Database Security

Database Security means to keep sensitive information safe and prevent the loss of data. Security of the database is controlled by Database Administrator (DBA). Database security is the technique that protects and secures the database against intentional or accidental threats. Security concerns will be relevant not only to the data residing in an organization's database: the breaking of security may harm other parts of the system, which may ultimately affect the database structure. Consequently, database security includes hardware parts, software parts, human resources, and data. To efficiently do the uses of security needs appropriate controls, which are distinct in a specific mission and purpose for the system. The requirement for getting proper security while often having been neglected or overlooked in the past days; is now more and more thoroughly checked by the different organizations. We consider database security about the following situations:

●Theft and fraudulent.

●Loss of confidentiality or secrecy.

●Loss of data privacy.

●Loss of data integrity.

●Loss of availability of data.

These listed circumstances mostly signify the areas in which the organization should focus on reducing the risk that is the chance of incurring loss or damage to data within a database. In some conditions, these areas are directly related such that an activity that leads to a loss in one area may also lead to a loss in another since all of the data within an organization are interconnected.

The following are the main control measures are used to provide security of data in databases:

1. Authentication

2.Access control

3.Inference control

4.Flow control

5.Database Security applying Statistical Method

6.Encryption

Authentication: Authentication is the process of confirmation that whether the user logs in only according to the rights provided to him to perform the activities of the database. A particular user can login only up to his privilege but he can't access the other sensitive data. The privilege of accessing sensitive data is restricted by using Authentication. By using these authentication tools for biometrics such as retina and figure prints can prevent the database from unauthorized/malicious users. It is the first step and done before authorisation. Also referred to as Verification. Authorisation: Authorization is a privilege provided by the Database Administer. Users of the database can only view the contents they are authorized to view. The rest of the database is out of bounds to them. It is done after authentication. Also referred to as Validation. The different permissions for authorizations available are:

●Primary Permission -This is granted to users publicly and directly.

●Secondary Permission -This is granted to groups and automatically awarded to a user if he is a member of the group.

●Public Permission -This is publicly granted to all the users.

●Context sensitive permission -This is related to sensitive content and only granted to a select user. The categories of authorization that can be given to users are:

●System Administrator -This is the highest administrative authorization for a user. Users with this authorization can also execute some database administrator commands such as restore or upgrade a database.

●System Control -This is the highest control authorization for a user. This allows maintenance operations on the database but not direct access to data.

●System Maintenance -This is the lower level of system control authority. It also allows users to maintain the database but within a database manager instance.

●System Monitor -Using this authority, the user can monitor the database and take snapshots of it.

Authorisation relates to the permissions granted to an authorised user to carry out particular transactions, and hence to change the state of the database (write item transactions) and/or receive data from the database (read-item transactions). The result of authorisation, which needs to be on a transactional basis, is a vector: Authorisation (item, auth-id, operation). A vector is a sequence of data values at a known location in the system. How this is put into effect is down to the DBMS functionality. At a logical level, the system structure needs an authorisation server, which needs to cooperate with an auditing server. There is an issue of server-to-server security and a problem with amplification as the authorisation is transmitted from system to system. Amplification here means that the security issues become larger as a larger number of DBMS servers are involved in the transaction. Audit requirements are frequently implemented poorly. To be safe, you need to log all accesses and log all authorisation details with transaction identifiers. There is a need to audit regularly and maintain an audit trail, often for a long period.

Access Control: The security mechanism of DBMS must include some provisions for restricting access to the database by unauthorized users. Access control is done by creating user accounts and to control the login process by the DBMS. So, that database access of sensitive data is possible only to those people (database users) who are allowed to access such data and to restrict access to unauthorized persons. The database system must also keep track of all operations performed by certain users throughout the entire login time.

Inference Control: This method is known as the countermeasures to statistical database security problem. It is used to prevent the user from completing any inference channel. This method protects the sensitive information from indirect disclosure. Inferences are of two types, identity disclosure or attribute disclosure.

Flow Control: This prevents information from flowing in a way that it reaches unauthorized users. Channels are the pathways for information to flow implicitly in ways that violate the privacy policy of a company are called covert channels.

Database Security applying Statistical Method: Statistical database security focuses on the protection of confidential individual values stored in and used for statistical purposes and used to retrieve the summaries of values based on categories. They do not permit to retrieve the individual information. This allows access to the database to get statistical information about the number of employees in the company but not to access the detailed confidential/personal information about specific individual employees.

Encryption: This method is mainly used to protect sensitive data (such as credit card numbers, OTP numbers) and other sensitive numbers. The data is encoded using some encoding algorithms. An unauthorized user who tries to access this encoded data will face difficulty in decoding it, but authorized users are given decoding keys to decode data. Why is access control important? Access control regulates which users, applications, and devices can view, edit, add, and delete resources in an organization's environment. Controlling access is one of the key practices to protect sensitive data from theft, misuse, abuse, and any other threats. There are two levels of access control: physical and logical.

Access control helps to mitigate both insider and outsider threats. That's why IT regulations and standards —NIST, HIPAA, PCI DSS, and others— enforce strict physical and logical access control measures. In this article, we discuss models of logical access control. There are several logical access control models: mandatory, discretionary, role-based, attribute-based, etc. The process of choosing and deploying an access control model looks different for each organization. This choice depends on:

●The nature of the protected data

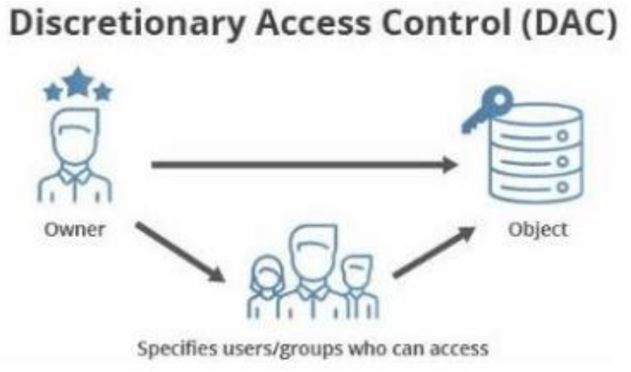
●IT requirements and industry standards

●The number of employees

●The cybersecurity budget Let's find out when to use mandatory and discretionary access control models.

DAC

Discretionary access control(DAC) is an identity-based access control model that provides users a certain amount of control over their data. Data owners (or any users authorized to control data) can define access permissions for specific users or groups of users. Access permissions for each piece of data are stored in an access-control list (ACL). This list can be generated automatically when a user grants access to somebody or can be created by an administrator. An ACL includes users and groups that might access data and levels of access they might have. An ACL can also be enforced by a system administrator. In this case, the ACL acts as a security policy, and regular users can't edit or overrule it.


Discretionary Access Control (DAC)
Owner
Object
Specifies users/groups who can access

Gaining access in the DAC model works like this:

●User 1 creates a file and becomes its owner or obtains access rights to an existing file.

●User 2 requests access to this file.

●User 1 grants access at their own discretion. However, user 1 can't grant access rights that exceed their own. For example, if user 1 can only read a document, they can't allow user 2 to edit it.

●If there's no contradiction between the ACL created by an administrator and the decision made by user 1, access is granted. Discretionary access control is quite a popular model because it allows a lot of freedom for users and doesn't cause administrative overhead.

However, it has several considerable limitations.

<u>Pros and cons of DAC</u>

Pros

●User-friendly — Users can manage their data and quickly access data of other users.

●Flexible — Users can configure data access parameters without administrators.

●Easy to maintain — Adding new objects and users doesn't take much time for the administrator.

●Granular — Users can configure access parameters for each piece of data. Cons

●Low level of data protection — DAC can't ensure reliable security because users can share their data however they like.

●Obscure — There's no centralized access management, so in order to find out access parameters, you have to check each ACL.

When to use DAC

DAC allows for a lot of flexibility and decreases the load on system administrators as users can manage access on their own. On the other hand, it doesn't provide a high level of security for several reasons:

●If user 1 shares access rights with user 2, there's no guarantee that user 2 needs this access to work or won't steal or corrupt data or grant access to a malicious user.

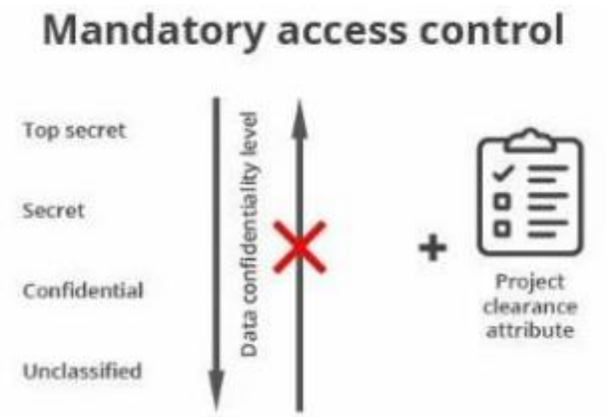
●It's impossible to control information flows inside the network.

●It's impossible to enforce the principles of least privilege, need to know, and separation of duties.

Because of these limitations, DAC can't be used by organizations that work with extremely sensitive data (medical, financial, military, etc.). At the same time, DAC is a good choice for small businesses with limited IT staff and cybersecurity budgets. It allows for sharing information and ensures the smooth operation of the business. This approach, when applied in an organization with 10 to 20 employees, lacks the complexity and oversight challenges associated with the use of DAC in organizations with hundreds or thousands of employees.

MAC

Mandatory access control(MAC) is a model of access control where the operating system provides users with access based on data confidentiality and user clearance levels. In this model, access is granted on need to know basis: users have to prove a need for information before gaining access. MAC is considered the most secure of all access control models. Access rules are manually defined by system administrators and strictly enforced by the operating system or security kernel. Regular users can't alter security attributes even for data they've created.



With MAC, the process of gaining access looks like this:

●The administrator configures access policies and defines security attributes: confidentiality levels, clearances for accessing different projects and types of resources.

●The administrator assigns each subject (user or resource that accesses data) and object (file, database, port, etc.) a set of attributes.

●When a subject attempt to access an object, the operating system examines the subject's security attributes and decides whether access can be granted. For example, let's consider data that has the "top secret" confidentiality level and "engineering project" security label. It's available to a set of users that have "top secret" clearance and authorization to access engineering documents. Such users can also access information that requires a lower level of clearance. But employees with lower levels of clearance will not have access to information that requires a higher level of clearance MAC brings lots of benefits to a cybersecurity system. But it has several disadvantages to consider.

<u>Pros and cons of MAC</u>

Pros

●High level of data protection — An administrator defines access to objects, and users can't edit that access.

●Granular — An administrator sets user access rights and object access parameters manually.

●Immune to Trojan Horse attacks — Users can't declassify data or share access to classified data. Cons

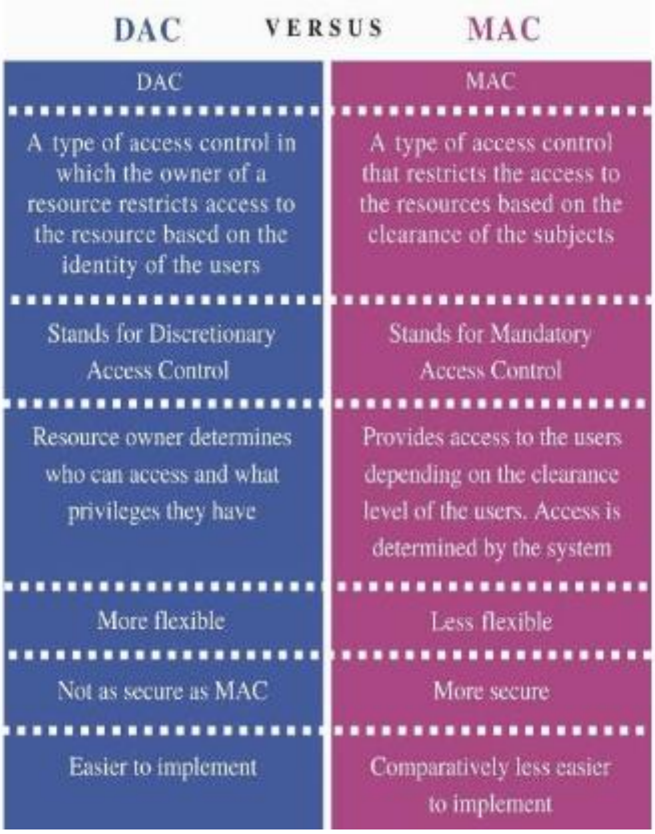
●Maintainability — Manual configuration of security levels and clearances requires constant attention from administrators.

●Scalability — MAC doesn't scale automatically.

●Not user-friendly — Users have to request access to each new piece of data; they can't configure access parameters for their own data.

When to use MAC

MAC is used by the US government to secure classified information and to support multilevel security policies and applications. This access control model is mostly used by government organizations, militaries, and law enforcement institutions. It's reasonable to use MAC in organizations that value data security more than operational flexibility and costs. Implementing MAC in a private organization is rare because of the complexity and inflexibility of such a system. A pure MAC model provides a high and granular level of security. On the other hand, it's difficult to set up and maintain. That's why it's common to combine MAC with other access control models. For example, combining it with the role-based model speeds up the configuration of user profiles. Instead of defining access rights for each user, an administrator can create user roles. Each organization has users with similar roles and access rights: employees with the same job position, third-party vendors, etc. An administrator can configure roles for these groups instead of configuring individual user profiles from scratch. Another popular combination is MAC and the discretionary access control (DAC) model. MAC can be used to secure sensitive data, while DAC allows co-workers to share information within a corporate file system.



DAC VERSUS MAC

DAC	MAC
A type of access control in which the owner of a resource restricts access to the resource based on the identity of the users	A type of access control that restricts the access to the resources based on the clearance of the subjects
Stands for Discretionary Access Control	Stands for Mandatory Access Control
Resource owner determines who can access and what privileges they have	Provides access to the users depending on the clearance level of the users. Access is determined by the system
More flexible	Less flexible
Not as secure as MAC	More secure
Easier to implement	Comparatively less easier to implement

RBAC

Role-based access control (RBAC) restricts network access based on a person's role within an organization and has become one of the main methods for advanced access control. The roles in RBAC refer to the levels of access that employees have to the network. Employees are only allowed to access the information necessary to effectively perform their job duties. Access can be based on several factors, such as authority, responsibility, and job competency. In addition, access to computer resources can be limited to specific tasks such as the ability to view, create, or modify a file. As a result, lower-level employees usually do not have access to sensitive data if they do not need it to fulfil their responsibilities. This is especially helpful if you have many employees and use third-parties and contractors that make it difficult to closely monitor network access. Using RBAC will help in securing your company's sensitive data and important applications.

EXAMPLES OF ROLE-BASED ACCESS CONTROL

Through RBAC, you can control what end-users can do at both broad and granular levels. You can designate whether the user is an administrator, a specialist user, or an end-user, and align roles and access permissions with your employees' positions in the organization. Permissions are allocated only with enough access as needed for employees to do their jobs. What if an end-user's job changes? You may need to manually assign their role to another user, or you can also assign roles to a role group or use a role assignment policy to add or remove members of a role group. Some of the designations in an RBAC tool can include:

●Management role scope - it limits what objects the role group is allowed to manage.

●Management role group - you can add and remove members.

●Management role - these are the types of tasks that can be performed by a specific role group.

●Management role assignment - this links a role to a role group.

By adding a user to a role group, the user has access to all the roles in that group. If they are removed, access becomes restricted. Users may also be assigned to multiple groups in the event they need temporary access to certain data or programs and then removed once the project is complete. Other options for user access may include:

●Primary - the primary contact for a specific account or role.

●Billing - access for one end-user to the billing account.

●Technical - assigned to users that perform technical tasks.

●Administrative - access for users that perform administrative tasks.

BENEFITS OF RBAC

Managing and auditing network access is essential to information security. Access can and should be granted on a need-to-know basis. With hundreds or thousands of employees, security is more easily maintained by limiting unnecessary access to sensitive information based on each user's established role within the organization. Other advantages include:

1. Reducing administrative work and IT support. With RBAC, you can reduce the need for paperwork and password changes when an employee is hired or changes their role. Instead, you can use RBAC to add and switch roles quickly and implement them globally across operating systems, platforms and applications. It also reduces the potential for error when assigning user permissions. This reduction in time spent on administrative tasks is just one of several economic benefits of RBAC. RBAC also helps to more easily integrate third-party users into your network by giving them predefined roles.

2.Maximizing operational efficiency. RBAC offers a streamlined approach that is logical in definition. Instead of trying to administer lower-level access control, all the roles can be aligned with the organizational structure of the business and users can do their jobs more efficiently and autonomously.

3.Improving compliance. All organizations are subject to federal, state and local regulations. With an RBAC system in place, companies can more easily meet statutory and regulatory requirements for privacy and confidentiality as IT departments and executives have the ability to manage how data is being accessed and used. This is especially significant for health care and financial institutions, which manage lots of sensitive data such as PHI and PCI data.

BEST PRACTICES FOR IMPLEMENTING RBAC

Implementing a RBAC into your organization shouldn't happen without a great deal of consideration. There are a series of broad steps to bring the team on board without causing unnecessary confusion and possible workplace irritations. Here are a few things to map out first.

●Current Status: Create a list of every software, hardware and app that has some sort of security. For most of these things, it will be a password. However, you may also want to list server rooms that are under lock and key. Physical security can be a vital part of data protection. Also, list the status of who has access to all of these programs and areas. This will give you a snapshot of your current data scenario.

●Current Roles: Even if you do not have a formal roster and list of roles, determining what each individual team member does may only take a little discussion. Try to organize the team in such a way that it doesn't stifle creativity and the current culture (if enjoyed).

●Write a Policy: Any changes made need to be written for all current and future employees to see. Even with the use of a RBAC tool, a document clearly articulating your new system will help avoid potential issues.

●Make Changes: Once the current security status and roles are understood (not to mention a policy is written), it's time to make the changes.

●Continually Adapt: It's likely that the first iteration of RBAC will require some tweaking. Early on, you should evaluate your roles and security status frequently. Assess first, how well the creative/production process is working and secondly, how secure your process happens to be. A core business function of any organization is protecting data. An RBAC system can ensure the company's information meets privacy and confidentiality regulations. Furthermore, it can secure key business processes, including access to IP, that affect the business from a competitive standpoint.

Intrusion

A network intrusion is any unauthorized activity on a computer network. Detecting an intrusion depends on the defenders having a clear understanding of how attacks work. In most cases, such unwanted activity absorbs network resources intended for other uses, and nearly always threatens the security of the network and/or its data. Properly designing and deploying a network intrusion detection system will help block the intruders.

Intruder:

In relation to computers, an intruder is an individual or software program that enters a computer system without authorization. An example of an intruder would be a hacker. Another example would be a software virus. Types of Intruder: Basically there are 3 types of intruder:

1. Masquerader or Outsider Intruder

2.Misfeasor or Inside Intruder

3.Clandestine user

1)Masquerader or Outsider Intruder: An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.

2)Misfeasor or Inside Intruder: A legitimate user who accesses data, programs, or resources for which such access is not authorized or who is authorized for such access but misuses his or her privileges. 3)Clandestine user: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

Intrusion Detection System (IDS):

An Intrusion Detection System (IDS)is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms. Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity. Intrusion prevention systems also monitor network packets inbound to the system to check the malicious activities involved in it and at once send the warning notifications.

Classification of Intrusion Detection System:

IDS are classified into 5 types:

1.Network Intrusion Detection System (NIDS): Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behaviour is observed, the alert can be sent to the administrator. An example of an NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.

2.Host Intrusion Detection System (HIDS): Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their layout.

3.Protocol-based Intrusion Detection System (PIDS): Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently reside at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

4.Application Protocol-based Intrusion Detection System (APIDS): Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application specific protocols. For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

5.Hybrid Intrusion Detection System: Hybrid intrusion detection systems are made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection systems are more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Detection Method of IDS:

1.Signature-based Method: Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures. Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in the system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

2.Anomaly-based Method: Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in the model. Machine learning based methods have a better generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

SQL Injection SQL injection is a technique used to exploit user data through web page inputs by injecting SQL commands as statements. Basically, these statements can be used to manipulate the application's web server by malicious users.

●SQL injection is a code injection technique that might destroy your database.

●SQL injection is one of the most common web hacking techniques.

●SQL injection is the placement of malicious code in SQL statements, via web page input. Exploitation of SQL Injection in Web Applications Web servers communicate with database servers anytime they need to retrieve or store user data. SQL statements by the attacker are designed so that they can be executed while the web-server is fetching content from the application server. It compromises the security of a web application.

Example of SQL Injection Suppose we have an application based on student records. Any student can view only his or her own records by entering a unique and private student ID. Suppose we have a field like below:

Student id: And the student enters the following in the input field: 12222345 or 1=1. So this basically translates to : SELECT * from STUDENT where STUDENT-ID == 12222345 or 1 = 1 Now this 1=1 will return all records for which this holds true. So basically, all the student data is compromised. Now the malicious user can also delete the student records in a similar fashion. Consider the following SQL query. SELECT * from USER where USERNAME = "" and PASSWORD="" Now the malicious can use the '=' operator in a clever manner to retrieve private and secure user information. So instead of the above-mentioned query the following query when executed, retrieves protected data, not intended to be shown to users. Select * from User where (Username = "" or 1=1) AND (Password="" or 1=1). Since1=1always holds true, user data is compromised. Impact of SQL Injection The hacker can retrieve all the user-data present in the database such as user details, credit card information, social security numbers and can also gain access to protected areas like the administrator portal. It is also possible to delete the user data from the tables. Nowadays, all online shopping applications, bank transactions use back-end database servers. So in-case the hacker is able to exploit SQL injection, the entire server is compromised.

Preventing SQL Injection

●User Authentication: Validating input from the user by pre-defining length, type of input, of the input field and authenticating the user.

●Restricting access privileges of users and defining as to how much amount of data any outsider can access from the database. Basically, users should not be granted permission to access everything in the database.

●Do not use system administrator accounts.