Cesar Cerrudo

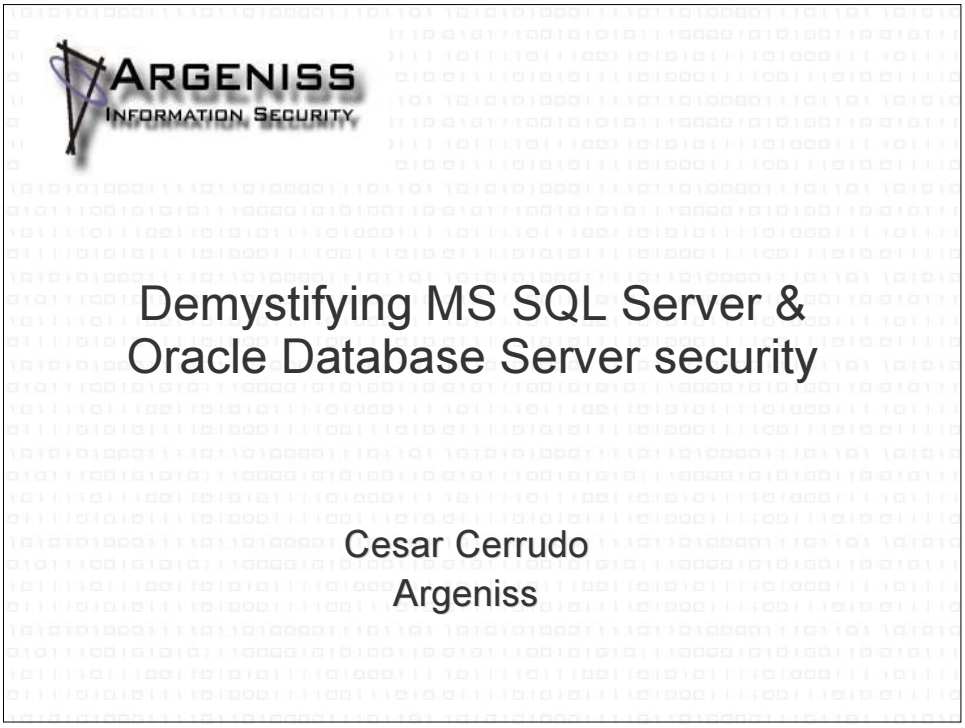
Argeniss

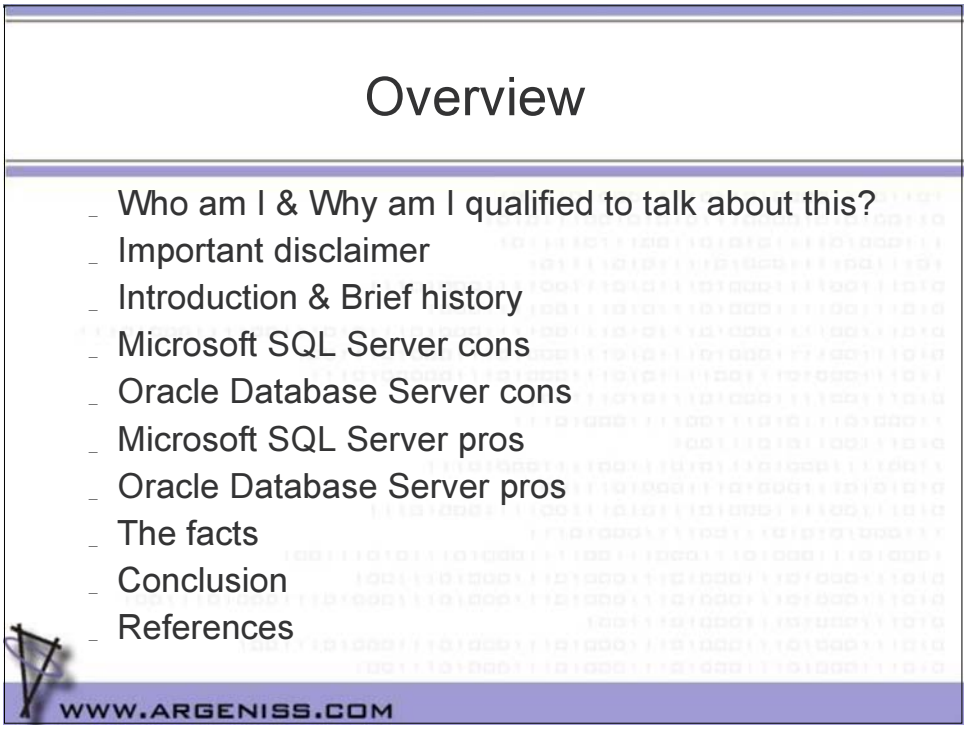
BLACK HAT BRIEFINGS

Demystifying MS SQL Server & Oracle Database Server Security

Databases are where your most valuable data rest, when you use a database server you implicitly trust the vendor, because you think you bought a good and secure product. This presentation will compare MS SQL Server and Oracle Database Server from security standpoint, comparison will include product quality, holes, patches, etc. This presentation will also show how both vendors manage security issues and how they have evolved over time. The main goal of this presentation is to kill the myths surrounding both products and let people know the truth about how secure these products are.

Cesar Cerrudo *is a security researcher specialized in application security. Cesar is running his own company, Argeniss. Regarded as a leading application security researcher, Cesar is credited with discovering and helping fix dozens of vulnerabilities in applications including Microsoft SQL Server, Oracle database server, Microsoft BizTalk Server, Microsoft Commerce Server, Microsoft Windows, Yahoo! Messenger, etc. Cesar has authored several white papers on database and application security and has been invited to present at a variety of companies and conferences including Microsoft, Black Hat, Bellua and CanSecWest.*


ARGENISS
INFORMATION SECURITY
Demystifying MS SQL Server &
Oracle Database Server security
Cesar Cerrudo
Argeniss


Overview
Who am I & Why am I qualified to talk about this?
Important disclaimer
Introduction & Brief history
Microsoft SQL Server cons
Oracle Database Server cons
Microsoft SQL Server pros
Oracle Database Server pros
The facts
Conclusion
References
WWW.ARGENISS.COM

Who am I & Why am I qualified to talk about this?

- Security researcher/consultant, software architect.
- Running own company: “Argeniss”.
- Strongly audited MS SQL Server (almost half year)
  - Found +40 security holes.
- Superficially audited Oracle DB Server (one month)
  - Found +20 security holes.
  - Esteban (talking in the other room) found +140 (a bit deeper audit) and he continues finding more...
- Dealt with both companies.
- Have been in the security arena for 5 years.

WWW.ARGENISS.COM

Important disclaimer

Opinions and comments here are from personal experience or first hand information.

This study is not paid for by Microsoft or Oracle.

WWW.ARGENISS.COM

Introduction

The media and advertising has a strong influence over people.

- Most of the time people buy what they read.
- Information is not always true.
- Causes loss of money and credibility to companies.
- Causes misinformation and propagation of myths.

Over the latest years there have been a myth about the security on databases servers:

"MS SQL Server is very insecure"

"Oracle Database Server is very secure"

"Oracle Database Server is much more secure than MS SQL Server"

WWW.ARGENISS.COM

Introduction

During this presentation I will show "real" information related to MS SQL Server and Oracle Database Server that impacts on security.

This talk is not about security features.

This talk is about all important aspects that are related to security.

At the end of this presentation you will know the truth about how secure both products are nowadays.

WWW.ARGENISS.COM

Brief history

2000-2001

- Database security starting to get more attention.

Late 2001 early 2002

- Voyager Alpha Force aka Cblade aka dnsservice.exe Worm
  - First MS SQL Server worm.
  - Exploit blank sa password.
- Oracle launches “Unbreakable” campaign.
- Microsoft launches Trustworthy Computing Initiative.
- MS SQL Server security issues start to call media attention.
- By this time I started to audit SQL Server.

WWW.ARGENISS.COM

Brief history

2002

- Spida MS SQL Server worm.
  - Second MS SQL Server worm.
  - Exploit blank sa password.
- MSRC bad days.
- MS released 12 security bulletins related to SQL Server and SP3 is released.
  - 2 remotely exploitable vulnerabilities.
  - Fixed the +40 vulnerabilities found by me.
    - After a couple of months of initial report.
- Worst MS SQL Server year.

WWW.ARGENISS.COM

Brief history

2002

- MS SQL Server security push
  - 3 months dedicated to security.
  - Claimed Most bugs fixed.
- Oracle released 9 security alerts related to database servers
  - 7 remotely exploitable vulnerabilities.

Brief history

2003

- Slammer/Sapphire Worm
  - Third MS SQL Server worm.
  - Exploits UDP port 1344 buffer overflow.
  - Patch for the overflow was available 5 months before.
- MS released 2 security bulletins related to SQL Server.
  - NO remotely exploitable vulnerabilities.
- MSRC improve.

Brief history

2003

- Oracle released 9 security alerts related to database servers.
  - 5 remotely exploitable vulnerabilities.
- By this time I started to audit Oracle
  - Found +20 security holes.
- Oracle security response center
  - No fast response (send an email and wait for weeks).
  - Is there one?
  - Amateurs running it?

WWW.ARGENISS.COM

Brief history

2004

- MS released 1 security bulletin related to SQL Server.
  - NO remotely exploitable vulnerabilities.
- Oracle released 4 security alerts related to database servers.
  - 3 remotely exploitable vulnerabilities.
  - Fixed most of the vulnerabilities found by me
    - After 10 months of initial report.

WWW.ARGENISS.COM

Brief history

2005

- No security bulletins related to MS SQL Server.
- No MS SQL Server unpatched vulnerabilites.
- Oracle released 2 critical patch updates related to database servers.
  - 13 remotely exploitable vulnerabilities.
  - Fixed a vulnerability found by me
    - After 15 months of initial report, no credit given.
  - Fixed some vulnerabilities found by Esteban
    - One of them after "1 _ year" of initial report.
- Still >100 of unpatched vulnerabilities on Oracle Database Server.

WWW.ARGENISS.COM

Brief history

In last three years

MS SQL Server
- 3 worms
- 15 security bulletins
- 2 remotely exploitable vulns
- 3 months security push

Oracle Database Server
- 0 worms
- **24** security alerts
- **28** remotely exploitable vulns
- Security push?

Today

MS SQL Server
- 0 unpatched vulnerabilities

Oracle Database Server
- **>100** unpatched vulnerabilities

WWW.ARGENISS.COM

Microsoft SQL Server cons

- Weak default installation
  - Improved after SP3.
- Many internet facing SQL Servers
  - Weakly deployed
    - Blank passwords.
    - Unpatched servers.
  - Juicy targets for worms.
- 3 worms in a year lapsus
  - Lots of money losses.
  - Make grow SQL Server bad security reputation.
- Mass media attention.

WWW.ARGENISS.COM

Oracle Database Server cons

- Weak default installation
  - Almost not improvement on 10g.
- Lots of vulnerabilities
  - Many remote ones.
  - Many unpatched ones.
    - Some remotes.
- Security patches sometimes are released almost a year or more after a vulnerability is reported.
  - Including remote vulnerabilities.
- Security patches extremely difficult to install.
- Security patches are not publicly available.

WWW.ARGENISS.COM

Oracle Database Server cons

- No security improvements
  - Vulnerabilities that affect version 8i also affect version 10g.
  - Security QA someday?
- Unresponsive security staff
  - Some security staff seem to barely knows what a buffer overflow is.
  - Cool Oracle security staff phrases:
    - We have like 14 security certifications.
    - Who will search for overflows on protocols?
      - So no need to fix them !.
    - Can you tell us what vulnerabilities have we patched?
  - Worried more about defending (the undefending) marketing campaings.

WWW.ARGENISS.COM

Oracle Database Server cons

- Bad security response center
  - Has not significantly improved over years.
  - Sometimes it takes months to get a response.
    - Or never get a response.
  - No vulnerability status
    - You know that it's patched after the alert is released.
    - Oracle is member of Organization for Internet Safety
      - Never adopted it's guidelines!.
- Bad relation with security researchers.
  - You are lucky if you get credit.
- Vulnerability rate not reduced over years.
- No tool to check for security.

WWW.ARGENISS.COM

Microsoft SQL Server pros

- Security patches easy to install.
- Security patches are released just a couple of months after a vulnerability is reported.
- Security patches are publicly available.
- Huge security efforts
  - MS SQL Server Security push.
  - Always working on improving security.
- Improved MSRC.
- Improved relation with security researches.

WWW.ARGENISS.COM

Microsoft SQL Server pros

- Good security staff.
- Vulnerability rate reduced over years.
- Released free tool to check for security
  - Microsoft Baseline Security Analyzer.

WWW.ARGENISS.COM

Oracle Database Server pros

No internet facing Database Servers.

No worms.

No mass media attention.

14 security certifications?

Good marketing staff :)

WWW.ARGENISS.COM

The facts

MS SQL Server	Oracle Database Server
Good security staff	Unresponsive security staff
Security patches easy to install	Security patches extremelly difficult to install
Security patches released quickly after a vulnerability is reported	Security patches **not** released quickly after a vulnerability is reported
Security patches publicly available	Security patches **not** publicly available

WWW.ARGENISS.COM

The facts

MS SQL Server

- Vulnerabilty rate reduced over years
- Huge security efforts
- Improved security response center
- Improved relation with security researchers

Oracle Database Server

- Vulnerability rate not reduced over years
- Security efforts?
- Bad security response center
- Bad relation with security researchers

WWW.ARGENISS.COM

Conclusions

If you think about a Database Server that:

- Has unresponsive security staff.
- Has security patches extremelly difficult to install.
- Takes almost a year to release security patches.
- Has not publicly available security patches.
- The vulnerabiltiy rate has not significantly been reduced over years.
- Has not done enough security efforts.
- Has a bad security response center.
- Has a bad relation with security researchers.
- Has many unpatched vulnerabilities.

Why do you think this Database Server is Secure?

WWW.ARGENISS.COM

Conclusions

If you think about a Database Server that:

- Has good security staff.
- Has security patches easy to install.
- Quickly releases security patches.
- Has publicly available security patches.
- The vulnerabiltiy rate has significantly been reduced over years.
- Has done huge security efforts.
- Has improved its security response center.
- Has improved its relation with security researchers.
- Has released a free tool to check security.

Why do you think this Database Server is not Secure?

WWW.ARGENISS.COM

Conclusions

You are smart and you have the final word....

WWW.ARGENISS.COM

References

www.oracle.com/oramag/oracle/02-mar/o22insight.html
www.oracle.com/technology/deploy/security/alerts.htm
www.microsoft.com/sql/techinfo/administration/2000/security/default.mspx
www.microsoft.com/technet/security/bulletin/summary.mspx
www.schneier.com/crypto-gram-0202.html#6

References

www.appsecinc.com/resources/alerts/oracle/
www.appsecinc.com/resources/alerts/mssql/
www.argeniss.com/research.html

Warning

I have the list of 100 Oracle unpatched vulnerabilities ready, think twice before saying something ;)

WWW.ARGENISS.COM

Fin

- Questions?
- Thanks.
- Contact: cesar>at<argeniss>dot<com

Argeniss – Information Security

http://www.argeniss.com/