Assessing DBMS Security

Afonso Araújo Neto, Marco Vieira
CISUC, Department of Informatics Engineering
University of Coimbra – Portugal
{acaneto, mvieira}@dei.uc.pt

Address:
Departamento de Engenharia Informática
Polo 2 – Universidade de Coimbra
3030 Coimbra, Portugal
Telephone: +351 239 790 000
FAX: +351 239 701 266

Keywords: Benchmarking, security, DBMS, security assessment.
Duration: Half day

1. Objective

Databases play a central role in the information infrastructure of most organizations and it is well known that security aspects must be an everyday concern of a database administrator (DBA). Typical Database Management Systems (DBMS) offer several mechanisms to protect data (e.g., user privileges, data encryption, authentication, auditing, etc.). However, in most DBMS, the effectiveness of those mechanisms is largely dependent on their actual configuration. Tuning a large database for high security is a very complex task that requires a lot of expertise and hard work. An additional difficulty is that database administrators, although having a very clear perception of the available functionalities and corresponding settings, seldom have feedback on how good a given configuration is concerning security aspects.

In this tutorial, we will present, explain and discuss ways to assess and enhance the security of DBMS installations. The tutorial is presented from a database administrator perspective, focusing on the aspects that are under the grasp and responsibility of a typical DBA: engine configuration and installation alternatives, definition of how applications, developers and users should interact with the DBMS, among other elements. We also present typical threats a DBA should have attention to, and discuss in what conditions they are or are not particularly important. Teaching how to assess and adequately avoid such threats is the main goal of this tutorial, which is centered on a research study that defined 64 generic security best practices for relational DBMS installations [1][3][4] and 8 typical DBMS security threats [2]. Moreover, we explore research opportunities that can be easily spotted in this particular domain.

2. Target Audience

The intended audience of this tutorial is researchers and practitioners interested in learning existing approaches to assess and enhance the security of DBMS installations. In addition to researchers, both database administrators and applications' developers can benefit from the tutorial, as a broad range of security topics is covered. No particular security knowledge is required, while in fact we also discuss and present methods of evaluating the security of DBMS installations without requiring security expertise from the evaluator's part. An overall knowledge of relational databases is expected.

3. Outline

In this tutorial we will discuss a range of topics concerning security of DBMS installations, from generic overviews to specific security discussions, along with some research approaches. The main outline for the tutorial is as follows:

1. **Contextualization and Introduction to key concepts:** We start by presenting an overview

and key concepts concerning of security of databases (of particular importance is the raise of security threats against web applications). The pervasiveness of software vulnerabilities in today's applications makes the correct configuration of the DBMS engine the last defense barrier between user's data and malicious attackers. We also delve in the differences between simple web applications with dedicated back-end databases to much more complex environments, such as, for instance, systems with several applications and dozens of developers interacting with a single huge database. These two types of scenarios pose different sets of problems to researchers and database administrators, and different security concerns. The main point that should be grasped by the attendees is that the correct configuration of such databases is as important as the security of the applications that utilizes it.

2. **DBMS Threats:** The threats that should be of concern to typical DBAs bear resemblance but are not exactly the same threats that a typical developer has to deal with. For instance, a DBA has very little influence on the bugs that the database engine may have, and can do little more against these than keeping the software updated with the latest vendors' patches. On the same perspective, the DBA also cannot do much against the undetected software vulnerabilities on the applications that use the database he manages. He can, however, have the system configured in such way that, in the case of a successful attack, the damage is as small as possible. Eight typical threats against databases installations are presented, and typical attacks accomplishing such threats are presented in order to serve as illustrations of the ideas presented.

3. **Security best practices:** considering 5 main categories (Environment, Installation setup, Operational procedures, System level configuration and Application level configuration and usage), we deeply explore several different security best practices for database installations, covering a wide range of aspects, that are recommended by security experts as a way to prevent security attacks. We cover what are the main ideas behind the practices, what they are expected to accomplish, what they do not accomplish, in what scenarios they make sense and, when the case, typical caveats and drawbacks. They are presented generically in a way that is applicable to any kind of relational database engine.

4. **Assessing the implementation of security practices:** In this topic we discuss practical and scientific methods for identifying the correct implementation of security best practices. Frequently, users may toggle switches in the system configuration in order to apply them, but cannot be certain that the measures are effectively in place. We discuss easy tests that can be carried out by the administrators in order to evaluate if the security practices are being correctly applied. The tests are presented in ways that require a minimal security expertise, demanding only technical knowledge about the installation being assessed.

5. **Security best practices as basis for scientific investigation:** In this topic, we present examples of scientific work that can be done based on a comprehensive set of security best practices about a domain. In particular, security best practices contain expert knowledge that can be extrapolated and be used in a variety of situations and investigations. To illustrate do idea, we present two scientific works that were based on the raw set of security best practices mentioned earlier. The first example is the development of security appraisals for database software packages (set of database plus operating system software), which allow to benchmark DBMS engine brands based on their out-of-the-box security capabilities. We also present some interesting conclusions that such appraisals might provide. In the second example we present the definition of a trust-based benchmark for a database configuration, which express the proneness of security threats to be actually explored in a target database based on the control and knowledge that the DBA has over the system configuration [2].

6. **Final discussion and closure:** In this final part we intend to foster discussion and brainstorming in order to consolidate the concepts presented before and to highlight the attendees' experiences regarding the topic. This is obviously a key part of the tutorial.

This tutorial intends to take the form of a class, mainly with the presentation of slides and extended discussion with the attendees. We intend to provide a small printed material with the reference to the main discussed security best practices and corresponding assessment tests. The proposers of this tutorial have a large experience on database security and assessment, having several publications in the domain.

In our opinion, this is a topic of utmost importance for researchers and practitioners working on databases, in particular reinforced by the visible lack of security specialists in most fields. In fact, the ascendance of networked information in our economy and daily lives has increased the awareness of the importance of security of web applications, and the corresponding databases they are based on. During the tutorial participants will understand in depth the key concepts behind security of databases, learn different approaches to assess and compare de security of real installations, and hopefully will be able to help cope with the problem of today's lack of security experts in this field.

The tutorial will follow a discussion-based approach (including a brainstorming activity close to the end of the tutorial). Attendees will be asked to comment on several aspects related to the topic in general and to provide their own perspective, experience and expertise in the domain. With this we intend to improve discussion dynamics and make participants to share their experience and their understanding regarding this topic.

4. Biographies

Marco Vieira is an Assistant Professor at the University of Coimbra, Portugal, and an Adjunct Associate Teaching Professor at the Carnegie Mellon University, USA. Marco Vieira is an expert on dependability benchmarking and is co-author of the first dependability benchmark proposal known – the DBench-OLTP. His research interests also include experimental dependability evaluation, fault injection, security benchmarking, software development processes, and software quality assurance, subjects in which he has authored or co-authored tens of papers in refereed conferences and journals. He has participated in many research projects, both at the national and European level. Marco Vieira has served on program committees of the major conferences of the dependability area and acted as referee for many international conferences and journals in the dependability and databases areas.

Afonso Araújo Neto has MSc. in Computer Science from the Universidade Federal of Rio Grande do Sul, Brazil, in the field of cryptography and holds a Ph.D. student position at the Department of Informatics Engineering of the University of Coimbra, Portugal, where he is finishing his PhD research in the area of Security Benchmarking of Transactional Systems. He is also an Information Technology Analyst working at Centro de Processamento de Dados of Universidade Federal do Rio Grande do Sul. Afonso has a fair amount of research experience and industry experience in the domains of security and databases.

5. References

[1] Araújo Neto, A. and Vieira, M. and Madeira, H. "An Appraisal to Assess the Security of Database Configurations", International Conference on Dependability (DEPEND 2009), Athens/Glyfada, Greece, June 2009.

[2] Araújo Neto, A. and Vieira, M. , "Appraisals based on Security Best Practices for Software Configurations", Fourth Latin-American Symposium on Dependable Computing (LADC 2009), João Pessoa, Paraíba, Brazil, September 2009.

[3] Araújo Neto, A. and Vieira, M. , "Benchmarking Untrustworthiness: An Alternative to Security Measurement", International Journal of Dependable and Trustworthy Information Systems, Vol. 1, # 2, pp. 32-54, IGI Publishing, April 2010.

[4] Araújo Neto, A. and Vieira, M. , "Towards Assessing the Security of DBMS Configurations", IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2008), Anchorage, USA, June 200824 (2), pp.125-36, February 1998.