

# ✓ INTEGRITY ✓

*Mission Critical Applications...*  
*...Mission Critical Security*



**NCOAUG Fall Apps Training Day 2005**

---

# **Oracle Security Current Issues**

**Stephen Kost**

Chief Technology Officer  
Integrigy Corporation

# Agenda

- **Introduction**
- **Oracle Security Patches**
- **Oracle Database Password Weaknesses**
- **Oracle “Voyager” Worm**

# Integrigy Background

- **Extensive experience with Oracle Applications**
  - Founded by former Big-6 consultants with significant experience on Oracle Applications implementations in Fortune 500 companies
  - Founders recognized a major gap in all implementations – little or no security auditing done on projects
  - Integrigy has found more security bugs in Oracle Applications than anyone else inside or outside of Oracle
- **An Oracle Applications company first, a security company second**
  - Products developed to support and enhance an Oracle Applications implementation – Integrigy understands the issues and risks challenging large Oracle implementations

# References

- **Oracle “Best Practices for Securing Oracle E-Business Suite 3.0.1” – Metalink Note 189367.1**
  - Many sections written by Integrigy (see page ii)
  - Assumes at least 11.5.9 with many patches
  - Comprehensive, but contains some errors and omissions
- **Integrigy Security Guides ([www.integrigy.com](http://www.integrigy.com))**
  - “Guide to Auditing in Oracle Applications”
  - “Oracle Applications 11i Security Quick Reference”
  - “Oracle Database Listener Security Guide”
  - Integrigy security alerts and advisories
  - Previous conference presentations

# Security Perspective

- **Goal is to improve security, can't make it perfect**
- **Security is a cost/benefit proposition**
  - **Risks and threats must be understood**
- **Balance security objectives with operational realities**
- **Perimeter network is secure, but internal network is open and insecure**
- **Internal threat is greater than external threat**
  - **Insider knowledge and understanding of Oracle Applications is far greater and more dangerous**
- **If someone wants in, they can get in**

# Oracle Security Perspective

## Oracle's security focus is on 11.5.9 and 11.5.10

- Best practices document is for 11.5.9 (with many patches)
- Secure coding standard mandated with 11.5.9 and onward
- **“Unbreakable” marketing campaign does not include Oracle Applications**
  - Nor does it include 8.1.7 and 9iAS 1.0.2.2.x
  - Oracle Applications is not externally audited for security
- **Undisclosed security holes exist in Oracle**
  - Integrigy has open 11i security bugs in process with Oracle
  - Security researchers have 100+ open Oracle security bugs

# Oracle 11i Security Weaknesses – Top 5

- Oracle Applications provides “foot in the door” with the **APPLSYSPUB** and **GUEST** accounts
- Many default account passwords and default configuration settings that are not secure
  - Especially prior to 11.5.10
- All products and modules installed by default
  - In 11.5.10, 200+ modules are installed even if only a few are used
- Oracle adds, but rarely removes
  - Many upgrade “artifacts” from minor (e.g., 11.5.5 → 11.5.10) and major upgrades (e.g., 10.7 → 11i)
- Customizations result in many security issues
  - 40% of all security issues identified during our audits are related to customer customizations

# Oracle Security Patches

- Fixes security bugs in the Oracle Database, Oracle Application Server, Oracle Applications, and other Oracle products
- Types of security bugs typically fixed by a security patch –
  1. Buffer Overflows
  2. SQL Injection
  3. Permission Issues
  4. Denial of Service
  5. Cross Site Scripting
- Security patches are released as Critical Patch Updates on a quarterly basis – 4 so far = 160 security bugs
  - CPU includes anywhere from 20 to 70 bugs fixes
  - Next CPUs – January 17, 2006 and April 18, 2006

# Security Patch Process

Bug reported

**Security researcher or customer reports bug to Oracle**

- Currently, 100-200 open bugs reported by a number of independent security researchers

**Oracle researches bug**

**Oracle develops bug fix**

- Finder not allowed to test fix or even notified about fix

**Oracle may include fix in new releases and patch sets**

- No notification of security fixes to customers

**Oracle includes fix in quarterly CPU**

**From report to security patch release is 6 months to 3 years**

- Bugs are rarely fixed in under 6 months
- Time to fix is not decreasing with move to CPUs

Elapsed time on average is 18 months

Bug fixed



# Security Patch Issues

- **Oracle is forcing customers to upgrade technology stack components in order to apply security patches**
- **Independent security researchers have reported the following issues with Oracle Database and Oracle Application Server patches –**
  - **A few patches don't update the correct files – an Oracle QA issue**
    - Difficult to thoroughly test patches for all versions and platforms
  - **Some fixes for security bugs are not robust**
    - Simplistic fixes applied – only address exploit, not true problem
- **Integrigy reviews and tests Oracle Applications 11i patches**
  - **No major issues found to date**

# Security Patch Advice

## ■ General advice –

- Apply the Database patch – cumulative for all CPUs and previous security alerts
- Apply Oracle Applications patches – not cumulative, must apply all patches from all previous CPUs
- Evaluate the effort to apply Developer 6i, Application Server, and JInitiator patches – depending on risk and effort, delaying these patches may be warranted

## ■ Specific advice –

- Integrity releases guidance for each CPU on our website
- Each CPU has unique issues and requirements, thus need to be evaluated independently

# Oracle Database Passwords

- **Standard Oracle passwords are a limited character set**
  - A...Z, 0...9, and \_ # \$
  - Passwords must start with an alpha character
  - More complex passwords can be set by enclosing the password in double quotes, however, many programs do not support these types of passwords
- **Oracle Password algorithm is published on the Internet**
  - Algorithm uses two cycles of DES encryption with the Username to produce a one-way hash of the password
  - Hash is unique to the username, but common across all versions and platforms of the Oracle database
  - APPS/APPS is always D728438E8A5925E0 in every database

# Cracking Database Passwords

- A number of efficient and quick password cracking programs exist for Oracle
  - Speed is around 1 million passwords per second
  - Only the hash and username are required
  - Estimated time to crack a password of x length –

<u>Length</u>	<u>Permutations</u>	<u>Time</u>
1	26 (26)	0 seconds
2	1,040 (26 x 39)	0 seconds
3	40,586 (26 x 39 x 39)	0 seconds
4	1,582,880	1.5 seconds
5	61,732,346	2 minute
6	2,407,561,520	40 minutes
7	93,894,899,306	1 day
8	3,661,901,072,960	42 days
9	142,814,141,845,466	1,600 days
10	5,569,751,531,973,200	64,000 days

# What does this mean to Oracle Applications?

- **Weaknesses in the Oracle password algorithm have been well publicized recently**
  - Whitepaper released (Google = weak oracle password)
  - At least 3 good password cracking programs exist
  - Assume your developers and other technical Oracle staff know this information
- **Prior to 11.5.10, APPLSYSPUB and any user with SQL\*Net access to the database can retrieve all database user password hashes from DBA\_USERS**
  - 11.5.1 to 11.5.9 – O7\_DICTIONARY\_ACCESSIBILITY = TRUE
- **Database passwords may be the same in production and development**
  - Must change all the database passwords after cloning

# Oracle “Voyager” Worm

- **10/31 – Source code for a proof of concept worm was released with title “Trick or treat Larry”**
  - Not really a worm – really a program to scan for unsecured databases to compromise
  - Nothing new and does not exploit any security vulnerabilities, except default configurations
  - Appears to be meant to embarrass Oracle
- **11/4 – Oracle releases customer update regarding Voyager worm**

“On October 31, 2005, an anonymous user published on the Internet code that attempts to take advantage of Oracle databases that have not been properly secured. As published today, no Oracle product security vulnerabilities are being exploited in this code and Oracle has had no reports of the code being used for malicious purposes. Nonetheless, it's important for customers to be aware of basic configuration steps that should be taken post-installation to help secure Oracle databases against hackers who may attempt to model more sophisticated attacks based on the code sketch.”

# What does this mean to Oracle Applications?

- **Anticipate more sophisticated and targeted worms and viruses in the future**
  - Worms targeting databases and applications are becoming more common and sophisticated
  - Oracle is a probable target because of the large install base
- **Hackers are now targeting specific organizations and industries**
  - Organized crime is much more involved and profit motive is driving many attacks (identity theft = \$50 per identity)
  - Several recent examples of companies being targeted – bypass the firewall through very targeted attacks
- **Worst case scenario – Every Oracle database in the data center is compromised**
  - What would be the impact to your organization?
  - How long would it take to recover?

# Oracle Worm Protection

- **Perform database and application hardening**
  - Change default passwords
  - Follow published hardening guidance for both database and applications
- **Change default and well known port numbers**
  - Change database listeners from 1521
  - “Security through obscurity” provides only limited protection from automated attacks
- **Limit direct SQL\*Net access to the database**
  - Use “Valid Node Checking”
  - 11.5.10 supports “Managed SQL\*Net Access”

# Summary

- **Security patches will keep coming**
  - Many unfixed security bugs and researchers are finding more
- **Relationship between Oracle and independent security researchers is deteriorating**
  - Expect more public disclosures of unfixed security bugs
  - As a customer, you are stuck in the middle
- **Threats to Oracle Applications are increasing as more information on vulnerabilities is published**
  - Insider threat is much greater than external threat
  - Many vulnerabilities are easy to exploit with limited technical knowledge

# Integrigy's Products and Services

## AppSentry™

- Security scanner for databases, application servers, and ERP packages
- Performs advanced penetration testing and in-depth security and controls auditing – performs over 300+ audits and checks on Oracle products
- Runs on any Windows PC and requires no software to be installed on the target servers

## AppDefend™

- Application firewall and intrusion prevention system for ERP packages
- Blocks common attacks like SQL injection, session hijacking, and cross site scripting
- Blocks access to unimplemented Oracle Applications modules

## Oracle Applications Security Assessments

- On-site security assessments of Oracle Applications (fixed fee and fixed duration)
- All aspects of the technical infrastructure are assessed from the technology stack (database, application server, and applications) to operational procedures to customizations.

# Contact Information

**Integrigy Corporation**  
**P.O. Box 81545**  
**Chicago, Illinois 60681**  
**888/542-4802**

**Website:** [www.integrigy.com](http://www.integrigy.com)

**Sales:** [sales@integrigy.com](mailto:sales@integrigy.com)

**Development:** [development@integrigy.com](mailto:development@integrigy.com)

**Support:** [support@integrigy.com](mailto:support@integrigy.com)

**Security Alerts:** [alerts@integrigy.com](mailto:alerts@integrigy.com)

Copyright © 2005 Integrigy Corporation. All rights reserved.