i<=n.

Relationship 3 (R3), for privileges and users, express this relationship as R3(P×U). P is a set of all the privileges, P1, P2, P3, …, Pn, in the integrated system. U is a set of all the users in the integrated system. Pi is a set of the privileges in autonomous system Si, while 1<=i<=n.

Relationship 4 (R4), for privileges and groups, express this relationship as R4(P×G). P is a set of all the privileges in the integrated system. G is a set of all the groups in the integration system.

Relationship 5 (R5), for groups and users, express this relationship as R5(G×U). G is a set of all the groups in the integration system. U is a set of all the users in the integrated system.

Relationship 6 (R6), for privileges and systems, express this relationship as R6(P×S). P is a set of all the privileges in the integrated system. S is a set of individual autonomous systems.

Next the relationships R1, R2, R3, R4, R5, and R6 and their contribution to the overall security concerns for the integrated system are analysed.

R1 is used to express the relationship with all the users within the integrated system and all the individual autonomous systems. The following matrix (Figure 1) illustrates the number of users and autonomous individual systems.

$$\begin{array}{cc} & \mathbf{S1\ \ S2\ \ S3\ \ S4\ \ S5\ \ S6\ \ldots\ldots\ldots\ \ Sn} \\ \begin{array}{c} \mathbf{U1} \\ \mathbf{U2} \\ \mathbf{U3} \\ \mathbf{U4} \\ \mathbf{U5} \\ \mathbf{U6} \\ \mathbf{..} \\ \mathbf{Un} \end{array} & \begin{pmatrix} N_{11}N_{12}N_{13}N_{14}N_{15}N_{16}\ldots\ldots\ldots\ldots N_{1n} \\ N_{21}N_{22}N_{23}N_{24}N_{25}N_{26}\ldots\ldots\ldots\ldots N_{2n} \\ N_{31}N_{32}N_{33}N_{34}N_{35}N_{36}\ldots\ldots\ldots\ldots N_{3n} \\ N_{41}N_{42}N_{43}N_{44}N_{45}N_{46}\ldots\ldots\ldots\ldots N_{4n} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ N_{n1}N_{n2}N_{n3}N_{n4}N_{n5}N_{n6}\ldots\ldots\ldots\ldots N_{nn} \end{pmatrix} \end{array}$$

Figure 1 Matrix R1 presents the number of users and autonomous individual systems

The value of Nkj is the number of users of Uj who become legal users of Sk through system integration.

From this matrix, the exact number of users for the overall system and all individual systems is available. It is very useful for each individual system to know its legal users after system integration and to provide the secure access for these users. From this matrix, we know the integrated system has the following number of users:

$$\text{Total user number (Tu)=} \sum_{i=1}^{n} Nii$$

Actually Nii is the original number of users of Si before system integration. Now the exact number of users for each individual autonomous system after system integration can be calculated. Ni is the number of users of Si after system integration. The following equation gives the number of users for any individual system.

$$\text{Ni=} \sum_{j=1}^{n} Nji \qquad (1 \le i \le n)$$

Now a new access control table for each individual autonomous system over the whole integrated system is available. When any user wants to access an individual system, if the user is not an original user of this system, this system will send a request to consult this outside access control table; if the user is listed in this outside access table, then the user can access this system and use its authorised resources. Otherwise the user will be denied access to this system.

R2 is the relationship between all the groups within the integrated system and all the individual autonomous systems. This relationship can be expressed by a matrix similar to R1. From this matrix (Figure 2), there follows two equations:
the number groups of the integrated system

$$\text{Total group number (Tg)=} \sum_{i=1}^{n} Mii$$

Any individual autonomous (Si) system will have the following number (Mi) of groups after the system integration.

$$\text{Mi=}\sum_{j=1}^{n} Mji \qquad (1 \le i \le n)$$

Based on this matrix, an access control table for the whole integrated system can be established. At the same time any individual autonomous system will have an expanded access control table to control group access especially for groups which are not its original groups.

$$\begin{array}{c|ccccccc|}
 & \mathbf{S1} & \mathbf{S2} & \mathbf{S3} & \mathbf{S4} & \mathbf{S5} & \mathbf{S6}\ldots\ldots & \ldots\mathbf{Sn} \\
\mathbf{G1} & M_{11} & M_{12} & M_{13} & M_{14} & M_{15} & M_{16}\ldots\ldots\ldots\ldots & M_{1n} \\
\mathbf{G2} & M_{21} & M_{22} & M_{23} & M_{24} & M_{25} & M_{26}\ldots\ldots\ldots\ldots & M_{2n} \\
\mathbf{G3} & M_{31} & M_{32} & M_{33} & M_{34} & M_{35} & M_{36}\ldots\ldots\ldots\ldots & M_{3n} \\
\mathbf{G4} & M_{41} & M_{42} & M_{43} & M_{44} & M_{45} & M_{46}\ldots\ldots\ldots\ldots & M_{4n} \\
\mathbf{G5} & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots \\
\mathbf{G6.} & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots \\
 & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots \\
\mathbf{Gn} & M_{n1} & M_{n2} & M_{n3} & M_{n4} & M_{n5} & M_{n6}\ldots\ldots\ldots\ldots & M_{nn}
\end{array}$$

Figure 2 Matrix R2 is the number of groups for the integrated systems

The value of Mkj is the number of groups of Gj who become legal groups of Sk through system integration.

R3 is the relation of privileges and users from an individual autonomous system. The following matrix (Figure 3) can be used to illustrate the relationship.

$$\begin{array}{c|cccccccc|}
 & \mathbf{U1} & \mathbf{U2} & \mathbf{U3} & \mathbf{U4} & \mathbf{U5} & \mathbf{U6} & \ldots\ldots & \ldots\mathbf{Un} \\
\mathbf{P1} & W_{11} & W_{12} & W_{13} & W_{14} & W_{15} & W_{16} & \ldots\ldots\ldots\ldots & W_{1n} \\
\mathbf{P2} & W_{21} & W_{22} & W_{23} & W_{24} & W_{25} & W_{26} & \ldots\ldots\ldots\ldots & W_{2n} \\
\mathbf{P3} & W_{31} & W_{32} & W_{33} & W_{34} & W_{35} & W_{36} & \ldots\ldots\ldots\ldots & W_{3n} \\
\mathbf{P4} & W_{41} & W_{42} & W_{43} & W_{44} & W_{45} & W_{46} & \ldots\ldots\ldots\ldots & W_{4n} \\
\mathbf{P5} & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\ldots\ldots\ldots & \ldots \\
\mathbf{P6} & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\ldots\ldots\ldots & \ldots \\
 & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\ldots\ldots\ldots & \ldots \\
\mathbf{Pn} & W_{n1} & W_{n2} & W_{n3} & W_{n4} & W_{n5} & W_{n6} & \ldots\ldots\ldots\ldots & W_{nn}
\end{array}$$

Figure 3 Matrix R3 is the relation of privileges and users from a whole individual autonomous system

Based on this relationship, *Wij* is 0 or 1 in this matrix, if *Wij* =0, then all the privileges (Pi) from the ith autonomous system (Si) can not apply to any of the users from the jth autonomous system (Sj). If *Wij* =1, then all the privileges (Pi) from the ith autonomous system (Si) can apply to all the users from the jth autonomous system (Sj). From this matrix, it is obvious that *Wij* =1 (1<=i<=n). Based on this matrix, one autonomous system's privileges can be obtained by all the users from another autonomous system. Furthermore a matrix can be expanded to include all of the privileges and all the users in the integrated system.

R4 is the relationship between the privileges and groups. It can be expressed by a matrix (Figure 4), which is quite similar to R3. The matrix is as follows.

$$\begin{array}{c|cccccccc|}
 & g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & \ldots\ldots\ldots & g_{Tg} \\
\mathbf{P1} & V_{11} & V_{12} & V_{13} & V_{14} & V_{15} & V_{16} & \ldots\ldots\ldots\ldots & V_{1Tg} \\
\mathbf{P2} & V_{21} & V_{22} & V_{23} & V_{24} & V_{25} & V_{26} & \ldots\ldots\ldots\ldots & V_{2Tg} \\
\mathbf{P3} & V_{31} & V_{32} & V_{33} & V_{34} & V_{35} & V_{36} & \ldots\ldots\ldots\ldots & V_{3Tg} \\
\mathbf{P4} & V_{41} & V_{42} & V_{43} & V_{44} & V_{45} & V_{46} & \ldots\ldots\ldots\ldots & V_{4Tg} \\
\mathbf{P5} & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\ldots\ldots\ldots & \ldots \\
\mathbf{P6} & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\ldots\ldots\ldots & \ldots \\
\mathbf{.} & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\ldots\ldots\ldots & \ldots \\
\mathbf{Pn} & V_{n1} & V_{n2} & V_{n3} & V_{n4} & V_{n5} & V_{n6} & \ldots\ldots\ldots\ldots & V_{nTg}
\end{array}$$

Figure 4 Matrix R4 is the relationship between the privileges and groups

Tg is the total number of groups in the integrated system. If Vij (1<=i<=n & 1<=j<=Tg)=0, the jth group can not obtain all of the privileges which the ith system has. If Vij=1, the jth group gets all the privileges which the ith system has. This matrix can be used to implement the group access within the integrated system.

R5 is the relationship between all the users and all the groups in the integrated system. The following matrix (Figure 5) is a representation.

$$\begin{array}{cc}
 & g_1\; g_2\; g_3\; g_4\; g_5\; g_6\;\ldots\ldots\ldots\ldots g_{Tg} \\
\begin{matrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \\ u_6 \\ . \\ . \\ . \\ u_{Tu} \end{matrix} &
\begin{pmatrix}
V_{11}V_{12}V_{13}V_{14}V_{15}V_{16}\ldots\ldots\ldots\ldots\ldots V_{1Tg} \\
V_{21}V_{22}V_{23}V_{24}V_{25}V_{26}\ldots\ldots\ldots\ldots\ldots V_{2Tg} \\
V_{31}V_{32}V_{33}V_{34}V_{35}V_{36}\ldots\ldots\ldots\ldots\ldots V_{3Tg} \\
V_{41}V_{42}V_{43}V_{44}V_{45}V_{46}\ldots\ldots\ldots\ldots\ldots V_{4Tg} \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
V_{Tu1}V_{Tu2}V_{Tu3}V_{Tu4}V_{Tu5}V_{Tu6}\ldots\ldots\ldots\ldots V_{TuTg}
\end{pmatrix}
\end{array}$$

Figure 5 Matrix R5 is the relationship between all the users and all the groups in the integrated system

If Vij (1<=i<=Tu & 1<=j<=Tg)=0, the jth group does not include the ith user as its member. If Vij = 1, the jth group includes the ith user as its member. The matrix gives exact members for each group. All the privileges which a group has will automatically be given to all its members.

R6 is the relationship between the privileges and individual autonomous systems. It can be represented by the following matrix (Figure 6).

$$\begin{array}{cc}
 & \mathbf{S1\;\; S2\;\; S3\;\; S4\;\; S5\;\; S6\;\ldots\ldots\ldots\; Sn} \\
\begin{matrix} \mathbf{P1} \\ \mathbf{P2} \\ \mathbf{P3} \\ \mathbf{P4} \\ \mathbf{P5} \\ \mathbf{P6} \\ \\ . \\ \mathbf{Pn} \end{matrix} &
\begin{pmatrix}
X_{11}X_{12}X_{13}X_{14}X_{15}X_{16}\ldots\ldots\ldots\ldots\ldots X_{1n} \\
X_{21}X_{22}X_{23}X_{24}X_{25}X_{26}\ldots\ldots\ldots\ldots\ldots X_{2n} \\
X_{31}X_{32}X_{33}X_{34}X_{35}X_{36}\ldots\ldots\ldots\ldots\ldots X_{3n} \\
X_{41}X_{42}X_{43}X_{44}X_{45}X_{46}\ldots\ldots\ldots\ldots\ldots X_{4n} \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_{n1}X_{n2}X_{n3}X_{n4}X_{n5}X_{n6}\ldots\ldots\ldots\ldots\ldots X_{nn}
\end{pmatrix}
\end{array}$$

Figure 6 Matrix R6 is the relationship between the privileges and individual autonomous systems

Based on this relationship, X_{ij} equals 0 or 1 in this matrix. If X_{ij}=0, all the privileges (Pi) from the ith autonomous system (Si) cannot apply to the jth autonomous system (Sj). If X_{ij}=1, all the privileges (Pi) from the ith autonomous system (Si) can apply to the jth autonomous system (Sj). From this matrix, it is obvious that X_{ij}=1 (1<=i<=n). Based on this matrix, one autonomous system' privileges can be obtained by another autonomous system. All six relationships (R1, R2, R3, R4, R5, and R6) can operate with each other to form a new control access policy. Sometimes these relationships can be optimized to reduce the overhead on system performance of this security architecture. This issue will be dealt with in future research.

5.2 Tier1 Security of Individual Autonomous System

This tier deals with security policies of individual autonomous systems. Thus different systems will have quite different security policies. These policies are based on various role-based access controls in the internal system. Most individual systems distinguish their legal users or groups by the userIDs/groupIDs as well as the passwords from unauthorised users/groups. In Tier 1, security policies only deal with users, groups and privileges, which are related to defined roles.

6. Two-tier security policy framework for an Integrated System

The security of an integrated system is divided into two tiers. Tier 1 is in charge of individual autonomous systems. Tier 2 is in charge of the whole integrated system. This relationship can be illustrated in Figure 7.

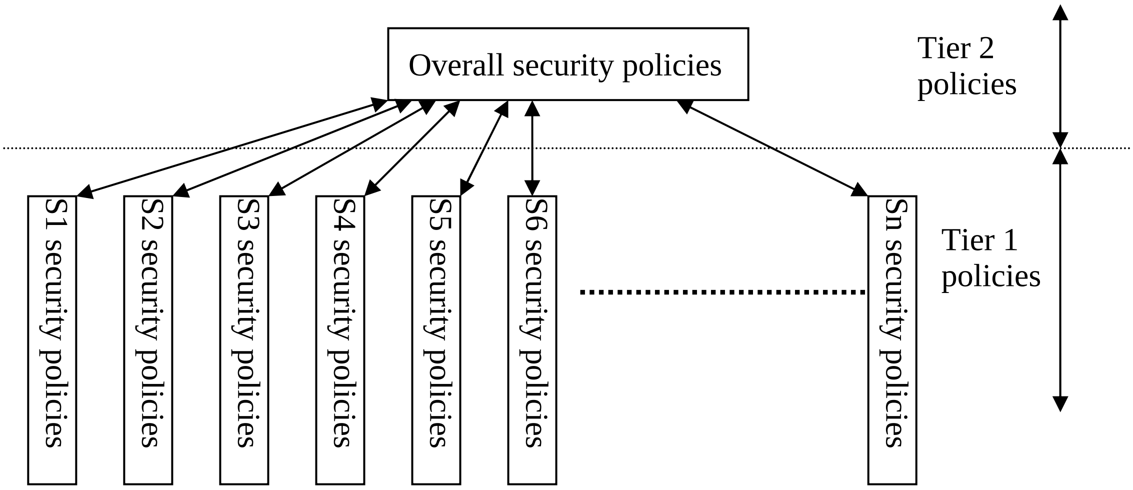

Figure 7 Logical security policies of an integrated system

From Figure 7, security policies can be implemented. First, if a user or a group wants to access any local system (S1, S2, S3, …, Sn), assume it is S1, and also the user or group belongs to S1, then this user or group will only be checked by S1 security policies, which only relate to Tier 2's polices. This is exactly the same as prior to the system integration. Second, suppose, a user or a group belongs to S1, and wants to access any other systems (S2, S3, …, Sn), assume the user or group will access S3. Table 3 shows appropriated steps for this situation:

Table 1 Steps required to determine if an individual system user can access another system within an integrated set of systems using the Tier 2 security architecture

Steps	**Actions**
1	S3 finds that the user or the group is not one of its local users or groups.
2	S3 sends a request to the security server which is in charge of security policies of the

	integrated system. Based on the responses from the security server in Tier 2, S3 will know what privileges can be granted to that user or group.
3	S3 will allow the access to the user or group according to its privileges or reject the access to the user or group because the user or group cannot be authenticated by this higher hierarchical security server, which implements the security policies at Tier 2.

Thus for a whole integrated system, the security policies are divided into Tiers 1 and 2. Sometimes Tier 1 can satisfy the security requirements alone. Sometimes Tier 1 needs the cooperation of Tier 2 to satisfy the security requirements to allow non-local users/groups to access a local system. Through this two tiers' security mechanism, a robust security system has been established for an integrated system so that all the individual autonomous systems cannot only keep their original security properties but also flexibly accept access from outside their integrated business partners.

7. Three-Tier Security Policy for Internet-Based Systems

In the previous two sections, a two-tier framework is well designed to enforce the security of an integrated system from the perspective of access control. After an integrated system is formed, this integrated system will become one part of the Internet. It is necessary to have a clear security policy for the Internet and its integrated subsystems. The overall security policy needs to have three tiers: Tier 1 for each individual local system, Tier 2 for an integrated system, Tier 3 for the Internet as a whole. Figure 8 illustrates this three-tier framework for Internet-based systems.

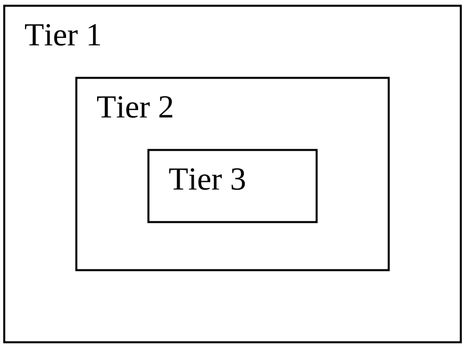

Figure 8 Relationships of three tiers for Internet-based systems

From Figure 8, we should have following expressions for the relationships between Tier1, Tier 2 and Tier 3.

$$Tier3 \subseteq Tier2 \subseteq Tier1$$

It means that all the security policies at Tier 3 should also be considered by and be transferred to Tier 2's security policies, all the security policies at Tier 2 should be considered by and be transferred to Tier 1's security policies. That will ensure all systems (e.g. individual local systems, integrated systems, the Internet as a whole) more secure and have a consistent security policy for all systems. In the previous sections, Tier 3 should cover all the security policies which tackle vulnerabilities of Section 2. Tier 2 should cover all the security policies of Sub-section 5.1. Tier 1 should cover all the security polices of Sub-section 5.2.

8. Conclusions

A mathematical proof of concept for the security requirements of an integrated system has been presented. According to requirements of system integration, it is concluded that six relationships (R1, R2, R3, R4, R5, R6), which correlate all the security requirements of individual autonomous systems (S) in a set of integrated systems, users (U), groups (G), and privileges (P). Based on these six relationships, a two-tiered security architecture for an integrated system is proposed, which can often be a large scale system integrated over the Internet to service the purpose of E-Commerce. This two-tiered security architecture ensures that the overall integrated system has a very reliable security policy and at the same time each individual autonomous system keeps its original security properties to service to its local users/groups but also utilises Tier 2's function to service all others user within the integrated system. Through this combination of tier1 and tier 2, the whole integrated system's security can be effectively implemented and at the same time any individual system's security can also be reinforced. After an integrated system merges into the Internet, an extended three-tier security policy is deduced to make all Internet-based systems more secure.

REFERENCES

Bacon, J., K. Moody, et al. (2002). "A Model of OASIS Role-Based Access Control and its Support for Active Security." *ACM Transactions on Information and System Security* ***5****(4): 492-540.*

Ball, M. O., M. Ma, et al. (2002). "Supply Chain Infrastructures: System Integration and Information Sharing." *ACM SIGMOD Record, SPECIAL ISSUE: Data management issues in electronic commerce* **31**(1): 61-66.

Bertino, E., C. Bettini, et al. (2000). TRBAC: A temporal role-based access control model. 5th *ACM workshop on Role-based Access Control (RBAC'00)*, Berlin, Germany, ACM New York.

Bolcer, G. A. and R. N. Taylor (1996). Endeavors: A Process System Integration Infrastucture. *The Fourth International conference on the Software Process (ICSP '96)*, Brighton, UK, IEEE, pages:76-89.

Covington, M. J., M. J. Moyer, et al. (2000). Generalized role-based access control for future applications, *23rd National Information Systems Security Conference*.

Georgiadis, C., I. Mavridis, et al. (2001). Flexible team-based access control using contexts. *6th ACM symposium on Access Control Models and Technologies*, New York, ACM.

Hasselbring, W. (2000). "Information System Integration." *Communications of the ACM* **45**(6): 32-38.

Hearst, M. A. (1988). "Information Integration." *IEEE Intelligent Systems* **13**(5): 12-24.

Olivier, M. S., R. P. v. d. Riet, et al. (1998). Specifying Application-level Security in Workflow Systems. 9th International Workshop on Database and Expert Systems Applications (DEXA'98), Vienna, Austria, IEEE, pages:346-351.

Riet, R. v. d., W. Janssen, et al. (1998). Security Moving from Database Systems to ERP Systems. *9th International Workshop on Database and Expert Systems Applications (DEXA'98)*, Vienna, Austria, IEEE, pages:273-280.

SANS (2004). Top twenty Internet vulnerabilities. Accessed on 15/01/2004. http://www.sans.org/top20/.

Soshi, M. and M. Maekawa (1997). The Saga Security System: A Security Architecture for Open Distributed Systems. *6th IEEE Workshop on Future Trends of Distributed Computing Systems (FTDCS '97)*, Tunis, TUNISIA, IEEE, pages:53-58.

Yong, J., M. S. Lane, et al. (2003). Enforcing Secure Access Control. *1st Australian Information Security Management Conference (InfoSecurity03)*, Perth, Australia.

Yong, J. and Y. Yang (2001). Modelling and Integration for Internet-based Workflow Systems. *IASTED Int. Conf. on Internet and Multimedia Systems and Applications (IMSA2001)*, Hawaii,USA, pages:345-350.

Yong, J. and Y. Yang (2003). Data Integration over the Internet for E-commerce. *IASTED International Conference on Communications Systems and Applications (CSA'03)*,, Banff, Alberta, Canada, pages:253-258.

Yong, J. and Y. Yang (2003). "A Framework of Tool Integration for Internet-based E-commerce." *Lecture Notes in Computer Science*, **3033**: 271-278.