

Security, Testing and Hackers

How vulnerable is your software

Three overlapping globes showing the Americas, Europe, and Asia, serving as a background for the contact information.

Tim Pelland, A+, CSTE, CSQA
Director of Technology & Education Services
Quality Assurance Institute, Orlando, Florida
tpelland@qaiworldwide.org

© Copyright / All rights reserved January, 2008

Software Security is NOT Security Software



- A new virus is born every four hours
- 15% of all client PC's are running malware of some type
- Software security is about understanding software-induced security risk and how to manage them

Terminology



- Defect – A deviation from the specification
- Bug – An implementation-level software problem
- Flaw – A problem at a deeper level
- Risk – These capture the probability that a bug/ flaw will impact the purpose of the software



Components of Software Security



- Risk Management
- Software security artifacts
- Knowledge



Risk Management



- Understand the business context
- Identify the business and technical risk
- Analyze and rank the risk
- What is the risk mitigation strategy
- Carry out fixes



Business Risk



- The software fails to perform critical operational functions correctly
- The software fails to meet acceptance criteria required for release
- System failures cause unplanned downtime
- Security weaknesses cause system failures

Technical Risk



- Developers do not have access to QA/QC tools
- Tests do not fully evaluate requirements
- Testing does not cover fault tolerance
- System is susceptible to DOS attacks
- Poor enforcement of access control rules
- Poor password choices make system easier to attack
- System does not require good passwords

Artifacts



- Code reviews
- Architectural risk analysis
- Penetration testing
- Risk based Security test
- Abuse cases
- Security requirements
- Security operations

Terminology



- Security and Testing

- Testing that validates that the application is protected from unauthorized use
- Testing that ensures data protected from unauthorized access and/or modification
- Testing that validates network security checkpoints
- Testing that is conducted by the test team during system test or by another team specifically assembled for this purpose



System Vulnerabilities



- Firewall Configuration
- Port Scans
- Network Design
- Installed Security Devices
- Data Bases
- User ID and Passwords
- Logs
- Protocols in use
- Network host configurations

Areas of Concern: Security



- External intrusion
- Protection of secured transactions
- Viruses
- Malware
- Access control
- Authorization control



Security Requirements

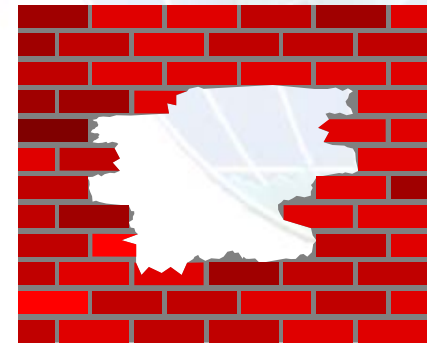


- Verify that security requirements are defined at the start of the project
- Refer to some type Security Requirements Definition Checklist to ensure all important areas have been addressed
 - Example: Do the requirements define where encryption begins and ends?
- Verify that all requirements have been stated in testable terms and are testable

Security Testing



- Security requirements must define where encryption begins and ends
- Digital Certificates, both server and client
- Additional private algorithms - must be same throughout application
- Sniffers may be required to validate encryption at start and end points
- SET or other standards



Security Testing



- Check time-outs due to inactivity
 - messages in the pipeline
 - sessions connection
 - tie to time out, not browser session
- Check impact of browser functions; disable them if necessary
 - bookmarks
 - back button
 - key or lock display open or closed?
 - view source
- Utilize intrusion experts to increase protection from “crackers”
- Frequent password changes



Security Testing



- Login logic
 - How many failed attempts are allowed?
 - Are login names and passwords stored in an encrypted format?
 - Bypass login by using a bookmark, a captured URL
 - Are logins/passwords encrypted at the application level?
- Identify points of vulnerability:
 - The client system:
 - Browser
 - Applications
 - The server side:
 - IIS, databases, other servers
 - The network
 - Online transactions
- Automatic logoffs (session timeouts)



Security Testing

- Are default passwords deactivated if a new password is chosen (for new passwords, 1st time login)?
- Are old passwords deactivated when a user changes his/her password?
- Database Server Considerations:
 - Can special access be granted to unauthorized users?
 - Is special access terminated?
 - Can users other than the database administrator create, modify, or delete stored procedures?
- Overflow buffers



Why Hackers Hack

because they can



- Hacking continues to get easier for several reasons
 - Increasing use of networks and Internet connectivity
 - Anonymity provided by computer systems working over the Internet
 - Increasing number and availability of hacking tools
 - Computer-savvy children
 - Unlikelihood that hackers are investigated or prosecuted if caught

Hackers Anonymous



- Keeping a low profile is a must
- Covering up tracks is a must
 - Borrow or steal accounts from friends or co-workers
 - Public computers at libraries, schools or kiosks
 - Internet proxy servers
 - Anonymous or disposable e-mail accounts.
 - Workstations or servers on the victim's own network
 - Open e-mail relays

What Systems to Hack



- What are your most critical systems?
- Which systems, if hacked, would cause the most trouble or greatest losses?
- Which systems appear to be the most vulnerable to attack?
- Which systems are not documented, are rarely documented?
- Which systems do you know least about?

Other Ways to Gain Information



- **Web searching**
 - Employee names and contact info
 - Important company dates
 - Presentations, articles and Webcasts
- **Web crawling**
 - Layout and configuration
 - HTML source code
 - Comment fields

Other Ways to Gain Information



- What ports are running
 - Protocols
 - Services running on the host such as e-mail or database
 - VPN Services, such as PPTP, SSL or IPsec
 - Presentation, articles and Webcasts
- Other Ports (65,535)
 - Kazaa and other file sharing applications



What You Can Do



- High level security risk assessments
- Strong security policies that are enforced
- Solid incident-response and business-continuity plans
- Effective security awareness and training initiatives

You must educate your entire staff to stay
one step ahead of the bad people



Question and Answers

