Michael Colliver & Jake Ellis

Professor Im

CIS 483

April 23, 2012

**Threat Prevention and Detection within Databases**

1. **Introduction to Threats**

According to Webster’s dictionary the definition of a threat is “An expression of intention to inflict evil, injury, or damage”. This means a threat can be physical, emotional, or even digital. Just as this is seen throughout the generality of information security it is also seen within the realm of security as it pertains to databases. Throughout this document we will be discussing the physical and digital threats posed upon databases and the proper techniques to prevent them.

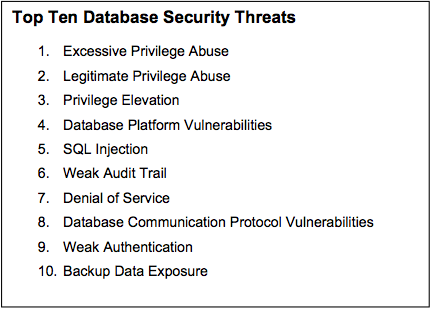
The scope of this document encompasses Privilege abuse, SQL injection, DOS, and Authentication threats. It is necessary to realize that these are real threats that are occurring within today’s database environment. Prior knowledge of the threat is the first step in combating it. Throughout the paper as we approach each threat, we will discuss it in detail and outline preventative and detective measures to take when dealing with each one.

1. **Need For Prevention & Detection**

Ideas of the first relational model database emerged in the early 1970s. Later on in this decade the Entity-Relationship database model was introduced. Later down the line, in the 1980s, SQL became the standard query language. Today database applications continue to grow. As we see the rapid expansion of the database and its uses it is clear that there will be threats, intentional and unintentional, thrown against it. This is evident as the application of the technology expands and the outreach of it finds its way to a greater many.

As threats arise the knowledge of these will be a great ally and combatant. This will help in the field of preventative measures. If the threat can be prevented completely then no harm or damage can be done to the system at all. That is the best case scenario and something to strive for when it comes to the preventative outlook. Detection will be the second-level defense and it primary purpose is to identify a threat within the system as quickly as possible. If able to do so then it can hopefully minimize damages. Note that it is also possible for a detection system to keep damage from occurring it can sound the alarm swiftly enough. The reduction of damage, hopefully to the point of nothing, is why prevention and detection systems are necessary.

1. **Top 10 Database Threats**



These are the “Top Ten Database Security Threats” according to Imperva’s Application Defense Center. Imperva is one of the leaders in data security which offers several of its solutions to top US commercial banks and global oil & gas companies. Below, each of the “Top Ten” threats will be examined individually and with a significant amount of detail. Prevention of these threats will then be discussed in a later section.

1. Excessive Privilege Abuse

This threat is defined directly by its title. It occurs, “when users (or applicants) are granted database access privileges that exceed the requirements of their job functions, these privileges may be abused for malicious purposes”. Notice here the last word in the title- “Abuse”. This is the crucial part. A user may have excessive privileges but there is no threat until there is a direct “Abuse” upon those excessive privileges. Often times these cases arise simply because administrators either overlook the situation or they do not have enough time to reduce the excess of privileges of the plethora of users within the system. (Shulman)

1. Legitimate Privilege Abuse

This is a threat posed from the user acting within the privileges he/she was given. This is often a threat that is unintentional where the user means no harm but can still produce harm because it causes the system to act in a way that was unintended. Often you see this where the user finds a work-around within the system in order to make their processes more efficient or their work easier. In some ways it resembles a hack but in fact the user is operating under system permissible actions.

1. Privilege Elevation

In simplest terms this is converting from a user to a superuser. “Attackers may take advantage of database platform software vulnerabilities to convert access privileges from those of an ordinary user to those of an administrator. Vulnerabilities may be found in stored procedures, built-in-functions, protocol implementations, and even SQL statements.” (Shulman)

1. Platform Vulnerabilities

This stems from weaknesses in the base operating system. One famous example is the Blaster Worm. It created a denial of service, but did so by taking advantage of vulnerabilities in the Windows 2000 operating system.

1. SQL Injection

This is probably the most commonly noted database threat. In this situation an attacker inserts characters forming a statement into the vulnerability. Depending on the injected statement and the vulnerability the whole database could potentially be uncovered.

1. Weak Audit Trail

Comparatively to those threats mentioned previously, this threat may seem curious but it is still a threat nevertheless. The threat of a weak audit trail implies that of a poor recording or tracking system. In other words, there is not proper documentation of sensitive database transactions. Depending on your organization this could pose anywhere from a very minor threat to an extremely major one. Consider the case of a banking company- especially in cases dealing with large sums of money. It is vital to the well-being of the company that every transaction is accounted for at all times. If this wasn’t the case then that company would not survive long.

1. Denial of Service

“Denial of Service (DoS) is a general attack category in which access to network applications or data is denied to intended users. Several techniques may be used to induce this threat. Some of the most common include network flooding, data corruption, and server resource overload. “Resource overload is particularly common in database environments.” (Shulman)

1. Database Communication Protocol Vulnerabilities

This is a threat that is getting a lot of recognition. “Four out of seven fixes in the two most recent IBM DB2 FixPacks address protocol vulnerabilities.” What this threat refers to is the conventions for the conveyance of data. (Shulman)

1. Weak Authentication

This is exactly as the title implies. An unauthorized user is granted access into the database because of the fact that the standards for authentication to access the database were inadequate. This unauthorized user can achieve this access by several different means- including brute force, social engineering, or some other tactic. It is important to note that a perpetrator may rely on a combination of strategies to obtain access rather than just one.

1. Backup Data Exposure

In many cases backups can become the afterthoughts of a project. Because of this they may become completely unprotected- either digitally or physically. Digitally in that they can be directly accessed without any authentication such as login or physically such as they can easily be stolen without immediate notice of their absence. In both situations a dire threat occurs depending upon the contents of the backups but this is a case that could be avoided if not so careless.

1. **Prevention & Detection of the Top 10 Threats**

Below again are the “Top Ten Database Security Threats” according to Imperva. In this section however we will be detailing preventative measures as well as how to detect the threats presented. Overall, this is the primary focus of the document and this should provide a clear view of how to better prepare and protect a database from the listed threats.

1. Excessive Privilege Abuse

In order to counter this threat, oppose it by setting the bar low. Give users minimum rights as possible. If it is discovers that they cannot accomplish their given task under those specifications only then should their privileges be raised. And when privileges are elevated they should increment slowly so as to not end up with the threat that began the whole process. The level of detection will depend on the degrees to which the admin(s) overlooks the system and/or the user changes aspects that he/she should not be allowed to change- hence excessive privileges. The admin(s) might also put monitoring measures in place to alert if there are significant changes within the system.

1. Legitimate Privilege Abuse

Again, some form of monitoring is the key here. “By enforcing policy for client applications, time of day, location, etc., it’s possible to identify users who are using legitimate database access privileges in a suspicious manner.” (Shulman)

1. Privilege Elevation

For prevention of this threat a combination of a combination of techniques may be used- including intrusion prevention systems (IPS) and query-level access controls. An IPS continually looks through the traffic flowing through the database and tries to identify vulnerabilities. If one is found then it can be granted the authority to shut down traffic to everything pertaining to the vulnerability. The query-level access controls are used to further enhance this process and help the IPS detect whether or not aspects of traffic are legitimate. (Shulman)

1. Platform Vulnerabilities

In order to oppose these threats you will want to implement suggested patches. When the software informs you of an update, not patching it can mean leaving a vulnerability. Be aware that you should only accept patches from the vendor of where the software originated from and that between update periods your database will be more vulnerable. This is where you will want to again have an IPS so attacks on the database can be detected.

1. SQL Injection

Multiple approaches can be used to help alleviate this threat: IPS, query-level access control, and event correlation. “IPS can identify vulnerable stored procedures or SQL injection strings. However, IPS alone is not reliable since SQL injection strings are prone to false positives. ..However, by correlating a SQL injection signature with another violation such as a query-level access control violation, a real attack can be indentified with extreme accuracy.” (Shulman)

1. Weak Audit Trail

To thwart this threat you may have to import other applications into your system until an appropriate level of transaction recording to meet your needs can be established. What you should look for in an auditing system is high performance- the database system isn’t dramatically slowed by having to keep extra records, separation of duties- the auditing system exists independently of the database transactions themselves, and cross-platforming- the auditing application supports leading database platforms and centralizes its operations. Not having these can be an indication that your database might have a weak audit trail. (Shulman)

1. Denial of Service

“DoS prevention requires protection at multiple levels. Network, application, and database level protections are all necessary. In this database-specific context, deployment of connection rate control, IPS, query access control, and response timing control are recommended.” (Shulman)

1. Database Communication Protocol Vulnerabilities

In the case of this threat what’s known as protocol validation can be used to combat it. What protocol validation does is it takes apart the traffic of the database and then it tries to match it to what it believes is expected within the system. If there is a match then no action has to be taken against the traffic. Otherwise, in the event of a match failure, alarms may be sounded or appropriate actions may be taken in order to offset the threat. (Shulman)

1. Weak Authentication

Common sense should reign here and tell you what is appropriate for the protection of a system; but there are standards that can be researched as well. When possible, use two-factor authentication. This will help with the aspect of prevention. Good password policy will advise you to implement a minimum length, character diversity, and etc.

1. Backup Data Exposure

It is best to encrypt backup data in the attempt to prevent threats. This can become an efficient process if implemented properly and will reduce the risk of losing valuable informational assets. Detection of a threat upon backup data is easy to be aware of- how many resources do you place in front of backups? If the answer is very little then chances are a threat might exist within the backups but encrypting is on measure to alleviate part of that problem. Also make sure that backups are in secure locations that require at least some form of authentication before access is granted.

1. **Where Threats Come From**

Once a threat has been determined it is appropriate to identify where exactly the particular threat is coming from. Breaking down the point of origin to simplest form the threat can either be internal or external. Assuming an organizational setting this means that the attacker is either a member of the company, an employee, or simply an average person outside the bounds of the company. Distinguishing which category the aggressor falls under can result in what actions you are able to take and also give you important information about the extent of the threat.

Having an internal threat means the origin of the threat is somewhat under your jurisdiction. What is meant under the circumstance is that you have the ability to provide that person with negative consequences depending on the severity. In many cases any internal threats most likely lead to firing because of the loss in degree of trust. Although there is still involvement with a company in external threat cases the company will not be able to decide the punishment as they would be it an internal threat.

Knowing where the threat comes from can also help with information gathering for the organization. It offers the opportunity to learn more about the threat itself. If you are aware that the threat comes from an internal source then that reveals that the person from who the threat originated from knows more than an average outsider of the company and therefore the level of threat is higher. With the attacker’s greater company knowledge there is the ability and risk that he/she might be able to do greater damage to the organization.

1. **Conclusion**

As databases progress even further they will become even harder to manage them securely. The obvious need for prevention and detection mechanisms is already overwhelmingly apparent within today’s environment. Prevention measures need to be set in place well before hand and there is an inherent need for detection devices to become more and more automated. This grants more time for administrators to focus on other aspects and also helps to catch threats that they might otherwise miss. As the complexity of threats continues one can only hope that opposing measures can keep up in order to keep database systems intact.

**References**

Imperva. *Company Overview*. 2012. Imperva. Retrieved from http://www.imperva.com/company/company.html

Intuit. *A Timeline of Database* History. Intuit QuickBase. 2012. Retrieved from http://quickbase.intuit.com/articles/timeline-of-database-history

Shulman, Amichai. *Top Ten Database Security Threats*. Imperva. 2006. Retrieved from http://www.schell.com/Top\_Ten\_Database\_Threats.pdf

"Threat". *Merriam-Webster.com*. 2012. Retrieved from http://www.merriam-webster.com