Abstract

Defects in production software can incur heavy damage to a business operation; yet most current approaches to software security assessment focus primarily on new code development. The paper aims at introducing a strategic approach for reducing the operational security risk. The familiar top-down structured development process used by internal development groups is totally inappropriate for risk analysis of production software systems. And generally the cost of finding and fixing a bug in a production system is regarded as too high. So there is an imperative necessity to focus on approaches tailored specifically for production software systems which is the one attempted here.
2005 Breach Analysis, April 2006
http://www.software.co.il/downloads/breachAnalysis2005.xls
- Privacy Rights Clearinghouse, http://www.privacyrights.org/
- Developing Secure Software, Noopur Davis,
http://www.softwaretechnews.com/stn8-2/noopur.html
- Top-down Security”, Alan Paller,
http://infosecuritymag.techtarget.com/articles/1999/paller.shtml
- In production, it's often 100 times more expensive than finding and fixing the bug during requirements and design phase”. Barry Boehm, Victor R. Basili, IEE Computer, 34(1): 135-137, 2001
- CVSS (Common Vulnerability Scoring System) is a standard way to convey vulnerability severity and help determine urgency and priority of response, http://www.first.org/cvss/intro/
Vendors such as Cisco, Symantec and Skype use CVSS to score their own application vulnerabilities.
- CLASP (Comprehensive, Lightweight Application Security Process),
http://www.owasp.org/index.php/CLASP

Index Terms
Computer Science
Software Engineering

Key words
Risk
Production Software System
Security Risk
Vulnerability
Software Components