“E-Commerce: The Enemy From Within”

Trevor Price, SIM, Group, UK
Thursday 22 November 2001

T2

e-Commerce: The Enemy From Within
Trevor Price

Trevor started his career in 1971 as a telecommunications technician within a major communications company (BT). After obtaining his Open University Technology degree in 1987 he was selected and given the opportunity to move from telecommunications into I.T. as a mainframe operator. Trevor quickly moved into system support monitoring mainframe performance and the production of capacity plans. In 1990 Trevor obtained a senior performance analyst position within the performance and capacity planning team of M&S. During this time Trevor set-up the performance monitoring of Mainframes, Midrange (AS400), Distributed Systems (UNIX, NT), Networks and Databases. Also Trevor became increasingly involved in software and hardware performance testing using automated testing techniques.

In 1998 Trevor joined the SIM Group as a Test Consultant. Since working at SIM Trevor has successfully managed a number of performance, load, stress and benchmarking testing projects and has further widened his knowledge of testing by managing a number of health checks, test strategies, functional testing and end-to-end testing projects. Trevor has been assigned projects within a wide variety of industry sectors including finance, banking, retailing, software development, and health-care. Trevor has been responsible for writing two SIM Group testing methodologies titled “Performance, Load and Stress Testing Methodology” and “Infrastructure Testing Methodology”.

Trevor was promoted to Senior Consultant in February 2000. During 2000 Trevor gained certification for LoadRunner. Which is part of Mercury Interactive load and performance testing tool set.

Currently Trevor is involved in two major insurance e-commerce infrastructure-testing projects, which also includes security testing. Trevor is also involved in a number of CSSA e-commerce, security and business continuity management, special interest groups, and has more recently had articles published in both the “Professional Tester” and I.T. Finance. Of which has now been accepted as speaker at Internet World (London June 2001) and EuroSTAR (Stockholm November 2001)
e – commerce: the enemy from within

By Trevor Price

trevor.price@simgroup.com
Security Typically Focused On:

- Firewalls
- Authentication
- Encryption
- Penetration testing
- Virus scanners
- Intrusion detection systems
✓ Firewalls in place and tested
✓ Authentication in place and tested
✓ Encryption in place and tested
✓ Penetration testing completed
✓ Virus scanners in place and tested
✓ Intrusion detection system in place and tested
• Therefore the strong perception is that the site is secure. Site builders and testers proudly say they have tried everything to make sure that the security defences are working and not penetrable by cyber criminals.

BUT CAN THEY?
• The cyber criminal community refers to large companies with: firewalls, authentication and encryption as being:

Hard and Crunchy on the outside;

Soft and Chewy on the inside
Cyber Criminal Perception

- As they often put up a perimeter fortress like front door while leaving all the windows wide open by ignoring their internal site, business logic and database security
Penetration Testing

- Independent security experts
- Typically accessed via the internet
- Automated scanning tools
- Only tests for **KNOWN** software security vulnerabilities. **NEEDS TO BE UPDATED** to keep track of new variants
- Manual testing with “**ethical hackers?**” That try to gain unauthorised access
Trojan (Horse), AV’s & IDS’s

- **Trojans are the hacker’s back door in**
- **Virus scanners**
  - Can only scan for **KNOWN viruses NEEDS TO BE UPDATED** to keep track of new variants
  - Used to actively test for Trojans
- **Intrusion detection systems (IDS)**
  - The burglar alarm of the internet
  - Continually **NEEDS TO BE UPDATED** to keep track of new variants
  - Compromised by cloaking techniques created by hacker “K2” who also works as a security consultant **FRIEND or FOE?**
• The business application
  – Greater complexities of software and databases than static web sites
  – n-tier architectures
  – Large amounts of constantly changing, diverse, complex, custom and bespoke software

IS THIS SECURE, DOES IT CONTAIN LOOPHOLES

Slide 9
• **Databases**
  – Use stored procedures
    • Essentially, mini programs stored in memory
  – Organisations secure the operating systems on their database host
  – But leave the database applications themselves with little protection

**RESULT IS: THE DATABASE SOFTWARE CAN BE USED TO LAUNCH AN ATTACK**
• Trap doors
  – Developers and vendors sometimes leave behind trap doors
    • Used to test the code
    • Used to make future modifications or updates

TRAP DOORS CAN BE USED BY INTRUDERS TO BREAK IN AND STEAL INFORMATION FROM YOUR SYSTEMS
SO WHAT IS THE SOLUTION?

HOW DO YOU PROTECT YOUR BUSINESS FROM THE ENEMY FROM WITHIN
Implementing a Test Strategy
Based on Continuous Testing
Continuous Testing

- Regularly test the business application
  - Testing every possible element and combination of circumstances is absolutely essential
  - It is not enough to test only what we think the users will use, it is important to test absolutely everything possible e.g. trap doors
Continuous Testing

- Regularly perform negative testing
  - Trying things that you are not supposed to be able to do
  - Integrity of the databases. Testing with unusual combinations of data

TESTERS COULD UNCOVER "FEATURES" THAT ARE HIDDEN SECURITY RISKS, USING UNUSUAL COMBINATIONS OF DATA MIGHT UNCOVER HIDDEN SECURITY LOOPHOLES.
Continuous Testing

- **Regular stress testing (very high volumes of data)**
  - System might perform differently under stress exposing hidden security loopholes
- **Regular testing during operational incidents and events**
  - The system might perform differently while operations are fixing, running batch, backing up restores, or installing. Thus exposing hidden security risks
Continuous Testing

- Regularly perform penetration tests
  - Not forgetting to update your vulnerability database
- Regularly perform virus scans
  - Not forgetting to update your virus scanner databases
- Regularly test your intrusion detection systems
  - Not forgetting to update it
Continuous Testing

• Regularly test Denial of Service Attacks
  – The best way to verify if an e-commerce site is susceptible to a denial of service attack is by simulating it across a network under controlled conditions
Continuous Testing

• **Continuous and regular testing is important**
  - This method checks that the e-commerce site is behaving as expected and no security risks exist
  - It is directly analogous to daily internal audits measuring inventory thus ensuring that the books are in order
Conclusion

• **Testing for security is a dynamic and ongoing process**
  – Sites change rapidly
  – Technical infrastructure and networks continue to evolve constantly
  – Security risks continuously change and grow
  – No organisation can deliver secure and resilient e-commerce business services if it is not actively continually testing the infrastructure, business application, and databases
• Remember the enemy from within. If your site is Soft and Chewy on the inside because you have not continuously tested then you are

**Then you are**

*THE WEAKEST LINK*

**Goodbye**