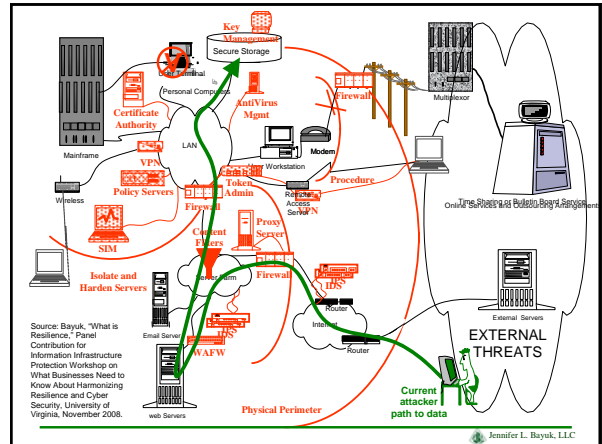


Securing Web Applications

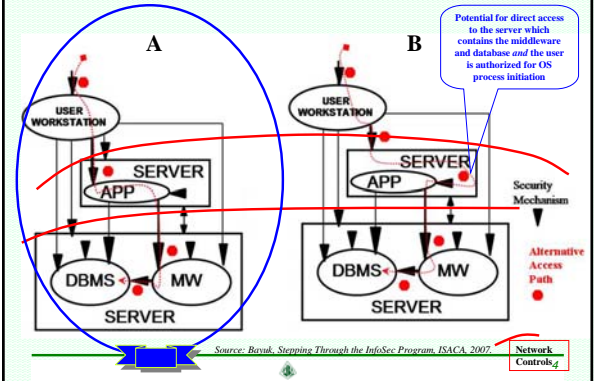
Jennifer L. Bayuk
 jennifer@bayuk.com
 www.bayuk.com



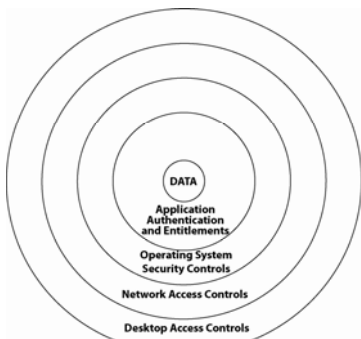
Web Application Security Roadmap

- Architecture
- Engineering
- Software Development
- Operation

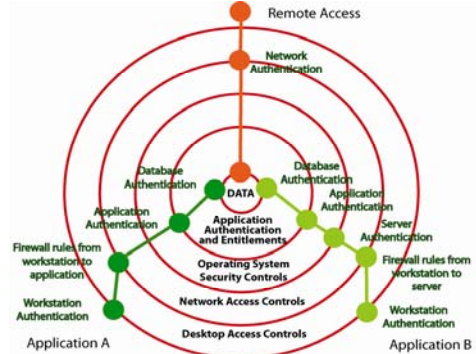
Architecture Alternatives

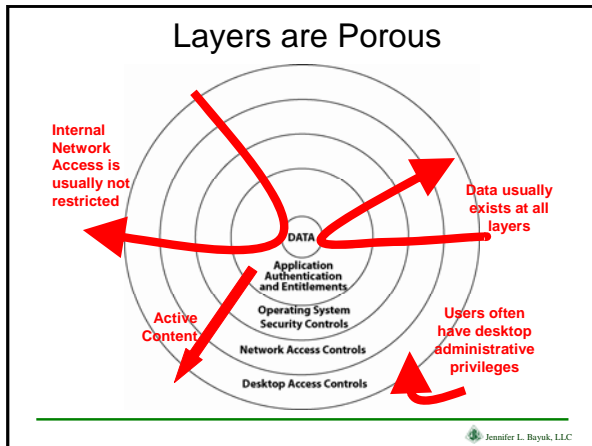


Defense in Depth



Defense in Depth





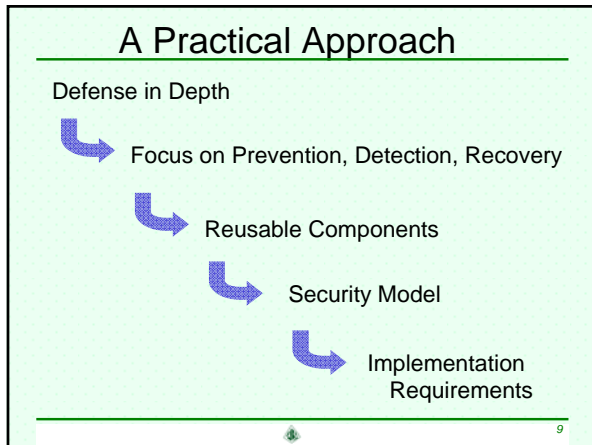
ISF Recommendation

There should be an enterprise-wide process for implementing coherent and consistent security services (eg identity services, authentication services and cryptographic services) and establishing common user and application programming interfaces (APIs).

Excellence in Simplicity

Source: *The Standard of Good Practice for Information Security, Security Management, 4.6.1, Information Security Forum, 2007. www.securityforum.org*

Jennifer L. Bayuk, LLC

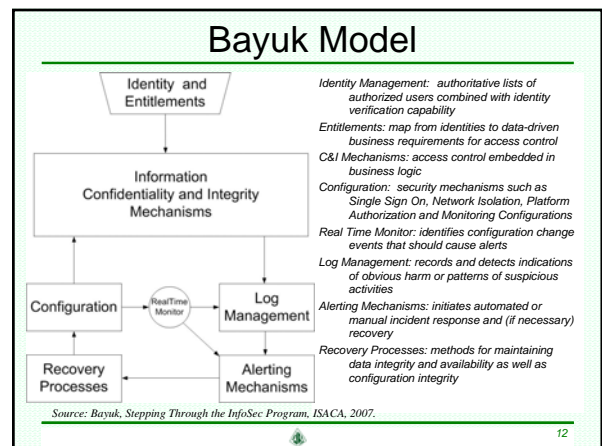
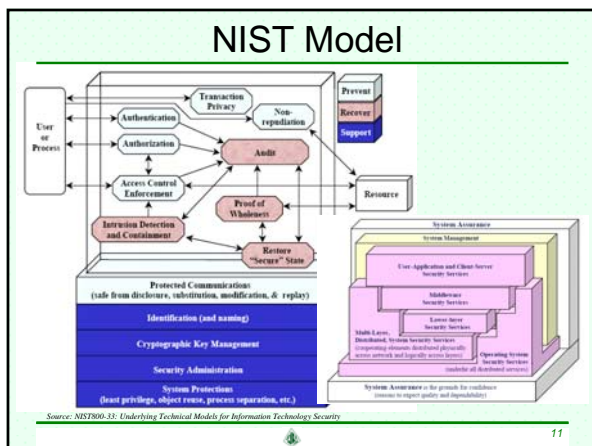


Triad Mining

App A: Control:	Data	Operating System	Application	Network	Workstation
Prevention	DBMS login	Password repository on local server	Password repository on local server	Handheld authentication Session-based filters	Centralized Identity and Access Mgmt
Detection	Logs on servers	File integrity checking	Operations log monitoring	Link and utilization monitoring	Intrusion detection and prevention
Recovery	Backup tapes	Cold standby	Cold standby	Redundant alternative routing	Automated imaging

App B: Control:	Data	Operating System	Application	Network	Workstation	
Prevention	DBMS login	Network isolation	Centralized Identity and Access Mgmt	Centralized Identity and Access Mgmt	Handheld authentication Session-based filters	Centralized Identity and Access Mgmt
Detection	Logs in centralized repository	File integrity checking	Operations log monitoring	Link and utilization monitoring	Intrusion detection and prevention	
Recovery	Storage mirroring	Cluster technology	Hot standby	Redundant alternative routing	Automated imaging	

Potential for Control Re-Use



Engineering

Use security model as auditable requirement.

Configuration, configuration, configuration....

Jennifer L. Bayuk, LLC 13

The Design/Architecture Review

Objective

Scope

Constraint

Approach

Result

To establish that a system corresponds to security model, and identify configuration parameters in the systems environment required comply.

Network and operating system placement diagrams, as well as detailed technical design documents on system security mechanisms.

Unknowns or lack of expertise in security mechanisms in externally-built components.

Map architecture onto model. Compare settable parameters of all systems components to known secure configurations.

List of issues to address, iterative process.

Jennifer L. Bayuk, LLC 14

Software

- 70% of all vulnerabilities are in application software¹
- Recently announced 25 known software flaws² have been compared to National Quality Forum's "Never Events"³
- OWASP Top Ten, Top 25 predecessor which was endorsed by the OCC⁴

¹ Gartner, 2008.
² MITRE, 2009.
³ Charette, R., *The Risk Factor*, IEEE Spectrum Online, January 14, 2009.
⁴ Office of the Comptroller of the Currency, 2008.

Jennifer L. Bayuk, LLC 15

Top 25 Security Mistakes

Insecure Interaction Between Components

- Improper Input Validation
- Improper Encoding or Escaping of Output
- Failure to Preserve SQL Query Structure
- Failure to Preserve Web Page Structure
- Failure to Preserve OS Command Structure
- Cleartext Transmission of Sensitive Information
- Cross-Site Request Forgery
- Race Condition
- Error Message Information Leak

Risky Resource Management

- Failure to Constrain Operations within the Bounds of a Memory Buffer

- External Control of Critical State Data
- External Control of File Name or Path
- Untrusted Search Path
- Failure to Control Generation of Code
- Download of Code Without Integrity Check
- Improper Resource Shutdown or Release
- Improper Initialization
- Incorrect Calculation

Porous Defenses

- Improper Access Control
- Use of a Broken or Risky Cryptographic Algorithm
- Hard-Coded Password
- Insecure Permission Assignment for Critical Resource
- Use of Insufficiently Random Values
- Execution with Unnecessary Privileges
- Client-Side Enforcement of Server-Side Security

Jennifer L. Bayuk, LLC 16

Roadmap to Secure Code

- Input Validation and Representation
 - parse, parse, parse
- API Abuse Prevention
 - use pre and post-conditions
- Security Features
 - close the front door and apply same security to windows
- Time and State
 - maintain authentication across threads, processes, time
- Error Handling
 - fail in safe mode
- Code Quality
 - security is a subset of reliability
- Encapsulation
 - trust no one

See McGraw, Gary, *Software Security: Building Security In*, also Ott and Fath, "Risk Associated With Web Application Vulnerabilities," ISACA Journal V1 2009.

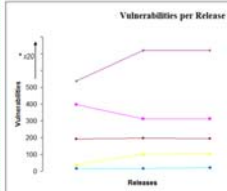
Jennifer L. Bayuk, LLC 17

Secure Software

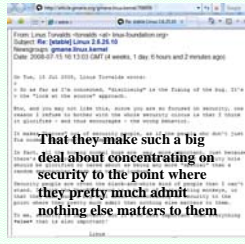
Adapted by permission from the book *Software Security: Building Security In* by Gary McGraw (Addison-Wesley, 2006) www.swsec.com
 See also: *The Security Development Lifecycle* by Howard and Lipner

Jennifer L. Bayuk, LLC 18

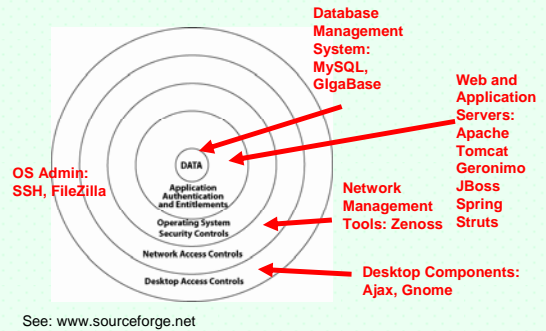
Using Open Source



* Hibernate's vulnerability numbers were divided by 20 to avoid presentation issues due to scale.
Source: Fortify Open Source Survey, 2008, www.fortify.com.



Open Source Examples



See: www.sourceforge.net

Using COTS

- Commercial Off-the-Shelf software should receive the same scrutiny with respect to the security model as any internally built product.
- Lack of access to source code may be mitigated via vendor commitment to secure software practices and increased level of abuse case testing.

CISO's Guide to Software Security

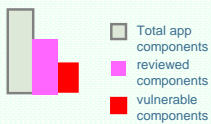
- SDLC Governance
- Outsourcing
- Open Source
- COTS
- SaaS
- Web 2.0

Source: Fortify CISO's Guide Series, 2009, <http://www.fortify.com/cisoguides>.

Software Security Review Metrics

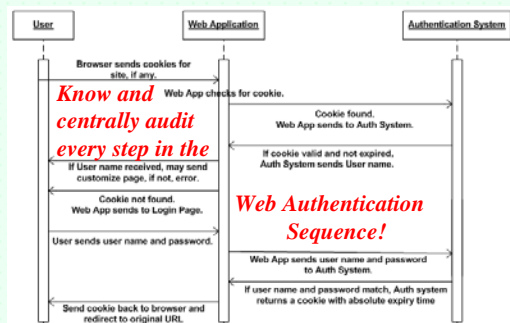
Need to include ALL software components

- App 1 = (component 1, component 2, component 3.....)
- App 2 = (Inhouse servlet, Apache Webserver, Oracle DBMS)
- App 3 = (Inhouse servlet, Solaris Webserver, MySQL DBMS)
- App 4 = (Spring servlet, Fuego Workflow Server, Ajax Mashup)



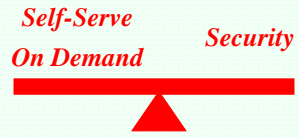
Review strategy may vary where source is not available, but still should be consistently performed.

Operation



Web User Administration

- Enrollment
- Login
 - Single Sign-on
- Password Reset
- Entitlements
 - Roles, Groups
- Audit



Questions? Discussion...

Jennifer L. Bayuk
jennifer@bayuk.com
www.bayuk.com