Oracle – A forewarning

By Mustafa Syed
Feb 09, 2006

Recently I happened to read an article titled "They know Oracle flaws – Test yourself" by an unknown IT professional on the vulnerabilities found in Oracle, though the article was written for the sole purpose of introducing an auditing product, ***Secure Ora Auditor***, it raised many questions in my mind. This new interest as evident from this article led me to investigate more and get hold of some statistics produced by some audits performed as demo of this product.

Though my forte has never been databases but playing with the numbers in hand further fuelled my interest to look at Oracle as the most universally and commercially used database. Before I go on to harp about the intelligence that I have gathered I would like to share some extracts from the above mentioned article to give some credit to the person that attracted my attention to it in the first place.

"*A multinational software company using Oracle was amazed when they tested their database and found 8000 vulnerabilities in it.* ***Why that happened?*** *We know that Oracle is the most universally and commercially used relational database server used in organizations to accumulate and manage large amounts of data, running with variety of operating systems.* ***But do you know?*** *When you install Oracle, you are installing number of vulnerabilities with it. Clients or Users using oracle, usually close their eyes to the default settings and fully trust on Oracle's claim that its database is 'completely secure'. But the default setting and some known security issues invite the attackers to attack and end result of these vulnerabilities is that the database can be hacked or crashed*".

Going further the article emphasizes on two major categories of vulnerabilities 1) Oracle's default settings and 2) vulnerabilities created by database administrators and other users. The following list from the article illustrates universally known users and objects that Oracle creates during installation as default settings.

Versions	8 (8.0.5)	8i (8.1.7)	9i(9.0.1.1.1)	9i R2	10g
Users	7	17	29	30	23
Objects	2629	24607	31185	28865	47098

A newsletter by Fran Foo (Managing Editor, edit@zdnet.com.au), titled "Oracle's Patchy Record" that I happened to read recently had the following message:

"*Database giant Oracle has come under considerable pressure from research firm Gartner and some in the security community for its software patching procedures*".

"*A week after Oracle released fixes as part of its quarterly CPU (Critical Patch Update) program, Gartner Research vice-president Rich Mogull delivered a scathing analysis of the company's approach towards serious vulnerabilities*".

"*In an advisory, he urged Oracle administrators to stay vigilant and reduced the company's 'bastion of security' image to a myth*". "*Many Oracle administrators rely on*

a combination of the company's historically strong security and the fact that Oracle applications and databases are typically located deep within the enterprise, and so neglect to patch their systems regularly. Moreover, patching is sometimes impossible, due to ties to legacy versions that Oracle no longer supports, Mogull said in the research note".

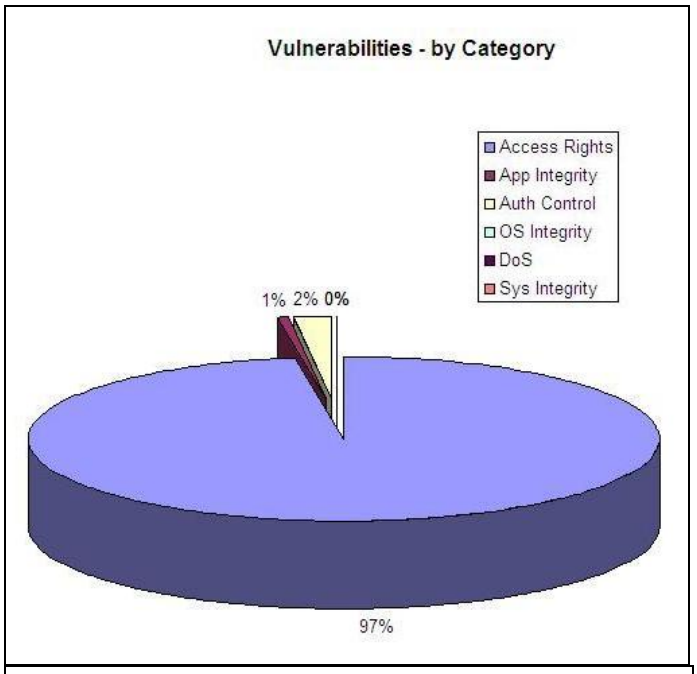
Most of us know Oracle as a relational database that we use for conveniently storing and retrieving information but the more technology savvy know that Oracle has been aggressively following a strategy and while pursuing its vision has not only developed various solutions it has also been shopping in the market and has positioned itself additionally as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), Human Capital Management (HCM), Project Management (PM), Financial Management (FM), Corporate Performance Management (CPM) and Identity & Access Management (IAM) system.

A publication released by Gartner Research titled "Oracle Acquisitions Could Change the IAM Landscape" (ID Number: G00136459) in November 2005 has commented in following manner "*By acquiring vendors with full-featured user-provisioning and virtual-directory products, Oracle has demonstrated its commitment to identity and access management (IAM), and could produce a powerhouse IAM offering*" and it goes further by suggesting that "*Oracle's offering of IAM products now pushes ahead of other IAM competitors such as BMC, Computer Associates International, Hewlett-Packard, IBM, Microsoft, Novell and Sun Microsystems*".

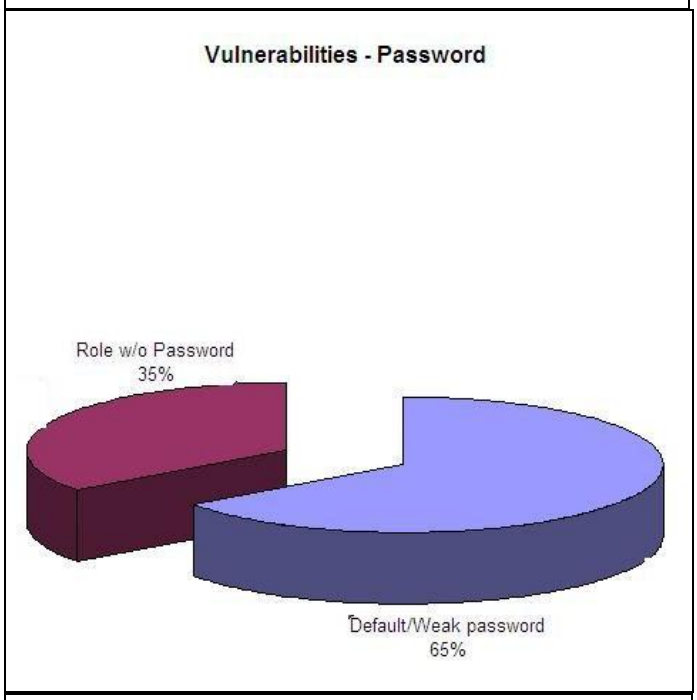
There is no doubt that Oracle has a wide range of very sound products and solutions and with ever increasing need for compliance to various legislations and to manage large amount information assets enterprises will depend more and more on integrated solutions that provide secure storage, retrieval and more so, fool-proof methods for identification of the users and controlled access to these assets.

What is demonstrated in the following section is in no way an attempt to evaluate any particular product but the intent is to emphasize on the need to extensively train IT professionals and to provide them good tools to continuously monitor and close any back-doors to enterprise's infrastructure.

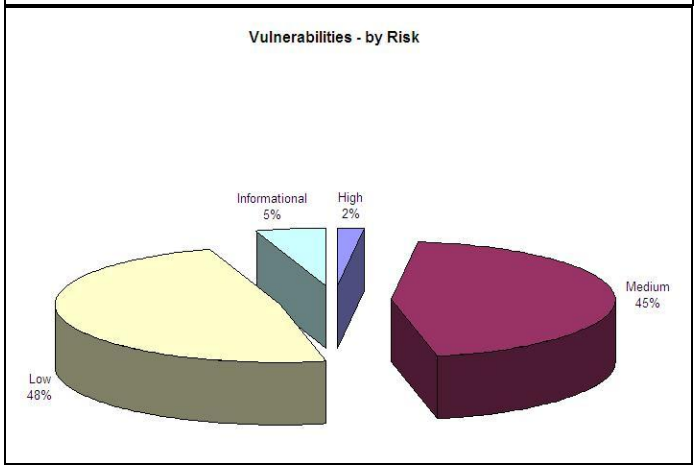
Now to tell the story of how the professionals and decision makers can live with a false sense of security I would like to share some figures collected (courtesy Secure-bytes Inc.) and compiled from various tests done in Pakistan. Though the sample is relatively small but represents top few institutions from both the private and public sector.



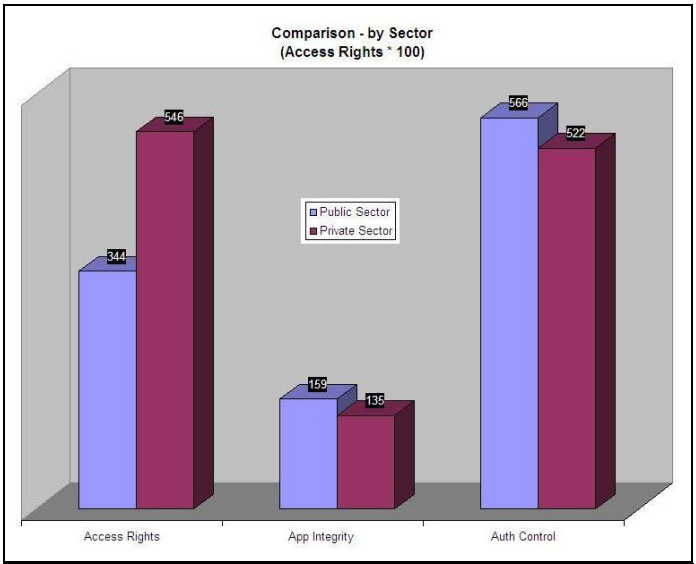
This first chart shows the categories of vulnerabilities for which the Oracle installations were tested. And the result clearly shows that most of the vulnerabilities were found in management of access rights



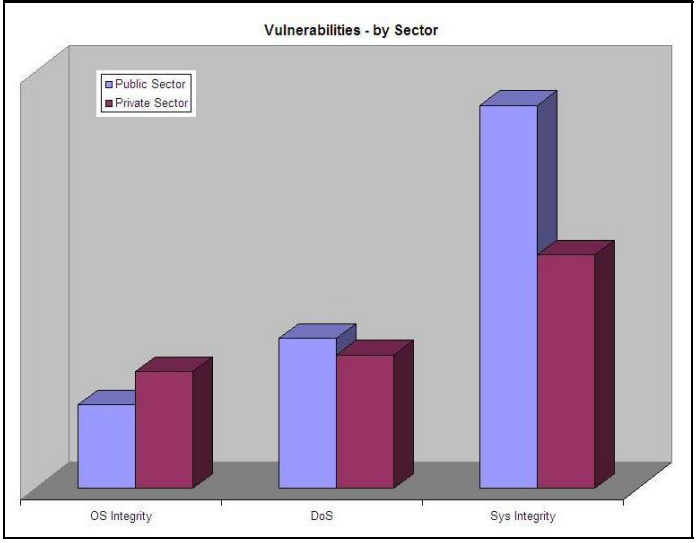
The second chart shows the resulting percentage of default and weak passwords compared to percentage of roles that existed without passwords.



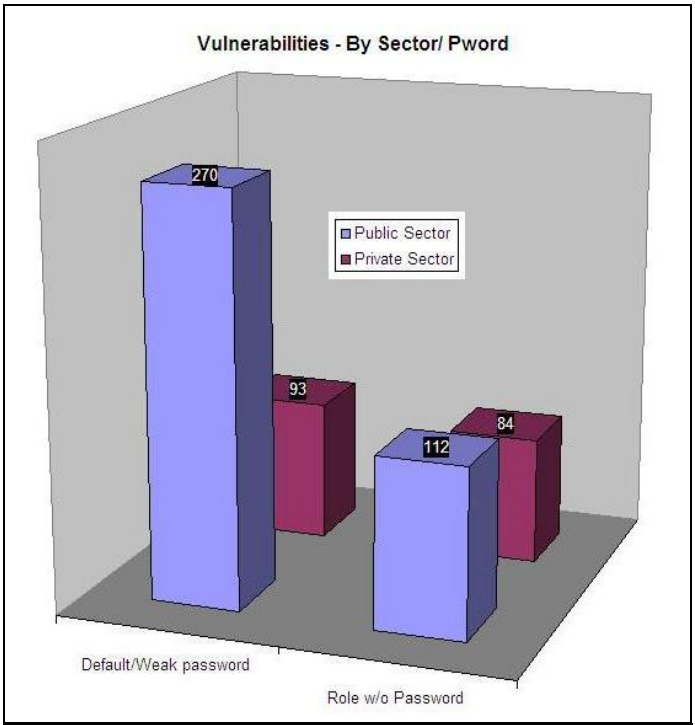
The adjacent chart (#3) shows percentages for various levels of risk. And it is clear that 93% of the vulnerabilities lie in medium and low risk levels



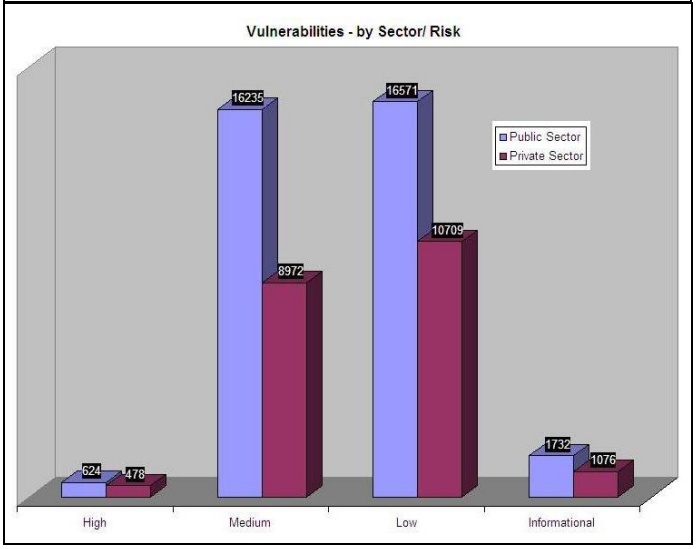
This chart (#4) illustrates a comparison between the public sector institutions and private sector enterprises. In the areas of application integrity and authorization control both stand side-by-side but surprisingly access right vulnerabilities in private sector have surpassed the public sector.



Another chart (#5) comparing private sector enterprises against public sector institutions shows that both sectors are equally vulnerable in OS integrity and DoS but public sector is clearly weaker in total system integrity.



We have earlier shown that 97% of the vulnerabilities lie in the category of access rights where public sector institutions performed better. The adjacent chart (#6) clearly shows public sector institutions taking a lead in both default/weak passwords and roles without passwords.



Last but not the least this chart (#7) provides a comparison between public sector institutions and private sector enterprises in vulnerabilities categorized by level of risk. And public sector is clearly shown weaker in all vulnerabilities, and as we have noted earlier low and medium risk levels constituted 93% of all vulnerabilities.

To conclude, what is evident from the above is that Oracle undoubtedly is pursuing a vision and aggressively positioning itself as an integrated solution provider. Like with any system we need tools, expertise and policies to continuously monitor the state of our systems and take measures to improve the security and convenience in accessing the information in an enterprise. Security is relative and has always been inversely related to ease of access.

It is also clear that extensive integration and complexity of the systems is making it an uphill task for enterprises to monitor and audit these systems, consequently the institutions also need to continuously invest in tools and building expertise and human capital. Unfortunately understanding of such dire need is rare in the decision making circles.

Mustafa Syed, M.Sc. Software Development, 30+ years IT related local & foreign experience, extensive experience of data centre operations, networking, software development, business and product development, currently holding position of Technical Support to CEO. Email: Mustafa@nift.com.pk, Web: www.nift.com.pk