

# Integrating Security into SDLC MnIPS Educational Seminar

Wendall A. Reimer  
May 3, 2006

The Midwave logo features the word "midwave" in a white, lowercase, sans-serif font. The letter "i" is stylized with a blue dot and a blue horizontal line. The logo is centered within a blue circular graphic that has a ripple effect, set against a dark blue background.

## Outline

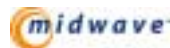
- Why do we care?
  - Integrating security into SDLC
  - What are the benefits?
  - Microsoft Principle
- Project conception/initialization
- Requirements gathering
- Design
- Build/Test
- Implementation/Ongoing Support

The Midwave logo, consisting of the word "midwave" in white lowercase letters with a blue dot and line on the "i", is positioned in the bottom left corner of the slide.

2

## Why do we care?

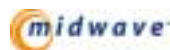
- Business requirements have changed
- Aggressive enforcement
- Business drivers (growth, speed of application dev., etc.)
- Customers require more attention on security
  - Contracts
  - Non-Disclosure Agreements
  - Service Level Agreements
  - Notification
- Industry regulations (GLBA, SOX, HIPAA, etc.)
- Audit requirements and audit efficiency
- Decision making process and documentation



3

## Integrating Security into SDLC

- Repeatable processes
  - Integrate security considerations into project templates
  - Integrate a consistent approach to risk analysis into the early stages of the SDLC process
  - Consistently applying security analysis and design will influence business units to be prepared for those discussions.
- Analyst/Developer Education
  - Common tools and mindset
  - Knowledge base of security standards and policies
  - Identify consistent methods and templates
  - Identify gaps in current practices
- Metrics and Accountability
  - A consistent review process to ensure compliance
  - Measure development life cycle components across projects
  - Reduce rework and/or risk exposure



4

## What are the Benefits

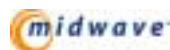
- Effectiveness
  - Security objectives are easier to achieve when security issues are considered as part of a routine development process.
  - Security safeguards can be integrated into the system during its design
  - Optimization of infrastructure security capabilities can be leveraged, consistently, by multiple applications.
- Expense
  - To retrofit security after implementation is generally more expensive than to integrate in from the start
- Less Obtrusive
  - When security safeguards are integral to a system, they are usually easier to use and less visible to the user



5

## Microsoft Principle

- SD<sup>3</sup> + C
- Secure by design
  - Architected, designed and implemented so as to protect itself and the information it processes
  - Resist attack
- Secure by default
  - Assume security flaws will be present
  - Default security settings should be to promote security and prevent disclosure or damage
  - Ex. Run with least necessary privilege
- Secure in deployment
  - Tools and guidance should accompany software or implementation/use procedures to help end users and administrators use it securely
- Communication
  - As security issues, concerns or gaps are identified, users, administrators and developers should communicate openly and responsibly to help make sure corrective action is taken



6

## Project Conception/Initiation

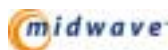
- Generally involves a request process from a business sponsor
- First opportunity to ask high-level risk questions
  - Does the system/application introduce new technology or make major changes to current technology?
  - What kind of information will be transmitted, processed and stored:
    - Client confidential
    - Non-public personal information (Including financial and health information)
    - Business critical
  - Will this be a hosted service (outsourced)?
  - What Information Security policies could come into play in the development and deployment of this application?
  - What are the potential requirements for this application from a regulatory standpoint?
  - Who are the primary users of the application?



7

## Project Conception/Initiation

- Identify level of risk (ex. high, medium, low)
- Level of risk will determine effort, time and potentially costs associated with project
- Role of a governance board
  - Overall project governance
  - Ensure security issues, concerns or requirements are identified and reviewed for clarity prior to authorization to proceed
  - Provide a consistent message to all project initiators on importance of reviewing security requirements early
  - Identify opportunities to leverage existing security framework and architecture
  - Identify opportunities to leverage the security efforts of previous projects
- Make questions and risk assessment part of standard templates for project charter, project plan, RFP's, etc.



8

## Requirements Gathering

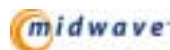
- Security requirements and considerations be included at the same time other requirements for the system are being identified
- Business analysts play a key role in ensuring this is consistently applied to all projects
- Business analysts are responsible for ensuring the appropriate questions are asked and answered to complete the initial security assessment
- The Security Department should be consulted to review analysis findings, project requirements and security considerations
- During this phase, initial efforts are made to identify key elements of the technical architecture that can/should be leveraged with regard to security
  - Identification/authentication (ex. how users are identified)
  - Authorization (ex. process of approval, user provisioning, etc.)
  - Password management (ex. standards, storage, encryption)
  - Audit requirements (ex. syslogs, application logs, etc.)
  - Data encryption requirements (ex. at-rest, in-transit, backup, etc.)



9

## Design

- The design phase identifies the overall structure of the system, including security
- The key elements of the design phase from a security perspective are:
  - Define security architecture and design principles
  - Identify specific security design for affected elements of the system
    - Identification/Authentication (ex. Active Directory, database)
    - Authentication (how users are authenticated)
    - Application access and authentication approval process
    - Data flow and storage security design
      - Only necessary amount of Client confidential, non-public personal information, and business critical data is transmitted and stored
      - Encryption design where required
      - Security of data backup
      - Data disposal procedures



10

## Design (cont.)

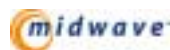
- Design specifications should make use of common security control capabilities in the security architecture
- Trust user input at your own peril
- Identify specific security design for affected elements of the system (cont.)
  - Document potential exposures to sensitive data or application processes
  - Identify and document mitigation strategies or solutions for potential exposures
- Review security design with Security Department
- Review security design with business unit sponsoring project (great educational opportunity)



11

## Build/Testing

- Use common code repositories for all code
- Use static-analysis code scanning tools to detect known coding flaws that result in vulnerabilities (buffer overflows, integer overruns, uninitialized variables, etc.)
- Conduct code reviews
- Use test cases to test potential security vulnerabilities based on requirements and design criteria (i.e. try to break the security controls)
- Thoroughly test failure and error processing code
- Final security review with Security Department
  - Review of test results
  - Review of security requirements and architecture
  - Ensure nothing changed since project inception
  - Validate system and system controls are able to be audited



12

## Implementation/Ongoing Support

- User training and documentation are a great opportunity to educate the user community on the security aspects of the system.
- User training should include specific security controls and user responsibilities associated with using the system
- User screens, web pages, reports, etc. should contain instructions or reminders to users about security controls and their responsibilities
- System enhancement or bug-fix processes need to refer to the security design and architecture when changes are made to the system
- Security should be reviewed as part of the production change control process (both applications and infrastructure)
  - Risk may have changed
  - New regulations could impact original risk
  - New elements of security architecture could be leveraged

