

A Survey of Database Security Challenges, Issues and Solution

Bhavin Fataniya

M.E(I.T) Student,I.T Department,L.D College of engineering Ahmedabad,Gujarat,India.

ABSTRACT

These days a Database security has turned into a critical issue in specialized world. The fundamental target of database security is to prohibit superfluous data presentation and change information while guaranteeing the accessibility of the required administrations. A quantities of security techniques have been made for ensuring the databases. Numerous security models have been created in view of various security parts of database. These security strategies are valuable just when the database administration framework is composed and creating for ensuring the database. As of late the development of web application with database at its backend Secure Database Management System is more fundamental than just a Secure Database. Consequently this paper feature on the Threats, Security Methods and Vulnerabilities in Database Management System with the assistance of review performed on the field of secure databases.

Keyword: - Database, Security, Encryption, Access Control.

1.INTRODUCTION

These days including the invention of internet technology securing database is a needed aspect in today's world. Individually we use database every day unknowingly when we browse on internet. The information we get on the web page is the consequences of query accomplished by the webpage to the database it is connected. Hence indirectly via the webpage we are connected to different databases. The web pages are open for any anonymous person in the world or we can say the databases are indirectly opened for everyone. As we know data in the database is the most valuable asset which can be the source of information. All the information cannot be revealed for everyone. Hence many security tools have been devised to protect the database. As the database is accessible via web pages security should be implemented in database management system(DBMS).Looking towards the implementation this paper focus on Vulnerabilities in Database Management System, Threats in Database Management System and Security Methods in Database Management System.

1.1 Database Security Properties

As mentioned in [1] a complete solution to data security must fulfilled the following three requirements Confidentiality, Integrity, Availability (CIA): these entire factors can gained in database using following ways:

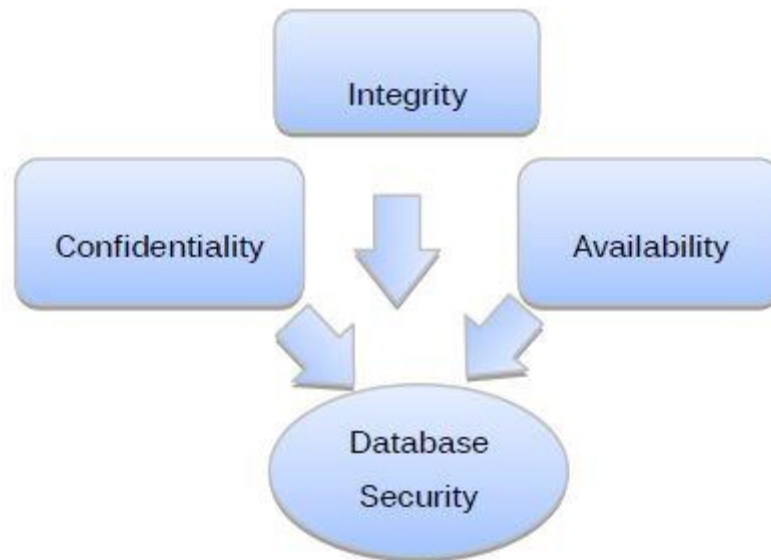


Fig -1: Security Properties

(1) Confidentiality

Means to the protection of data against unauthorized disclosure can be achieved using access control mechanism. It is already further enhanced by the use of encryption techniques is applied to data when being stored on secondary storage or transmitted on a Network.

(2) Integrity

Means to the prevention of unauthorized and improper data modification and can be achieved in combination of access control mechanism by semantic integrity constraints.

(3) Availability

Means to the prevention and recovery from hardware and software errors and from malicious data access denials making the database system inaccessible. The data that are available on the Web can be powered by the use of techniques protecting against denial-of-service attacks and such as the ones based on machine learning techniques.

2. Security Risks to Databases

The initiative database organization is subject to prodigious variety of threats. Some serious threats are envisioned in this document. This list is taken from a white paper presented by Imperva's Application Defense Center. [2]

2.1 Excessive Privilege Abuse

When users are specified with the access rights that allow them to perform other tasks not included in their job, harmful intent can be discovered through such tasks thus leading to misuse of such privileges. When we talk of such abuse, an example of university can be quoted in which an administrator who is given access to all databases and holds the privilege to change the records of any student. This may lead to misuse such as changing of grades, marks of students or change in the amount of fine charged to any student. As a result, all users who perform different tasks are given default level of privileges that grants access in excess.



Fig -2: Security Risks to Databases

2.2 Legitimate Privilege Abuse

Legitimate privilege abuse can be in the form of misuse by database users, administrators or a system manager doing any unlawful or unethical activity. It is, but not limited to, any misuse of sensitive data or unjustified use of privileges.

2.3 Privilege Elevation

Excessive exposure leads to discovery of flaws which is taken advantage of by attackers and may result in the change of privileges e.g. ordinary user given the access of administrative privileges. The loss of which could result in bogus accounts, transfer of funds, misinterpretation of certain sensitive analytical information. Such cases are also found to be in database functions, protocols and even SQL statements.

2.4 Database Platform Vulnerabilities

Vulnerabilities in the previous operating systems such as Windows 98, Windows 2000, etc. may create data loss from a database, data corruption or service denial conditions. For instance, the blaster worm created denial of service conditions from a vulnerability found in Windows 2000.

2.5 SQL Injection

Random SQL queries are executed on server by some spiteful attacker. In this attack SQL statement is followed by a string identifier as an input. That is validated by the server. If it does not get validated it might get executed. Through these unobstructed rights may gain by the attackers to the whole database.

2.6 Weak Audit Trail

A database audit policy ensures automated, timely and proper recording of database transactions. Such a policy should be a part of the database security considerations since all the sensitive database transactions have an automated record and the absence of which poses a serious risk to the organization's databases and may cause instability in operations.

2.7 Denial of Service

It is the attack that prevents the legitimate users of a program/application/data to use or access that specific service. DOS can take place using different technique. Attacker may get access to database and tries to crash the server or resource overloading, network flooding and data corruption can be the techniques for creating conditions of DOS attack. It is a serious threat for any organization.

2.8 Database Communication Protocol

Vulnerabilities Large number of security weaknesses is being identified in the database communication protocols of all database retailers. Deceitful activity directing these susceptibilities can varies from illegal data access, to data exploitation, to denial of service

2.9 Weak Authentication

A weak authentication strategy renders the databases more vulnerable to attackers. The identity of database users are stolen or the login credentials are obtained through some source which then helps in modification of data or obtaining sensitive information and if authentication is not properly implemented and is weak, it helps the attacker to steal data.

2.10 Backup Data Exposure

Backup data exposure is an important threat that needs to be taken care of. Since backups on tapes, DVD's or any external media are exposed to high risks, they need to be protected from attack such as theft or destruction. So far we have discussed some important threats to database security. Now we shall see what can be done to limit these risks and threats.

3. THE VULNERABILITIES IN DATABASE MANAGEMENT SYSTEM.

Based on our survey conducted the vulnerabilities in database are defined as: poor architecture, mis configurations, and vendor bugs incorrect usage [3].

3.1 Vendor bugs refer to buffer overflows and other programming errors that result in users executing the commands they are allowed to be execute. Furthermore Downloading and applying patches usually fix vendor bugs and viruses.

3.2 Poor architecture refers the result of inadequate factoring security into the design of how an application works there. These vulnerabilities are typically the hardest to fix because they require a major rework by the vendor. We can give an example of poor architecture; it would be when a vendor utilizes a weak form of inscription.

3.3 Mis configurations are caused by not accurately locking down databases. Mostly the configuration options of databases can be set in a way that compromises security and safety for that database. Some of these parameters are concluded insecurely by default. But mostly it is not a problem unless you unsuspectingly change the configuration and setting. An example of this in Oracle is the REMOTE_OS_AUTHENT parameter. When you set REMOTE_OS_AUTHENT to true you are allowing unauthenticated users to connect to your database, so that he can do his task correctly.

3.4 Incorrect usage means to building applications utilizing developer tools in ways that can be used to break into a database. SQL injection is an example of incorrect usage for developer.

The authors Marco Vieira and Henrique Madeira [4] have defined that the vulnerabilities in DBMS are an internal factor related to the set of security mechanisms available or not available in the database, the correct configuration of those mechanisms (it is a responsibility of the DBA), and the hidden flaws on the system configuration. He has described that security in database can be violated due to points as given below:

3.5 Irresponsible DBA: Refers to deactivation of the necessary security mechanisms such that user privileges, authentication, auditing, data encryption which allows intruders to find a way to getting access the data into database.

3.6 Incorrect configuration: Permits unauthorized users or hackers to access the data in our system.

3.7 Hidden flaws in the database: May allow hackers to connect to the database server by exploring those faults.

3.8 Unauthorized users: Means these users “still” the credentials of authorized users in order to access the database server for searching the data.

3.9 Misused Privileges: Refers to authorized users take advantage of their privileges to maliciously access or destroy our data in a database.

3.10 Configuration and Installation: Using a default installation and configuration that is known by publicly. For example failure to change default password or default privileges or permissions.

3.11 User Mistakes: *Sometimes Carelessness* in implementing procedures failures to follow directly, or accidental errors with some faults. For example users lack bad authentication process, technical information or implementation, untested disaster recovery plan in a database.

3.12 Software: Refers to vulnerabilities found in commercial software for all types of programs such that all applications, operating systems, database management systems and network systems with other different programs.

3.13 Design and Implementation: Inaccurate software analysis and design as well as coding problems and faults may lead to vulnerabilities in a database.

4. SECURITY METHODS IN DATABASE MANAGEMENT SYSTEM

Here we will discuss about some security methods in DBMS. In early days security methods in database management system focus only on role base access control or maintaining the confidentiality or authenticity of the database. But in the current scenario the unauthorized user working on a web page which is connected via internet connection has access to the database, since all the queries sent by the user is converted to SQL query in that database. The user may send malicious query and confirm or modify the transactions of the database without affecting the performance of the database. This type of attack is called SQL injection. But in the current scenario the security method of database should focus on role base access control and maintain CIA and avoid attacks due to network. This section emphasizes the same, based on various papers and books available on similar topic or same issue.

4.1 A SECURING DATABASE BASED ON ACCESS CONTROL:

In this section we will discussed about the database security based on access control. The role based access control method has been proposed by Guoliang Zou, Jing Wang, Dongmei Huang [5]

where he has implemented security using the following points:

- Preventing illegal users from logging the system
- Indentify validation
- Access Control Interface
- Verification codes
- Database security: storage procedure

- Database security: oracle parameter

The author Ravi Sandhu has created various security approaches [1] where he has considered that access control policies in early days were based on the development of two different classes of models, the discretionary access control policy and on the required access control policy and procedure. Based on these models of early days [7] have proposed two assumptions:

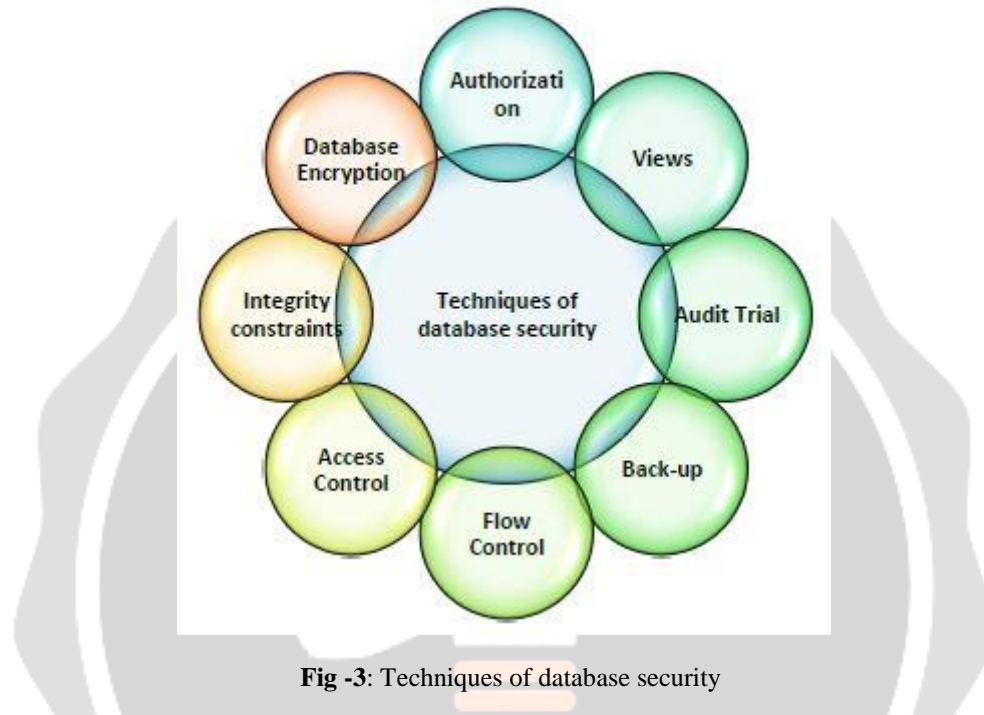


Fig -3: Techniques of database security

- The first assumption was that the access control models for databases should be defined in terms of the logical data model; hence authorizations for a relational database should be defined in terms of relational model such as relations, relation attributes and tuples etc.
- The second assumption is that for databases, in accession to name-based access control, where the secure and protected objects are categorized by giving their names, content-based access control has to be promoted.

Discretionary access control policy has subsidized in the creation and development of System R access control for relational database management system which altered strongly on some key features such as distributed authorization administration, effective grant and revoke of authorizations and the use of views for supporting and developing content-based authorizations. Furthermore the access control policies of an object oriented database (OODBMS) are defined in [8]. Here in this point the author has discussed about two proposed security models for OODBMS. They are given below as:

- *Sorion Security Model*: This is a security model proposed by Thuraiasingham to associate a secure access control into the ORION model system.
- *Jajodia-Dogan Security Model*: Jajodia-Dogan has proposed a security model for OOBMS that control access by using the encapsulation characteristic of object oriented database.

Henceforth using the access control policies and procedure the confidentiality of the database can be supported. The second security issue of database management systems has various fields of database integrity as described in [6]:

- *Physical database integrity protection*: It manages data integrity through physical obstacles such as fires and power failures.
- *Logical data integrity protection*: It refers to the assertion that information is can be changed only by users.
- *Data element integrity protection*: It involves data efficiency and data regularity.

And the third security issue availability as described above belongs to the data availability from the database management system. Henceforth, Due to the availability of company's whole information on the web page which is connected via Internet to its database, the whole data of that company is available using the SQL injection. Thus below section describes the security methods to prevent SQL injection in that scenario.

4.2 SOME SECURITY METHODS TO PREVENT SQL INJECTION

Hence as a protection from SQL injection many Intrusion Detection Systems (IDS) have been suggested. A brief description of these IDS is discussed below:

- *Misuse Detection System for DBMS*

This method has been proposed by Chung *et al.* (1999). It is called a misuse-detection system, created for relational databases. It uses audit data log to retrieve profiles describing typical behaviour of users in Database Management System. The method is present by Lee *et al.* (2000). This method is based on intrusions. Hence this method has used time signatures to discover database intrusions. On the other way similar work was proposed by Low *et al.* (2002). This method is used for Detecting Intrusion in Databases through Fingerprinting Transactions (DIDAFIT). It is a system created using misuse detection approach to show database intrusion detection at the application level in a database. But another approach towards a database specific intrusion detection mechanism is by Hu and Panda (2003). They proposed and developed a mechanism that is more capable of finding data dependency relationships among transactions and use this information to find hidden anomalies in a database log. Ke Chen *et al.* (2005) developed an intrusion detection model for a database system based on digital amnesty. It gives an additional layer of security against DBMS misuse. On other hand a real-time intrusion detection mechanism based on the profile of user roles has been prescribed by Bertino *et al.* (2005). This total approach is based on mining SQL queries stored in audit log files in a database. Rietta (2006) described an application layer intrusion detection system, which should take the form of a proxy server and apply an anomaly detection model based on distinct characteristics of SQL and the transaction history of a appropriate user application and user. Aziah Asmawi has proposed SQL Injection and Insider Misuse Detection System (SIIMDS) in 2008 to define both types of intrusions from external and internal threats. Malicious users may access a series of safe information and then apply different techniques to retrieve sensitive data by using that information. To address this inference problems, Yu Chen in [9] has created a semantic inference model (SIM) that symbolize all the possible inference channels from any attribute in the system to the set of elevated sensitive attributes. Hence based on the SIM, the violation detection system keeps track of a user's query history in a database. When a new query is stified, all the channels where sensitive information can be stored will be recognizing. If the probability of inferring sensitive information increased a more specified threshold, then the current query request will be revoked. Using the security methods mentioned in section A and B secure and safe database can be created. It may be accessed from anywhere and the security would be managed Even though there is no such thing as a 100 percent guarantee in network security, awful obstacles can be placed in the path of SQL injection attack. Anybody of these defenses extremely reduces the chances of a successful SQL injection attack to prevent our data. Implementing all four is a best practice that will supply high degree of protection and safety. Despite its extensive application, your web site does not have to be SQL injection's next suspect. The next section briefs up all the vulnerabilities, threats and security methods of database management system in tabular format which will be beneficial for the development of secure and safe database. There actually is a lot method that web site owners can do to secure against SQL injection attack.

4.3 Encryption in databases

Paper	Methods	Algorithm	Where encryption is performed
A Novel Framework for Database Security based on Mixed Cryptography	Mixed Cryptography Technique based on data classification methods	Any symmetric Encryption algorithm can be used	Encryption is done at <ul style="list-style-type: none"> • Client side • Untrusted database • Server
Database	Hash Security Module	State –of-the art algorithm	Encryption can be at:

Encryption	Encryption Strategy	and mode of operation should be used.	<ul style="list-style-type: none"> Storage Level Database Level Application Level
A Database Encryption Scheme for Enhanced Security and Easy Sharing	Combination of the conventional encryption and public key encryption, utilizing the speed of conventional encryption and convenience of public key encryption.	X	X
Transparent Data Encryption-Solution for Security of Database Contents	Transparent Data Encryption used by Master database key	X	Page level
Fast, Secure Encryption for Indexing in a Column-Oriented DBMS	Fast Comparison Encryption	Symmetric encryption algorithm	Data Warehouses

4.4 RECENT USED DATABASE SECURITY TECHNIQUES

- **Securing Database using Cryptography**

Sesay et al. proposed a database encryption scheme. In this scheme the users are divided into two levels: Level 1 (L1) and Level 2 (L2). Level 1 users have access to their own private encrypted data and the unclassified public data, whereas Level 2 users have access to their own private data and also classified data which is stored in an encrypted form. Liu et al. proposed a novel database encryption mechanism [10]. The proposed mechanism performs column-wise encryption that allows the users to classify the data into sensitive data and public data. This classification helps in selecting to encrypt only that data which is critical and leaves the public data untouched thereby reducing the burden of encrypting and decrypting the whole database, as result of which the performance is not degraded. Mixed Cryptography Database [9] scheme is presented by Kadhem et al. The technique involves designing a framework to encrypt the databases over the unsecured network in a diversified form that comprise of owning many keys by various parties. In the proposed framework, the data is grouped depending upon the ownership and on other conditions.

- **Securing Database using Steganography**

Das et al. explained various techniques in steganography that can be implemented to hide critical data and prevent them from unauthorized and direct access. The various techniques include still image steganography, audio steganography, video steganography, IP Datagram steganography. Naseem et al. presented a method that uses steganography to hide data. In the proposed scheme the data is embedded in the LSB's of the pixel values. The pixels values are categorized into different ranges and depending on the range certain number of bits is allocated to hide the sensitive data. Kuo et al. presented a different approach to conceal data. In this scheme the image is divided into fixed number of blocks. Histogram of each block is calculated along with the maximum and minimum points to mask the data. This mechanism increases the hiding capacity of the data. Dey et al. employs a diverse approach to efficiently hide the sensitive data and escalate the data hiding capacity in still images. The technique involves using prime numbers and natural numbers to enhance the number of bit planes to cloak the data in the images.

- **Securing Database using Access Control**

Bertino et al. explains an authorization technique for video databases. In the proposed scheme, the access to the database and to a particular stream of the video is granted only after verifying the credentials of that user. The credentials may not just be the user-id but it may be the characteristics that define the user and only after successful verification of the credentials the user is granted the permission to access the database. Kodali et al. presented a generalized authorization model for multimedia digital libraries. The scheme involves integrating the three most common and widely used access control mechanisms namely: mandatory, discretionary and role-based models into a single framework to allow a unified access to the protected data. The technique also addresses the need of continuous media data while supporting the QoS constraints alongside preserving the operational semantics. An authorization model is proposed by Rizvi et al. In the explained technique is based on authorization views which enable authorization transparent querying in which the user queries are formed and represented in terms of database relations and are acceptable only when the queries can be verified using the information contained in the authorization rules. The work presents the new techniques of validity and conditional validity which is an extension of the earlier work done in the same area.

5. Comparison of Encryption Methods/Techniques

Methods	Advantages	Disadvantages
Mixed Cryptography Technique based on data classification methods	Sensitive data is protected from attacks even at multiple levels because of having many keys to different parties. Secure data storage and data transmission is performed to ensure the maximum protection of sensitive data.	Performance of queries and security analysis is affected because of encryption algorithms. Access control methods are not defined.
Hash Security Module Encryption Strategy	Security server is not tampered Encryption keys are never exposed.	Complex
Transparent Data Encryption used by Master database key	Provides protection to sensitive data on disk drives and backup media from illegal access. Cost of user management is reduced. Provide privacy management.	Encryption across communication channels is not provided. Database could not be opened if the certificate is not available and the backup of certificate and private key is not maintained. Database becomes inaccessible after altering the certificates to be password protected.
Fast Comparison Encryption	Fast indexing operation Low decryption Overhead.	


6. CONCLUSIONS

Data to any organization is a most valuable property. Security of sensitive data is always a big challenge for an organization at any level. In today's technological world, database is vulnerable to hosts of attacks. In this study major security issues faced databases are identified and some encryption methods are discussed that can help to reduce the attacks risks and protect the sensitive data. It has been concluded that encryption provides confidentiality but give no assurance of integrity unless we use some digital signature or Hash function. Using strong encryption algorithms reduces the performance. The future work could be carried out make encryption more effective and efficient.

7. REFERENCES

- [1] Elisa Bertino, Fellow, IEEE, and Ravi Sandhu, Fellow, IEEE, “Database Security—Concepts, Approaches and Challenges” in IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 2, NO. 1, JANUARY-MARCH 2005
- [2] Amichai Shulman; Top Ten Database Security Threats, How to Mitigate the Most Significant Database Vulnerabilities, 2006 White Paper.
- [3] Andriy Furmanyuk, Mykola Karpinsky, Bohdan Borowik, “Modern Approaches to the Database Protection” in IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 6-8 September 2007, Dortmund, Germany
- [4]. Marco Vieira, Henrique Madeira, “Detection of Malicious Transactions in DBMS”, 11th Pacific Rim International Symposium on Dependable Computing
- [5] Guoliang Zou, Jing Wang, Dongmei Huang, LiangJun Jiang, “Model Design of Role-Based Access Control and Methods of Data Security”, 2010 International Conference on Web Information Systems and Mining.
- [6] Aziah Asmawi, “System Architecture for SQL Injection and Insider Misuse Detection System for DBMS”, my - 1-4244-2328 6/08/\$25.00 © 2008 IEEE
- [7] E.B. Fernandez, R.C. Summers and C. Wood, Database Security and Integrity. Addison-Wesley, Feb. 1981.
- [8] Premchand B. Ambhore, B.B. Meshram, V.B. Waghmare, “A IMPLEMENTATION OF OBJECT ORIENTED DATABASE SECURITY”, Fifth International Conference on Software Engineering Research, Management and Applications.
- [9] Kadhem, H.; Amagasa, T.; Kitagawa, H.; A Novel Framework for Database Security based on Mixed Cryptography; Internet and Web Applications and Services, 2009. ICIW '09. Fourth International Conference on; Publication Year: 2009, Page(s): 163 –170
- [10] Tanya Bacca; Making Database Security an IT Security Priority A SANS Whitepaper – November 2009.
- [11] Security in Database Systems By Abdulrahman Hamed Almutairi.
- [12] Web Database Security Techniques International Journal of Advance Research in Computer Science and Management Studies.
- [13] Database Security and Encryption: A Survey Study International Journal of Computer Applications · May 2012.

BIOGRAPHIES

 A portrait of a young man with dark hair and glasses, wearing a green and white checkered shirt. He is looking directly at the camera with a neutral expression.	<p>Bhavin Fataniya received B.E degree in Information Technology from GEC,Bhavnagar and now pursuing M.E(I.T) from L.D College of Engineering,Ahmedabad.</p>
--	--

