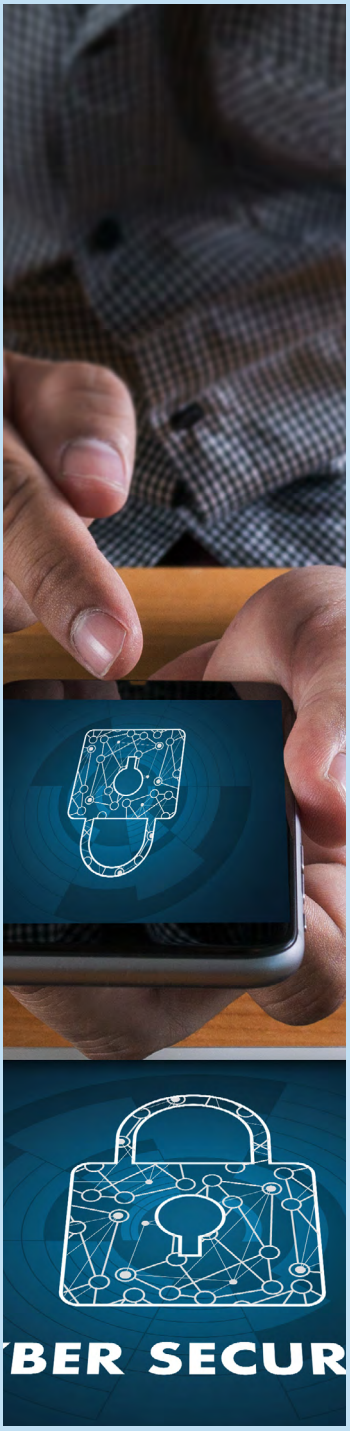
VIEW POINT



BEST PRACTICES TO ENSURE SEAMLESS CYBER SECURITY TESTING

Abstract

In a post COVID-19 world, the need to become digitally-enabled is more pressing than ever before. Enterprises are accelerating digital strategies and omni-channel transformation projects. But while they expand their digital footprint to serve customers and gain competitive advantage, the number and extent of exposure to external threats also increases exponentially. This is due to the many moving parts in the technology stack such as cloud, big data, legacy modernization, and microservices. This paper looks at the security vulnerabilities in open systems interconnection (OSI) layers and explains the best practices for embedding cyber security testing seamlessly into organizations.

Infosys®
Navigate your next

Introduction

Open systems interconnection (OSI) comprises many layers, each of which has its own services/protocols. These can be used by hackers and attackers to compromise the system through different types of attacks.

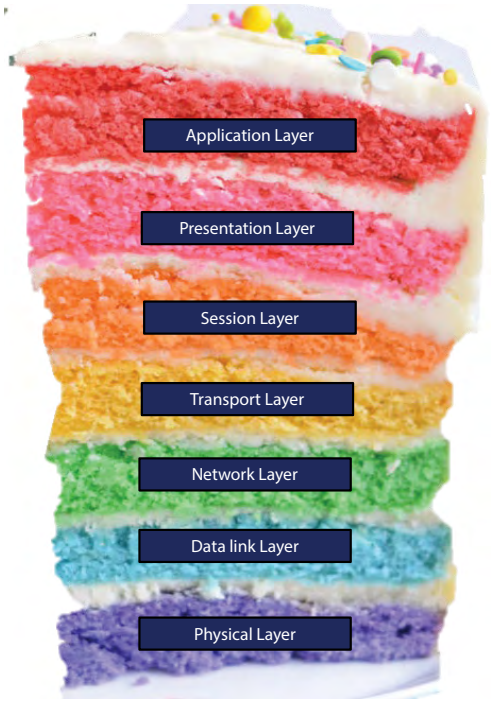
OSI Layers	Services/Protocols	Types of attacks
	File transfer protocol, simple mail transfer protocol, Domain Name System	SQL injection, Cross-site scripting software attack (persistent and non-persistent), Cross-site request forgery, Cookie poisoning
	Data representation, Encryption and Decryption	SSL attacks, HTTP tunnel attacks
	Establishing session communications	Session hijacking, sequence prediction attack, Authentication attack
	TCP, UDP, SSL, TLS - protocols	Port scanning, ping flood and Distributed Denial-of-Service (DDoS) attack
	Networks, IP address, ICMP protocol, IPsec protocol, OSPF protocol	External attacks such as packet sniffing, Internet Control Message Protocol (ICMP) flood attack,
	Ethernet, 802.11 protocol, LANs, Fiber optic, Frame protocol	Denial of Service (DoS) attack at Dynamic Host Configuration Layer (DHCP), MAC address spoofing etc.- These are primarily internal attacks
	Transmission media, bit stream (signal) and binary transmission	Data theft, Hardware theft, Physical destruction, Unauthorized access to hardware/connections etc.,

Fig 1: Points of vulnerability across OSI layers

For some OSI layers like Transport, Session, Presentation, and Application, some amount of exposure can be controlled using robust application-level security practices and cyber security testing. From a quality engineering perspective, it is important for testers to be involved in the digital security landscape.

While there is no single approach to handle cyber security testing, the following five best practices can ensure application security by embedding cyber security testing seamlessly into organizations:

1. Defining and executing a digital tester's role in the DevSecOps model
2. Understanding and implementing data security testing practices in non-production environments
3. Security in motion – Focusing on dynamic application security testing
4. Understanding the vulnerabilities in infrastructure security testing
5. Understanding roles and responsibilities for cloud security testing

Best practice 1: Defining and executing a digital tester's role in the DevSecOps model

DevSecOps means dealing with security aspects as code (security as a code). It enables two aspects, namely, 'secure code' delivered 'at speed'. Here is how security-as-a-code works:

- Code is delivered in small chunks. Possible changes are submitted in advance to identify vulnerabilities
- The application security team triggers scheduled scans in the build environment. Code checkout happens from SVN or GIT (version control systems)
- Code is automatically pushed for scanning after applying UI and server-based pre-scan filters. Code is scanned for vulnerability
- Results are pushed to the software security center database for verification
- If there are no vulnerabilities, the code is pushed to quality assurance (QA) and production stages. If vulnerabilities are found, these are backlogged for resolution

DevSecOps can be integrated to perform security tests on networks, digital applications and identity access management portals. The tests focus on how to break into the system and expose vulnerable areas.

Best practice 2: Understanding and implementing data security testing practices in non-production environments

With the advent of DevOps and digital transformation, there is a tremendous pressure to provision data quickly to meet development and QA needs. While provisioning data across the developing pipelines is one challenge, another is to ensure security and privacy of data in the non-production environment. There are several techniques to do this as discussed below:

- Dynamic data masking, i.e., masking data on the fly and tying database security directly to the data using tools that have database permissions
- Deterministic masking, i.e., using algorithm-based data masking of sensitive fields to ensure referential integrity across systems and databases
- Synthetically generating test data without relying on the production footprint by ensuring referential integrity across systems and creating a self-service database
- Automatic clean-up of the sample data, sample accounts and sample customers created

Best practice 3: Security in motion – Focus on dynamic application security testing

This test is performed while the application is in use. Its objective is to mimic hackers and break into the system. The focus is to:

- Identify abuse scenarios by mapping security policies to application flows based on the top 10 security vulnerabilities for Open Web Application Security Project (OWASP)
- Conduct threat modeling by decomposing applications, identifying threats and categorizing/rating threats
- Perform a combination of automated testing and black-box security/ penetration testing to identify vulnerabilities

Best practice 4: Understanding the vulnerabilities in infrastructure security testing

There are infrastructure-level vulnerabilities that cannot be identified with UI testing. Hence, infrastructure-level exploits are created and executed, and reports are published. The following steps give insights to the operations team to minimize/eliminate vulnerabilities at the infrastructure layer:

- Reconnaissance and network vulnerability assessment including host fingerprinting, port scanning and network mapping tools
- Identification of services and OS details on hosts such as Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP)
- Manual scans using scripting engine and tool-based automated scans
- Configuration reviews for firewalls, routers, etc.
- Removal of false positives and validation of reported vulnerabilities

Best practice 5: Understanding roles and responsibilities for cloud security testing

With cloud transformation, cloud security is a shared responsibility. Cloud security testing must involve the following steps:

- Define a security validation strategy based on the type of cloud service models:
  - For Software-as-a-Service (SaaS), the focus should be on risk-based security testing and security audits/ compliance
  - For Platform-as-a-Service (PaaS), the focus should be on database security and web/mobile/API penetration testing
  - For Infrastructure-as-a-Service (IaaS), the focus should be on infrastructure and network vulnerability assessment
- Conduct Cloud Service Provider (CSP) service integration and cyber security testing. The focus is on identifying system vulnerabilities, CSP account hijacking, malicious insiders, identity/access management portal vulnerabilities, insecure APIs, shared technology vulnerabilities, advanced persistent threats, and data breaches
- Review the CSP's audit and perform compliance checks

These best practices can help enterprises build and create secure applications right from the design stage.

Infosys has a dedicated Cyber Security Testing Practice that provides trusted application development and maintenance frameworks, security testing automation, security testing planning, and consulting for emerging areas. It aims to integrate security into the code development lifecycle through test automation with immediate feedback to development and operations teams on security vulnerabilities. Our approach leverages several open-source and commercial tools for security testing instrumentation and automation.

Conclusion

The goal of cyber security testing is to anticipate and withstand attacks and recover quickly from security events. In the current pandemic scenario, it should also help companies adapt to short-term change. Infosys recommends the use of best practices for integrating cyber security testing seamlessly. These include building secure applications, ensuring proper privacy controls of data in rest and in motion, conducting automated penetration testing, and having clear security responsibilities identified with cloud service providers.

About the Authors

Arun Kumar Mishra
Senior Practice Engagement Manager, Infosys

Sundaresasubramanian Gomathi Vallabhan
Practice Engagement Manager, Infosys

References

1. https://www.marketsandmarkets.com/Market-Reports/security-testing-market-150407261.html
2. https://www.infosys.com/services/validation-solutions/service-offerings/security-testing-validation-services.html

For more information, contact askus@infosys.com

Infosys®
Navigate your next