Approaches to Secure Software

Ravid Lazinsky
Technical Manager
Applicure Technologies, Ltd.
www.applicure.com

Applicure Technologies, Ltd.

AppliCure Technologies

Applicure Technologies Ltd creates software-based products for web application security and application compliance. We believe security and IT controls have to be cost effective and efficient so our customers are free to focus on their business goals.

dotDefender

Software based, Web Application Firewall

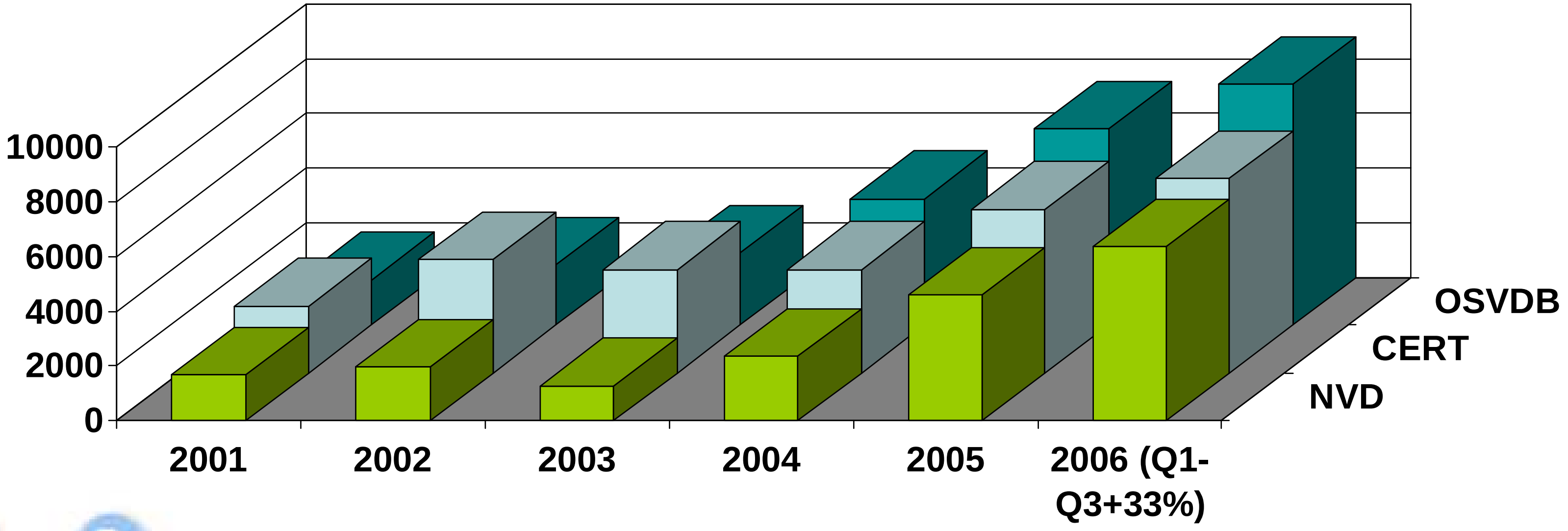
TotalShield™ *Database Compliance*

Enterprise-wide audit trail for database compliance

Definition of secure software

A secure product is one that protects the confidentiality, integrity, and availability of the customers' information, and the integrity and availability of processing resources under control of the system's owner or administrator.

-- Source: Writing Secure Code (Microsoft.com)



Causes of security vulnerabilities

- Human factor
- Insufficient training and awareness
- Limited resources
- Tight schedules
- Software complexity
- Poor secure software engineering practices
- Poor design decisions

Approaches to secure software

- Secure coding and testing
- Secure SDLC/ SD^3
- Web application firewall (realtime control)

Secure Coding and Testing

- Code
  - Secure development
  - Coding guidelines
  - Certified components
  - Targeted security
  - Meet specific requirements

- Test
  - Secure code review
  - Static code analyzer
  - Automated Application Assessment

Secure Coding and Testing

- Tools
  - Static Code Analyzer
  - Certified Components
  - Security Development Guidelines
  - Automated security tool
  - Manual Penetration Test

- Deliverables
  - Working application
  - Problems, defects, enhancements logged
  - Detailed test results

Secure Coding -- Challenges

- Identify all security risks
- Create general solution to recurrent security problems
- Flexibility in adapting to application changes
- Protecting against new modes of attack
- Re-usable security in different development technologies
- Programmer training and continuous training
- Security training and awareness for QA staff

Secure SDLC/ SD^3

SD^3

- Secure by Design
- Secure by Default
- Secure by Deployment

- Define security architecture
- Identify security critical components
- Identify design techniques (e.g., layering, managed code, least privilege, attack surface minimization)
- Identify attack surface
- Create threat models (e.g., identify assets, interfaces, threats, risk) and mitigate
- Define automated and manual testing

Secure SDLC/ SD3

SD^3
- Secure by Design
- Secure by Default
- Secure by Deployment

Security Push
- Threat models reviewed
- Code reviewed
- Attack testing
- New threats evaluated

Final Security Review
- Unfixed bugs reviewed
- New bugs reviewed
- Penetration testing completed
- Documentation

Secure SDLC -- Challenges

- Identify all security risks ✓
- Create general solution to recurrent security problems ✓
- Flexibility in adapting to application changes
- Protecting against new modes of attack
- Re-usable security in different development technologies
- Programmer training and continuous training
- Security training and awareness for QA staff

Web Application Firewall

- Additional layer for realtime protection
- Immediately mitigate new modes of attack
- Deep packet inspection of all HTTP methods, HTTP headers, HTTP post data
- Anti-evasion: normalisation/ canonicalisation/ transformation
- Reporting capability:
  - Identify internal malicious users
  - Information on actual attack attempts

WAF Techniques

- Negative security model
  - Filters malicious input
  - Rapid implementation
  - Low false positive rate
- Positive security model
  - Allow only approved input
  - Learning curve
  - High false positive rate

WAF Solutions

- Server plug-in/ embedded
  - Easy to implement
  - No SSL termination
  - Uses web server resources
- Network appliance/ Reverse proxy:
  - External to application
  - Block attacks before they get to server
  - Performance issues
  - SSL termination
  - Must have copies of SSL keys

Software WAF Deployment

- Web server plug-in:
  - Standard implementation
  - Internal enterprise web solutions
  - Distributed enterprise web architecture
  - OEM

WAF -- Challenges

- Identify all security risks ✓
- Create general solution to recurrent security problems ✓
- Flexibility in adapting to application changes ✓
- Protecting against new modes of attack ✓
- Re-usable security in different development technologies ✓
- Programmer training and continuous training
- Security training and awareness for QA staff

Best Practices

- Secure SDLC * :
  - Strives to be a repeatable process
  - Requires team member education
  - Tracks metrics and maintains accountability
- WAF
  - Additional security layer
  - 0-day attack protection
  - Continuous protection against emerging threats
  - Can compensate for human error

** "Writing Secure Code" 2nd Ed., Howard & LeBlanc*
"The Trustworthy Computing Security Development Lifecycle" by Lipner & Howard

Thank You !

Ravid Lazinsky: ravid@applicure.com