# SECURITY ARCHITECTURE CHEAT SHEET FOR INTERNET APPLICATIONS

This cheat sheet offers tips for the initial design and review of an application's security architecture.

## #1: BUSINESS REQUIREMENTS

### Business Model

What is the application's primary business purpose?

How will the application make money?

What are the planned business milestones for developing or improving the application?

How is the application marketed?

What key benefits does the application offer users?

What business continuity provisions have been defined for the application?

What geographic areas does the application service?

### Data Essentials

What data does the application receive, produce, and process?

How can the data be classified into categories according to its sensitivity?

How might an attacker benefit from capturing or modifying the data?

What data backup and retention requirements have been defined for the application?

### End-Users

Who are the application's end-users?

How do the end-users interact with the application?

What security expectations do the end-users have?

### Partners

Which third-parties supply data to the application?

Which third-parties receive data from the applications?

Which third-parties process the application's data?

What mechanisms are used to share data with third-parties besides the application itself?

What security requirements do the partners impose?

### Administrators

Who has administrative capabilities in the application?

What administrative capabilities does the application offer?

### Regulations

In what industries does the application operate?

What security-related regulations apply?

What auditing and compliance regulations apply?

## #2: INRASTRUCTURE REQUIREMENTS

### Network

What details regarding routing, switching, firewalling, and load-balancing have been defined?

What network design supports the application?

What core network devices support the application?

What network performance requirements exist?

What private and public network links support the application?

### Systems

What operating systems support the application?

What hardware requirements have been defined?

What details regarding required OS components and lock-down needs have been defined?

### Infrastructure Monitoring

What network and system performance monitoring requirements have been defined?

What mechanisms exist to detect malicious code or compromised application components?

What network and system security monitoring requirements have been defined?

### Virtualization and Externalization

What aspects of the application lend themselves to virtualization?

What virtualization requirements have been defined for the application?

What aspects of the product may or may not be hosted via the cloud computing model?

## #3: APPLICATION REQUIREMENTS

### Environment

What frameworks and programming languages have been used to create the application?

What process, code, or infrastructure dependencies have been defined for the application?

What databases and application servers support the application?

### Data Processing

What data entry paths does the application support?

What data output paths does the application support?

How does data flow across the application's internal components?

What data input validation requirements have been defined?

What data does the application store and how?

What data is or may need to be encrypted and what key management requirements have been defined?

What capabilities exist to detect the leakage of sensitive data?

What encryption requirements have been defined for data in transit over WAN and LAN links?

Authored by Lenny Zeltser, who leads the security consulting practice at Savvis and teaches at SANS Institute. You can find him on Twitter. Special thanks to Slava Frid for feedback. Page 1 of 2.

### Access

What user privilege levels does the application support?

What user identification and authentication requirements have been defined?

What user authorization requirements have been defined?

What session management requirements have been defined?

What access requirements have been defined for URI and Service calls?

What user access restrictions have been defined?

How are user identities maintained throughout transaction calls?

### Application Monitoring

What application auditing requirements have been defined?

What application performance monitoring requirements have been defined?

What application security monitoring requirements have been defined?

What application error handling and logging requirements have been defined?

How are audit and debug logs accessed, stored, and secured?

### Application Design

What application design review practices have been defined and executed?

How is intermediate or in-process data stored in the application components' memory and in cache?

How many logical tiers group the application's components?

What staging, testing, and Quality Assurance requirements have been defined?

## #4: SECURITY PROGRAM REQUIREMENTS

### Operations

What is the process for identifying and addressing vulnerabilities in the application?

What is the process for identifying and addressing vulnerabilities in network and system components?

What access to system and network administrators have to the application's sensitive data?

What security incident requirements have been defined?

How do administrators access production infrastructure to manage it?

What physical controls restrict access to the application's components and data?

What is the process for granting access to the environment hosting the application?

### Change Management

How are changes to the code controlled?

How are changes to the infrastructure controlled?

How is code deployed to production?

What mechanisms exist to detect violations of change management practices?

### Software Development

What data is available to developers for testing?

How do developers assist with troubleshooting and debugging the application?

What requirements have been defined for controlling access to the applications source code?

What secure coding processes have been established?

### Corporate

What corporate security program requirements have been defined?

What security training do developers and administrators undergo?

Which personnel oversees security processes and requirements related to the application?

What employee initiation and termination procedures have been defined?

What application requirements impose the need to enforce the principle of separation of duties?

What controls exist to protect a compromised in the corporate environment from affecting production?

What security governance requirements have been defined?

### Additional Resources

OWASP Guide to Building Secure Web Applications
http://www.owasp.org/index.php/OWASP_Guide...

ISO 27002 Standard: Code of Practice
http://www.iso.org/iso/catalogue...

BITS Standards for Vendor Assessments
http://www.sharedassessments.org/download...

Guidance for Critical Areas ... in Cloud Computing
http://www.cloudsecurityalliance.org/guidance...

Payment Card Industry (PCI) Data Security Standard
https://www.pcisecuritystandards.org/security...

How to Write an Information Security Policy
http://www.csoonline.com/article/print/495017

IT Infrastructure Threat Modeling Guide
http://www.microsoft.com/downloads...

Authored by Lenny Zeltser, who leads the security consulting practice at Savvis and teaches at SANS Institute. You can find him on Twitter. Special thanks to Slava Frid for feedback. Page 2 of 2.