



Software Testing and Cyber Security

Dr. Robin Poston, University of Memphis
Nicole Samson, University of Memphis



Overview

- Target Breach
- Literature Review
- Security Testing Coverage Matrix
- Conclusion/Next Steps



Target Breach

- December 2013
- 40 Million Customers
- Vendor Portal
- POS Systems

Could Testing Have Helped?



Target Breach and Testing

- Vendor Portal
- POS Systems
- Passwords
- Responding to Alerts

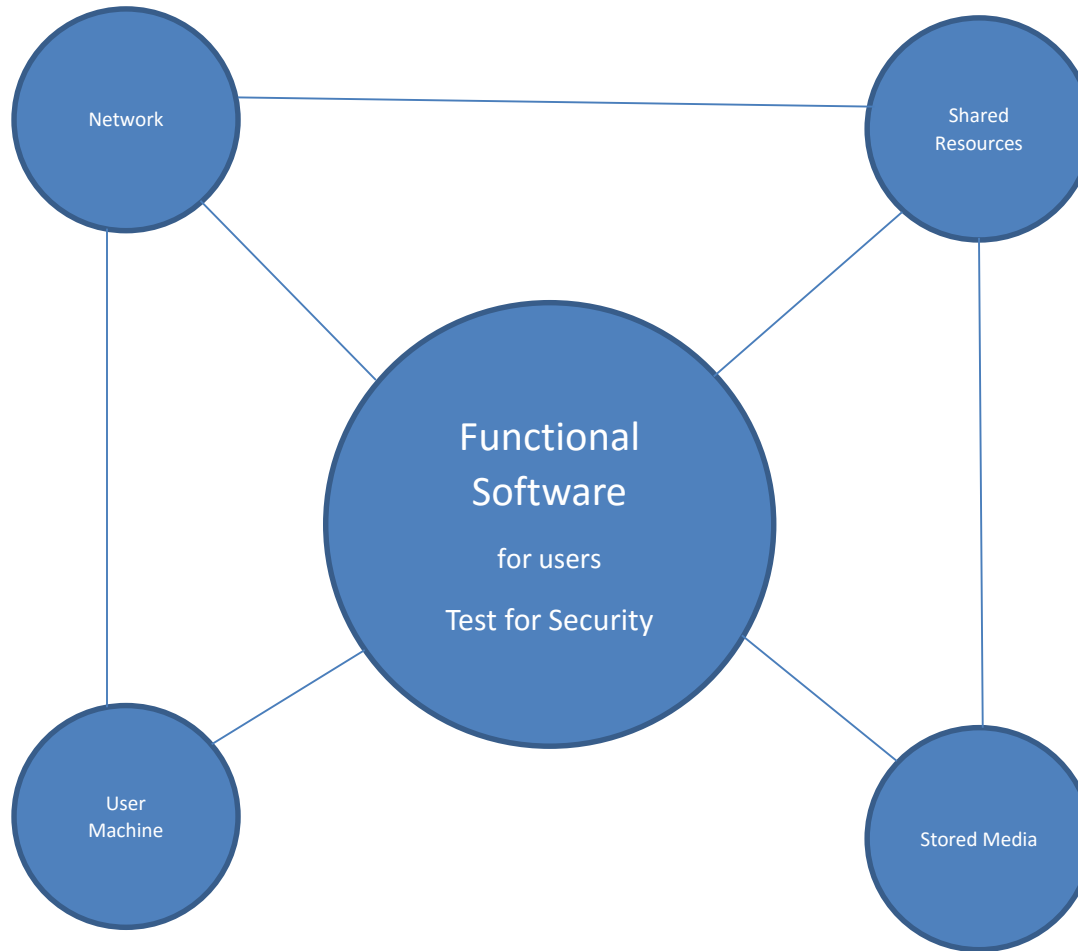


Literature Review

- Best Practices
 - National Institute of Standards and Technology (NIST) Controls
- Security Areas
- Testing Types

Resulted in focus on security and testing matrix for software development and testing regarding the robustness of built-in security defenses

Realm of Potential Security Concerns





Security Testing Coverage Matrix - Detailed

	Malware	Access Controls	Risk and Accountability Controls	Identification and Authentication Controls	Media Protection Controls	System and Communication Protection Controls	System and Information Integrity Controls
Penetration Fuzzing/Porting IP Scan and Attack Insecure Direct Object Reference Password Lookup Basic Fuzz Attack Dictionary Attack UDP Flooding Smurfing Denial of Service DDOS, SYN/DDOS SYN/DDOS Flood Attack Check Flood Spoof Trojan Horse Virus/Worm/Steer Adware Backdoor/Trojan Rootkit		Account Management Account Enumeration Password Policy Enforcement Least Privilege Separation of Duties/Segregation Privilege Least Privilege Document Control List Session Lock Session Timeout Password Aging and Complexity Password History Account Lockout Account Lockout for Failure and Multiple Attempts Use of Encrypted/Protected Systems Audit/Log Control of Audit Records Audit Storage Capacity Program to Audit Processing Failure Audit Monitoring, Analysis, and Reporting Audit Protection and Report Separation Time Storage Protection of Audit Information Access/Availability	User Identification and Authentication Secure Identification and Authentication Identity Management Authentication Management Authentication Feedback Cryptographic Secure Authentication Multi-Factor Media Labeling Media Storage Media Transport Media Sanitization and Disposal Application Patching Security Patch/Updates Information Management Control of Access Privileges Business Continuity Information Integrity Information Confidentiality Network Recovery Network Path Cryptography Use of Cryptography Public Access Privileges Confidentiality Protection of Security Properties Public Key Infrastructure Certificates Mobile Code User Controlled Physical Secure Management Resilience Tests Authentication and Authorization for Non-Interactive Resources Session Authentication File Encryption Malicious Code Protection Information System Monitoring Tools for Intrusion Security Alerts and Auditing Security Functionality Evaluation Software and Information Integrity Source Protection Information System Resilience Information Access, Configuration, Usability, and Availability User Reporting Information Output Integrity and Report				
Address Alpha Beta Boundary Value Comparison Conformance Database Equivalence Class Equivalence Happy Path Interface Invalid-Down Orthogonal Array Exhaustive Parameter Random States							
Backward Compatibility Binary Portability Device Compatibility Certification Conversion Forward Compatibility Format							
Branch Coverage Condition Coverage Data Flow Coverage Decision Coverage Edge Coverage/Gears End-to-End Test Vectors Path Coverage							
Acceptance Accessibility Field Installation/Configuration Model-Based Operational Readiness Path-Based Source Specification-Based Static							



Security Testing Coverage Matrix – Cont'd

Test Type	Test Category	Test Sub-Category	Release	Access Controls	Audit and Accountability Controls	Identification and Authentication Controls	Media Protection Controls	System and Communication Protection Controls	System and Information Integrity Controls
			Release	Access Controls	Audit and Accountability Controls	Identification and Authentication Controls	Media Protection Controls	System and Communication Protection Controls	System and Information Integrity Controls
Functional Testing	Fuzzer	Code							
		UI							
Functional Testing	Regression	Security							
		Stress							
Functional Testing	Usability	Accessibility							
		Performance							
Integration Testing	API Integration	System Integration							
		Component Integration							
Integration Testing	System Integration	Integration							
		Deployment							
Structural Testing	Code Review	Code Review							
		Documentation							
Structural Testing	Code Coverage	Code Coverage							
		Documentation							
Performance Testing	Load Testing	Load							
		Stress							
Performance Testing	Stress Testing	Stress							
		Spikes							
Misc Testing	Penetration Testing	Penetration							
		Usability							
Misc Testing	Dependency	Dependency							
		Error Handling							
Misc Testing	Logic	Logic							
		Negative							
Misc Testing	Testability	Testability							
		Code-Oriented							
Misc Testing	Component	Component							
		Deployment							



Security Testing Coverage Matrix – High Level

	Phishing/Pharming	Bot/Botnet	SQL Injection	Click Fraud	Access Controls	Audit and Accountability Controls	Identification and Authentication Controls	System and Information Integrity Controls
Black Box Testing	✓	✓		✓	✓	✓	✓	✓
Compatibility Testing					✓			
Functional Testing					✓	✓	✓	✓
Integration Testing								
Nonfunctional Testing			✓		✓	✓	✓	✓
Performance Testing							✓	
Security Testing	✓	✓	✓	✓	✓	✓	✓	✓
Operational Readiness testing							✓	
Unit Testing						✓		✓
White Box Testing			✓		✓		✓	
Coverage Testing	✓	✓	✓	✓				✓



Conclusion/Next Steps

- Using the Matrix
- Getting Expert Opinions
- Creating a Matrix for Expanded Security Testing Types Only
- Publishing Our Work