Is Your Data Secure? (better check again!)

Michael G Solomon, CISSP PMP CISM
Solomon Consulting Inc.
www.solomonconsulting.com

Agenda

- Are you secure?
- A case for security
- Risks and vulnerabilities
- Assessment tools
- Assessment walkthrough
- What's next?

Is Your Data Secure?

- How secure is your data?
  - Can you qualify your security readiness?
  - Can you justify your claims?
- How confident are you?
- Would you testify in court?
  - Why do you care?
  - Think about it . . .

You may be called on to testify!

- Ernst & Young
- Iowa State University
- NASDAQ
- Bank of America
- Authorize.net
- RSA Security
- Cryptologic
- OpenBSD

How do you measure security?

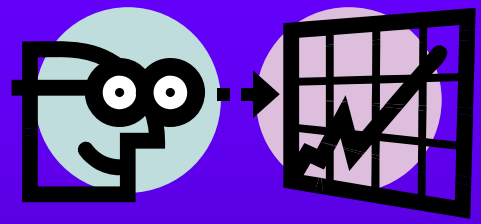
- You MUST measure security readiness
- Assess risks to your data FIRST!
  - Unless you know the risks, searching for vulnerabilities is arbitrary
- Assess vulnerabilities next
  - Vulnerabilities can allow risk to be realized
- OpenEdge® context – focus on:
  - Database – data at rest
  - Application – data in use
  - Data access channels – data in transit

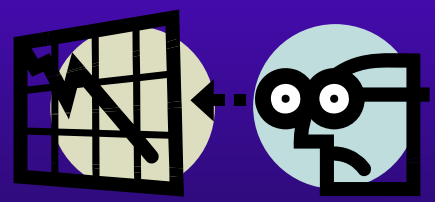
OpenEdge security considerations

- Your database is the core of your application
- You must protect your data in all states
  - At rest / at home & away
    - Consider mobile data and backup media
  - In use
  - In transit
- Data security issues
  - Confidentiality
  - Integrity
  - Availability

Business enabler

- Good security always promotes your business
  - Protect your customers' privacy
  - Protect intellectual property
  - Protect your organization's reputation
  - Protect from loss of money and time
- Will any of these hurt your business?
  - Database downtime
  - Information disclosure
  - Information modification





Successful attack consequences

- Monetary loss
  - Simple loss of sales (sometimes difficult to quantify)
- Confidence loss
  - Legal issues DO NOT matter here!
  - Rumors can kill confidence!
  - Loss of existing and new customers
- Regulatory action
  - Fines and penalties
- Legal action
  - Lawsuits and legal fees (even if you win!)

Why is it hard to ensure security?

- No clear charter
  - No stated purpose or justification
  - No risks defined
- No formal methodology
  - You must have a “method to your madness”
    - Ad hoc scanning abounds – little true value
  - Most assessments are not run as projects
    - (Hint, hint – get used to solid project management)

Assessment service types

- Vulnerability scanning
  - Hunt for specific known vulnerabilities
- Network/Application/Database security assessment
  - More expansive than a simple vulnerability scan
- Penetration testing
  - Don’t just hunt for vulnerabilities; try to realize them!
- Security audit
  - Find out if your system fulfills your security policy
  - May include vulnerability assessments and penetration testing

Project charter (PM 101)

- Justification – why are we doing this?
- Scope – how much will we do?
- Methodology – how will we do it?
- Authorization – who provides the authority?
  - And money!

Regulatory justification

- SOX – Sarbanes-Oxley
- HIPAA – Health Insurance Portability and Accountability Act
- GLBA – Gramm-Leach-Bliley Act
- FISMA – Federal Information Security Management Act
- Basel II - *International Convergence of Capital Measurement and Capital Standards*
- Contracts and SLAs
- Perhaps the most important, CYA

Risk Methodologies

- NIST
  - National Institute of Standards and Technology, document 800-30
- OCTAVE
  - Operationally Critical Threat, Asset and Vulnerability Evaluation
- AS/NZS
  - Australian/New Zealand Standard 4360:2004

Frameworks

- CobiT
  - Control Objectives for Information and related Technology
  - “ISACA IT governance framework and supporting toolset”
- ISO 17799
  - International security standard
  - “Comprehensive set of controls comprising best practices in information security”
- COSO
  - Committee of Sponsoring Organizations of the Treadway Commission
  - Model for corporate governance

Risk assessment

- Vulnerability assessment
  - Looks for risk that may be realized
  - No identified risks = no vulnerabilities!
- No risk register
  - Just shooting in the dark

Vulnerability assessment targets

- Perimeter/network devices
  - Routers/gateways/switches/firewalls
- Operating systems
  - Each OS has specific issues and weaknesses
- Databases
  - Direct or indirect access to sensitive data
- Applications
  - Generally granted direct access to sensitive data
- Personnel
  - The easiest way to your data – social engineering

Assessment methodology

- Get buy-in first – IN WRITING!
  - No written permission = BIG TROUBLE!!
- Scan/search for vulnerabilities
  - Identify IP devices/probe for active ports
  - Search for unsafe procedures/practices
  - Assess access controls and access paths
- Validate discovered vulnerabilities
- Exploitation of confirmed vulnerabilities
- Report
- Remediate
- Repeat

Assessment tools

- nmap
- Nessus
- MBSA
- nsat
- SuperScan
- Core IMPACT
- ISS Internet Scanner
- Cisco Secure Scanner
- StillSecure VAM
- epdump
- nbstat
- usrstat
- nslookup
- host/dig
- ghba

More assessment tools

- Sam Spade
- GFI LANguard NSS
- WebInspect
- appDetective
- N-Stalker/N-stealth
- CGIchk
- nikto
- SAINT
- Proactive Password Auditor
- Cain & Abel
- Effective File Search
- EtherPeek & AiroPeek
- Ettercap
- Metasploit
- Google

Unsafe data storage practices

- Removable media accessible
- Unencrypted sensitive content
  - Removable media
  - In transmission
  - At rest
- Poor cryptographic key management
  - Overused, stale, or unprotected keys
- Nonexistent/limited redundancy for critical information
- Poor security for backup storage

Most common database issues

- Weak access control
  - Operating system resources
  - Data table contents
  - Weak/stale passwords
- Weak development controls
- Lack of encryption for sensitive data
- Poor control of secondary data copies
- Weak recovery strategies

Assessment walkthrough

- Initial network scan
  - Identify all devices
  - Identify device purpose and operating system
- Open/Active port follow-up
  - Identify all running processes
  - Know which processes are generally problematic
  - Find running Progress processes
    - Look for default ports

Assessment walkthrough

- Investigate known vulnerabilities
  - Start with operating system and running services
  - Research known database/web application vulnerabilities
  - Look for data storage vulnerabilities
- Test for selected vulnerabilities
  - Choose which vulnerabilities to test
    - Project charter and risk assessment

Validate and rank vulnerabilities

- Make sure each identified vulnerability is real
  - Eliminate false positives
- Rank valid vulnerabilities by severity
  - Probability of occurrence
  - Consequence (cost) of occurrence
  - Cost of remediation

Remediate critical vulnerabilities

- Fix the “worst” vulnerabilities first
  - Highest probability of occurrence
  - Greatest impact is realized
- Keep going as long as budget and time allow
  - Get the “low hanging fruit”

Summary

- You need to assess your security
- Use a structured, repeatable approach
- Identify risks first
- Search for vulnerabilities
- Rank vulnerabilities and remediate the worst ones first

Resources

- Solomon Consulting Inc.
  - www.solomonconsulting.com
  - Vulnerability assessment services
  - Cryptographic management software
  - Progress® database and application performance enhancement
  - Roundtable® implementation and best practices assessment

More resources

- Vulnerability databases
  - Security Focus - http://www.securityfocus.com
  - Packet Storm – http://packetstormsecurity.com
  - CERT/CC – http://www.kb.cert.org/vuls
  - CVE - http://cve.mitre.org/cve
  - National Vulnerability DB - http://nvd.nist.gov
- Insecure.org Top 75 Security Tools
  - http://www.insecure.org/tools.html
- ISECOM – Institute for Security and Open Methodologies - http://isecom.org/osstmm
- SANS Top 20 Vulnerabilities List – http://www.sans.org

Even more resources

- Sarbanes-Oxley - http://www.sarbanes-oxley-forum.com/
- HIPAA - http://www.hipaa.org/
- GLBA - http://www.ftc.gov/privacy/privacyinitiatives/glbact.html
- FISMA - http://csrc.nist.gov/sec-cert/
- Basel II - http://www.federalreserve.gov/generalinfo/basel2/

Even more resources

- NIST - http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- OCTAVE - http://www.cert.org/octave/
- AS/NZS - http://www.broadleaf.com.au/tutorials/Tut_Standard.pdf
- CobiT - http://www.isaca.org/cobit/
- ISO 17799 - http://www.iso-17799.com/
- COSO - http://www.coso.org/

Where to get the tools

- Nmap - http://www.insecure.org/nmap/
- Nessus - http://www.nessus.org/
- MBSA - http://www.microsoft.com/technet/security/tools/mbsahome.mspx
- Nsat - http://nsat.sourceforge.net/
- SuperScan - http://www.foundstone.com/resources/proddesc/superscan.htm
- Core IMPACT - http://www.coresecurity.com/products/coreimpact/index.php

Where to get the tools

- ISS Internet Scanner - http://www.iss.net/
- Cisco Secure Scanner - http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csscan/csscan2/csscug/overview.htm
- StillSecure VAM - http://www.stillsecure.com
- Epdump - http://www.securityfocus.com/tools/532
- Sam Spade - http://www.samspade.org/
- GFI LANguard NSS - http://www.gfi.com/lannetscan/

Where to get the tools

- WebInspect - http://www.spidynamics.com/
- appDetective - http://www.appsecinc.com/products/appdetective/
- N-Stalker - http://www.nstalker.com/
- CGIchk - http://sourceforge.net/projects/cgichk/
- Nikto - http://www.cirt.net/code/nikto.shtml
- SAINT - http://www.saintcorporation.com/saint/

Where to get the tools

- Proactive Password Auditor - http://www.elcomsoft.com/ppa.html
- Cain & Abel - http://www.oxid.it/cain.html
- Effective File Search - http://www.sowsoft.com/search.htm
- EtherPeek - http://www.wildpackets.com/
- Ettercap - http://ettercap.sourceforge.net/
- Metasploit - http://www.metasploit.com/

Questions?


THANK
YOU