# DATABASE SECURITY POLICIES FOR INTERNET ARCHITECTURE

**Dorin Iordache**
Lecturer eng., Romanian Naval Academy “Mircea cel Bătrân”
Fulgerului nr.1, Constanta, 8700, Romania
email: diordache@seanet.ro

**Abstract**
Databases introduce a number of unique security requirements for their users and administrators. On one hand, databases are designed to promote open and flexible access to data. On the other hand, it’s this same open access that makes databases vulnerable to many kinds of malicious activity. This article is the first in a series that will look at a number of database-specific security concerns and guide you as you attempt to steer your databases clear of these obstacles.

Threats, vulnerabilities, and attacks for operational safety can be caused by both unauthorized and authorized activities of some database users. For this reason, it is important to build a security database management systems. The recent expansion in communication and data distribution networks has resulted in a range of new security threats. The Internet architecture generates new threats, new problems that have to solve.

*Key words*: database security, authentication, security, information security.

## INTRODUCTION

Internet systems are very complex, they involve a variety of machines, operating systems, languages, and applications exchanging information using a rather simple protocol. The complexity of the systems involved and the limitations of the typical protocols used provide ample opportunities for hackers to attack these systems.

Security is a journey, not a destination. You should never assume that any product or technique is secure, because you can't possibly know what new attacks will become possible in the future. Many security vulnerabilities aren't published because attackers want to delay a fix, and manufacturers want to avoid negative publicity. There's an ongoing and unresolved debate over whether publishing security vulnerabilities encourages or helps prevent further attacks.

Over the last ten years, organizations have embraced Intranets and Extranets enthusiastically. This is not surprising. Intranets and Extranets offer clear cost savings and ease of installation compared with older leased line networks or WANS based on proprietary technology. Furthermore, they enable highly productive and cost effective new ways of working. Organizations can use Intranets and Extranets to distribute information more cost effectively and in a more timely manner. They can use them to build a wide range of self-service applications that help reduce administrative costs. And, they can use them to improve collaboration among employees across the organization and with business partners.

When we analyse the information security system we must consider the following questions:

- How real are the threats?
- Can easy access information the employers?
- The information can be secure transmitted through network? How can the institution fight against unauthorised access?
- How, when and what information access the users?
- How institutions administrate that wide system?

Information security is huge and wide subject and it covers a lot of imperfections. In few words, the security information assures the necessary mechanism against unauthorised users.

The information that has to protect is:

- Complex: classified or protected information;
- Simple: computer address, employee address or email address, etc.

## SYSTEM SECURITY ENGINEERING

Determination of security requirements and mitigation of threats, vulnerabilities, and attacks are nontrivial activities for most computer systems. To deal with this problem, a new discipline has emerged in the security community known as system security engineering. This discipline allows one to determine the optimal approach for a particular system based on an identification of all relevant factors and impediments to security.

The system security engineering suppose the following process [AMO94], shown in figure 1:

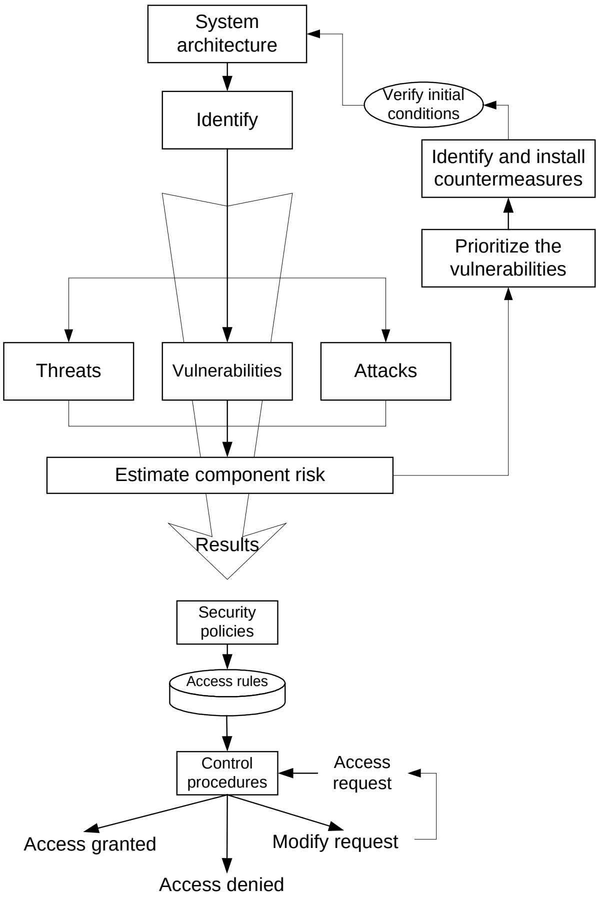

Figure 1. System security engineering

In order to define a good security policy is necessary to determine basic threats that may be present on a computer system and the associated vulnerabilities and attacks that make such threats possible.

In short terms, the security [SUM97] is the protection against:

- Illegal (unauthorized) data disclosure (*confidentiality*)
- Illegal data modification (*integrity*)
- Illegal data destruction
- Denial of service

and type of attacks:

- Viruses and worms [COH94, KAN00];
- Web site defacing and hijacking [YAH00];
- Illegal access to information [CHI00, GAR97];
- Privacy violations;
- Denial of service [FAR00];
- Cyberterrorism;
- Spam activities, etc.

In order to understand the database security policies it is possible to visualise the structure of a computer system as a hierarchic set of levels. These levels correspond to the levels of the structure of the software / hardware architecture.

## DATABSE SECURITY MECHANISM

Database security mechanism normally is applied to one or more of these levels, as follow:

- At the physical or network level. At this point, cryptographic protocols may be applied. It corresponds to the management of the files system.
- At the Operating System (OS) we have memory protection and file rights.
- At the DBMS level. There is many authorisation models that have been proposed. [DENN82, DION81, CAST94, IORD01, HRU76].
- At the application level it can be define authorisations using the conceptual model of the system, and other functionality users procedures, including visual cryptography.

In the case of the INTERNET architecture we can interpret these levels as shown in figure 2.

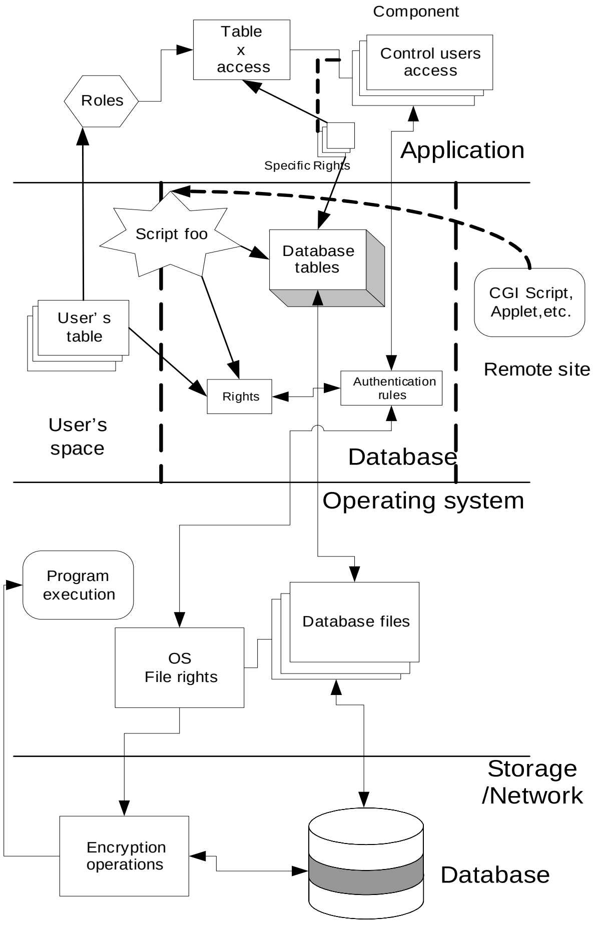

Figure 2. Security levels for Internet architecture

The database Internet structure is defined based on security levels shown in figure 2. In that way, the database designer answers the information security system questions. So, he can build the database security policy.

## DATABASE SECURITY POLICY

The policy power consists in the institution capability for implementing a strategic users access control plan. This plan has to contain practical solutions in order to solve the threats, vulnerabilities, and attacks detected.

The security policy advert to:

1. Access control:
   - Users authentication;
   - Interaction authorised between users and protected information.
2. Firewall:
   - In order to decide the rules of access.
3. Management and administration instruments:
   - Centralised management;
   - Administration ( creation, sustenance, and deletion users and their rights);
   - User's activities account.
4. Audit, monitoring , and warning technologies:
   - Recording system events;
   - Monitoring the whole activities;
   - Automatic notification of a pre-set or unusual event.
5. Antiviral solution:
   - For prevention, detection and/or virus signature correction or his effects.
6. Cryptographic technologies:

   to assure:

- Privacy;
- Integrity;
- Non-repudiation,

through software and hardware mechanisms.

7. Management cryptographic key technologies:
   - In order to assure the cryptographic support for coding and digital signature:
     - generate,
     - emitting,
     - revoke,
     - destroy

   cryptographic keys.

8. Increasing level for users authentication technologies:
   - Hardware devices such as smartcard, fingerprint, etc. for intruder detection:
   - Network scanning for network security attacks detection;
   - Incidents detection.
9. Physical level security:
   - Physical access.
10. Advise:
    - To establishing a proper security policy;
    - To designing, selecting, implementing, and setting a proper environment of security.

For example, in order to user's access control, we can use de visual cryptography elements.[NSH94, IORD01, STIN98, STA98] as it is shown in figure 3.:

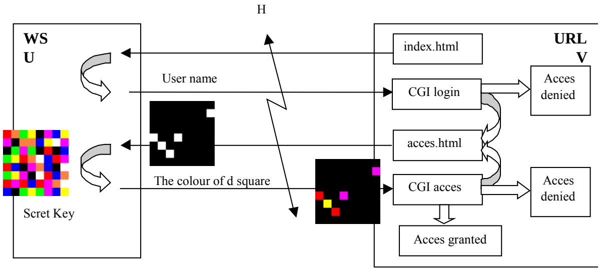

Figure 3. Visual cryptography applied

Also, this method can be used against operations over Internet architecture that are execute by a program or application, without human presence.

If the database designer and database administrator has answers or solutions for every issue of the security policy we can say the database security system is secure or the security is improved.

## CONCLUSIONS

The complexity and variety of the database Internet will continue to increase. New technologies will become widespread and bring along new problems. Attacks will increase, with new modes of attacks that generates new vulnerabilities. What this means is that the Internet as a whole will continue being insecure and the most we can do is to secure our own systems. This also means that there are ample opportunities for research and for new products.

To implement the security policy, the designer should consider:

- Design or rebuild de database system structure;
- Identify the threats, vulnerabilities, and attacks;
- Estimate component risks;
- Identify and install countermeasures;
- Implement countermeasure for every issues of security policy;
- Estimate financial costs.

We propose here a methodology to coordinate database security mechanisms that should increase total system security. The idea is to define a set of issues. The designer should find answers for almost all of them.

## REFERENCES

AMO94 Amoroso E. 1994, *Fundamentals of Computer Security Technology*, Prentice Hall International Editions

CAST94 Castano S., Fugini M.G., Martella G., Samarati P., 1994, *Database Security*, Addison-Wesley Publishing Company

CHI00 M. Chittenden, *Hackers tap into 24,000 credit cards*, *The Sunday Times*, UK, June 25, 2000.

COH94 F. Cohen, *A short course on computer viruses (2nd Ed.)*, J. Wiley,1994.

DENN82 Denning D.E. 1982, *Cryptography and Data security*, Addison-Wesley,

DION81 Dion L.C. 1981, *A Complete Protection Model*, in proceedings IEEE Symp. on Security and Privacy, Oakland, CA

FAR00 R. Farrow, *Distributed denial of service attacks*, *Network Magazine*, March 2000.

GAR97 S.Garfinkel and G.Spafford, *Web security and commerce* , O'Reilly and
Assocs., Inc., 1997.

HRU76 Harrsion M., Ruzzo W.L., Ullman J.D. 1976, *Protection in Operating System*, Communications of the ACM, vol 19

IORD01 Iordache D. 2001, *Amenințări asupra securității sistemelor de calcul*, Buletinul ştiințific al ANMB nr. 3-4

IORD01 Iordache D. 2001, *Detecția intruşilor într-o rețea UNIX ( LINUX )*, Buletinul Ştiințific al ANMB, nr. 1

IORD01 Iordache D. 2001, *Modele de securitate pentru bazele de date*, Buletinul ştiințific al ANMB nr. 2

KAN00 M. Kane, *ILOVEYOU e-mail worm invades PCs*, *ZDNet News*, May 4, 2000.

NSH94 Naor M. şi Shamir A., *Visual Cryptography*, Lecture Notes in Computer Science LNCS 950, Advances in Cryptology: EUROCRYPT'94, Springer-Verlag, 1994, pp. 1-12.

SANDHU S. Oh, R.Sandhu, *A Model for Role Administration Using Organization Structure,* http://www.list.gmu.edu/confrnc/sacmat/sacmat02-oh.pdf

SCOT03 Scott N. 2003, *Database security: protecting sensitive and critical information,* http://www.infosyssec.org

STA98 Stallings W., *Cryptography and Network Security: Principles and Practice*, Prentice Hall,1998, pp. 26-28.

STIN98 Stinson D., *Visual Crytography and Threshold Schemes*, Dr. Dobb's Journal, April 1998, pp.36-43.

SUM97 R.C.Summers, *Secure Computing: Threats and Safeguards*, McGraw-Hill, 1997.

TIPT97 Krause M., Tipton H. 1997, *Handbook of Information Security Management,* CRC Press LLC

TSICH77 Tsichritzis D., Klug A. 1977, *DBMS framework report of the study group on database management systems,*AFIPS Press

ULLM80 Ullman J.D. 1980, *Principles of Database Systems*, Computer Science Press

WOOD79 Wood C., Summers R.C., Fernandez E.D. 1979, *Authorization in Multilevel Database Models*, Information Systems Pergamon Press, vol. 4

YAH00 *Yahoo Asia News*, *Hackers force Hong Kong government website to shut down for second time*, June 11, 2000.