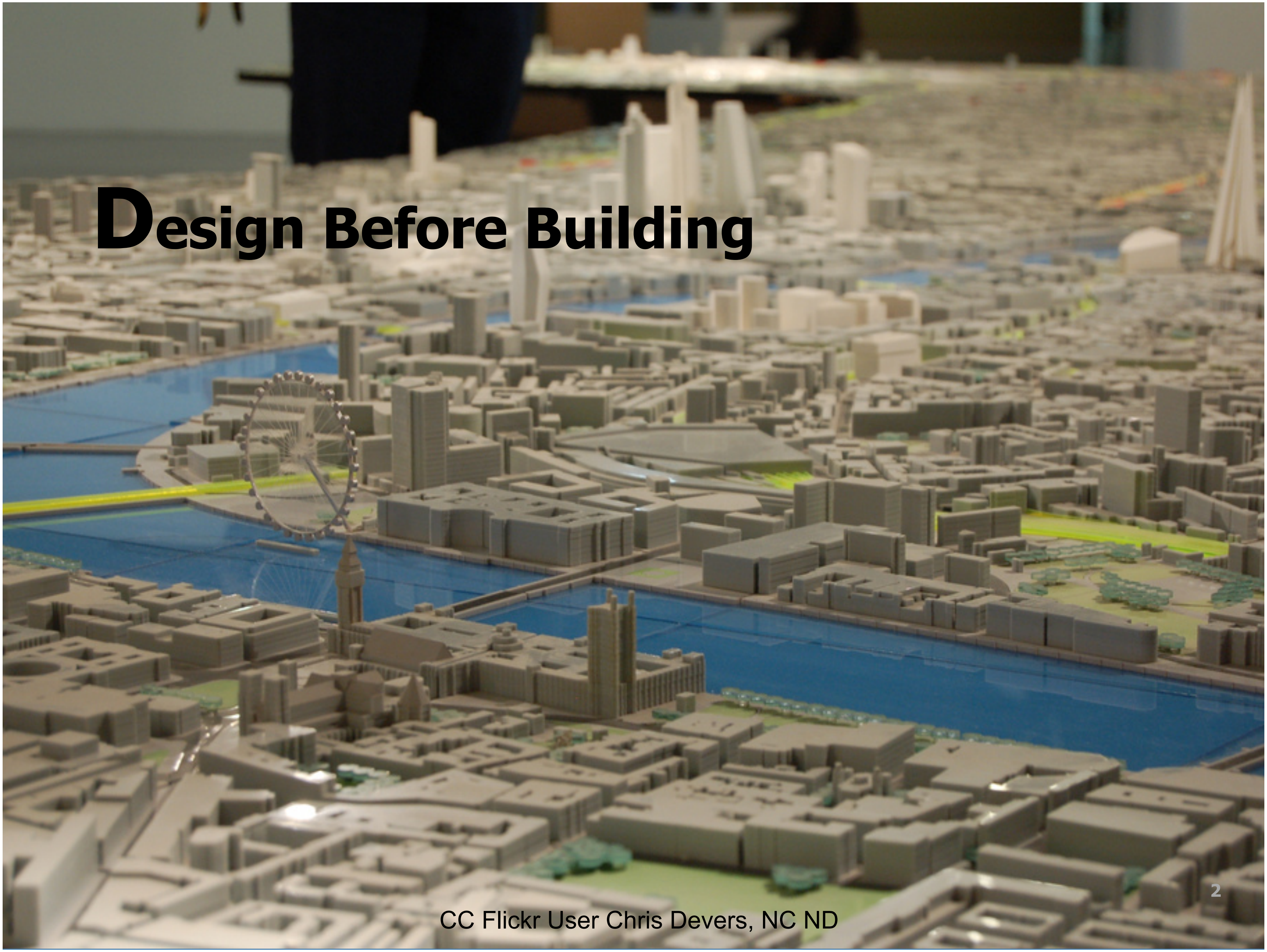
Securing the Core J2EE Patterns

Rohit Sethi & Krishna Raja
Project leader, Secure Pattern Analysis Project
Security Compass
rohit@securitycompass.com
krish@securitycompass.com

AppSec DC
Sep 21, 2009

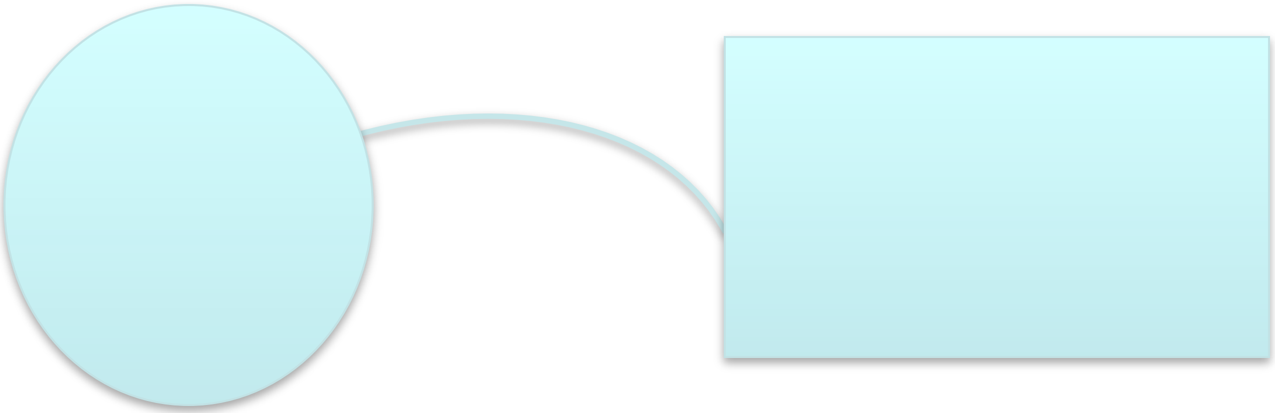
The OWASP Foundation
http://www.owasp.org

Design Before Building

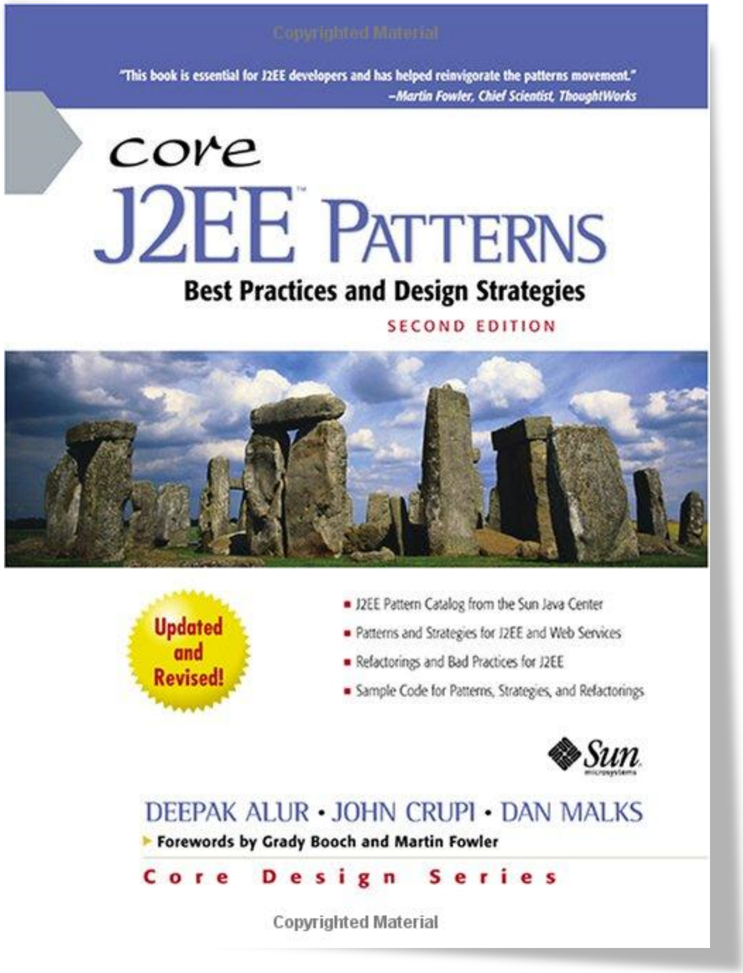


CC Flickr User Chris Devers, NC ND

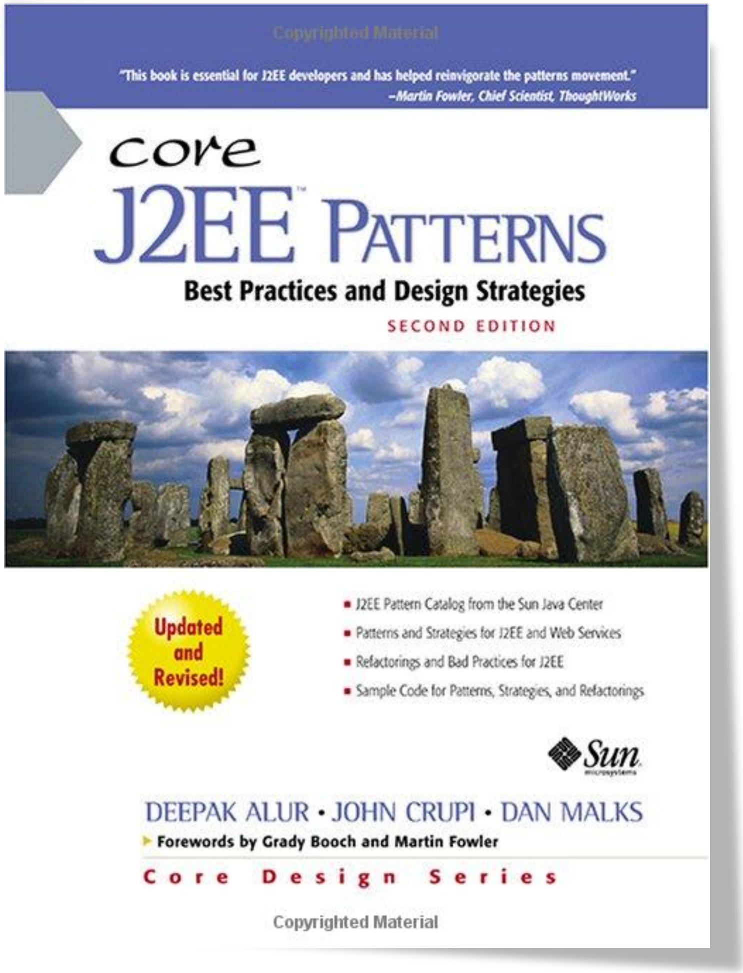
We create Threat Models on Completed Designs



What About *During* Design?


Copyrighted Material
"This book is essential for J2EE developers and has helped reinvigorate the patterns movement."
–Martin Fowler, Chief Scientist, ThoughtWorks
core
J2EE™ PATTERNS
Best Practices and Design Strategies
SECOND EDITION
Updated and Revised!
J2EE Pattern Catalog from the Sun Java Center
Patterns and Strategies for J2EE and Web Services
Refactorings and Bad Practices for J2EE
Sample Code for Patterns, Strategies, and Refactorings
Sun microsystems
DEEPAK ALUR • JOHN CRUPI • DAN MALKS
Forewords by Grady Booch and Martin Fowler
Core Design Series
Copyrighted Material

Design Patterns are Used During Design



Copyrighted Material

"This book is essential for J2EE developers and has helped reinvigorate the patterns movement."
–Martin Fowler, Chief Scientist, ThoughtWorks

core
J2EE™ PATTERNS
Best Practices and Design Strategies
SECOND EDITION

Updated and Revised!

- J2EE Pattern Catalog from the Sun Java Center
- Patterns and Strategies for J2EE and Web Services
- Refactorings and Bad Practices for J2EE
- Sample Code for Patterns, Strategies, and Refactorings

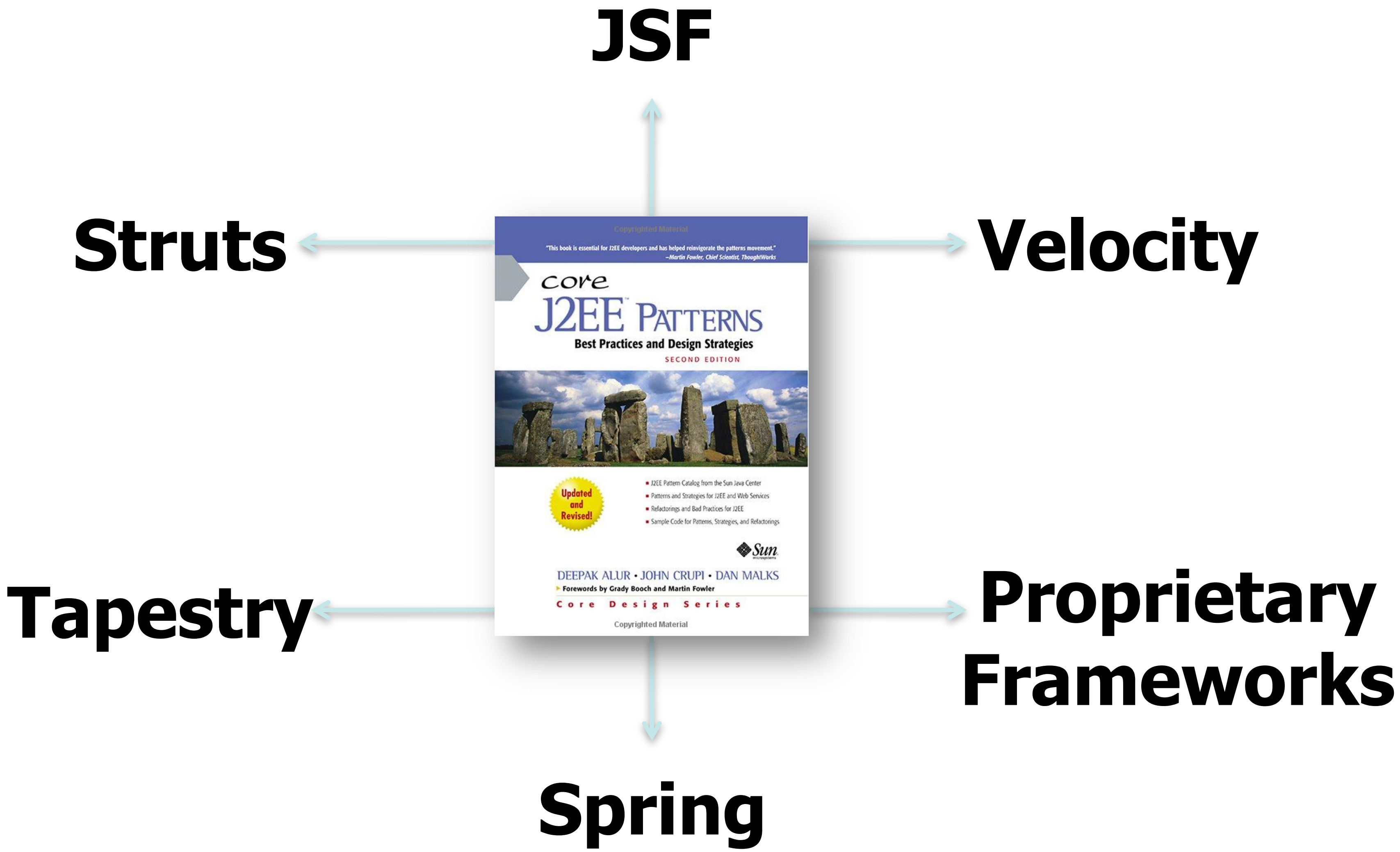
Sun microsystems

DEEPAK ALUR • JOHN CRUPI • DAN MALKS
Forewords by Grady Booch and Martin Fowler

Core Design Series

Copyrighted Material

Core J2EE Patterns are Used Extensively



JSF

Struts

Velocity

Copyrighted Material

"This book is essential for J2EE developers and has helped reinvigorate the patterns movement."
–Martin Fowler, Chief Scientist, ThoughtWorks

core J2EE™ PATTERNS

Best Practices and Design Strategies

SECOND EDITION

Updated and Revised!

- J2EE Pattern Catalog from the Sun Java Center
- Patterns and Strategies for J2EE and Web Services
- Refactorings and Bad Practices for J2EE
- Sample Code for Patterns, Strategies, and Refactorings

Sun microsystems

DEEPAK ALUR • JOHN CRUPI • DAN MALKS

Forewords by Grady Booch and Martin Fowler

Core Design Series

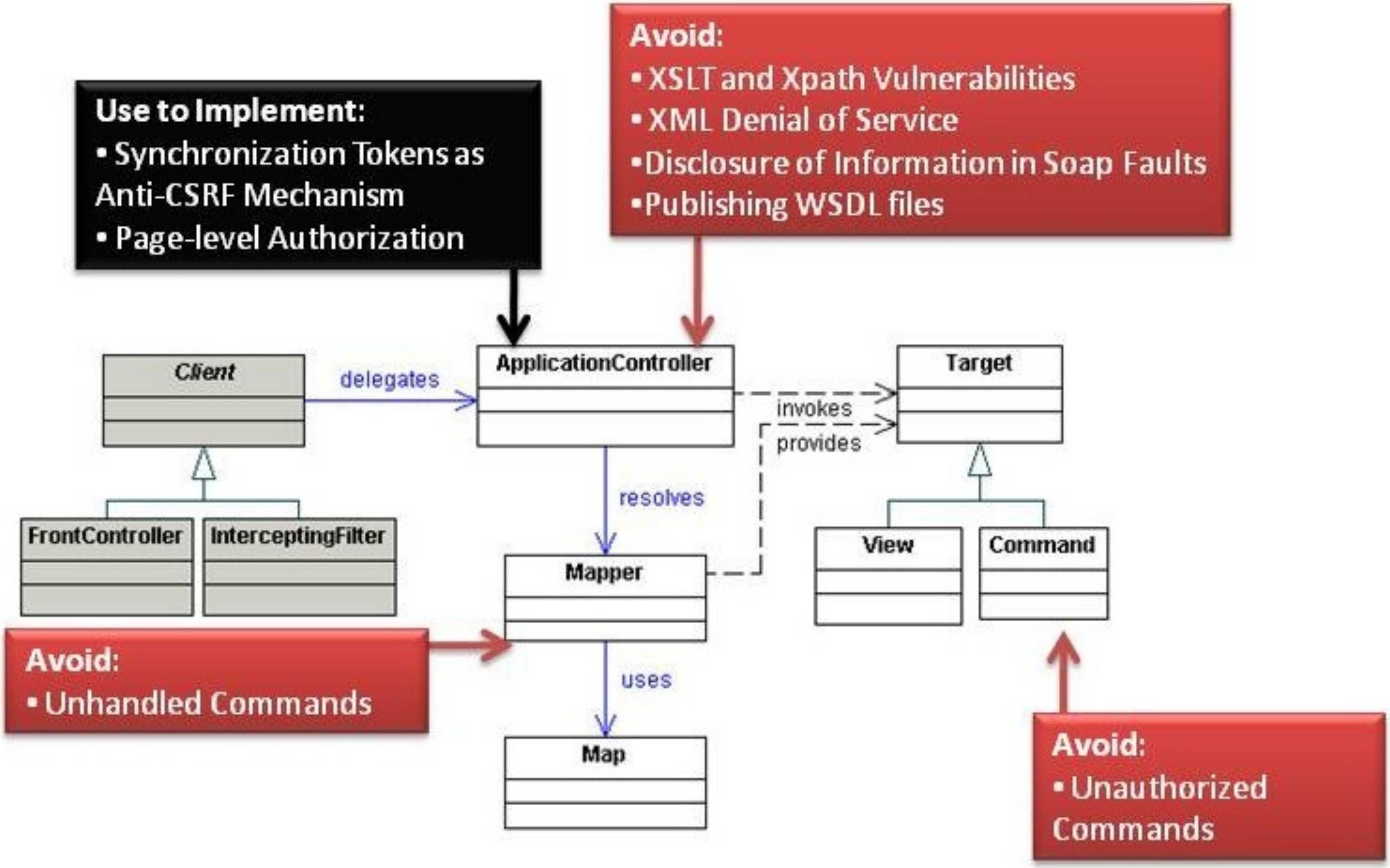
Copyrighted Material

Tapestry

Proprietary Frameworks

Spring

Project: Analyze Patterns



Use to Implement:

- Synchronization Tokens as Anti-CSRF Mechanism
- Page-level Authorization

Avoid:

- XSLT and Xpath Vulnerabilities
- XML Denial of Service
- Disclosure of Information in Soap Faults
- Publishing WSDL files

Avoid:

- Unhandled Commands

Avoid:

- Unauthorized Commands

Project Goals

- Analyze patterns for security pitfalls to avoid
- Determine how patterns can implement security controls
- Provide advice portable to most frameworks

Not Overlapping

"From the ground up, the Java platform was designed for security. Read this book to learn how to apply patterns and proven technologies to secure your J2EE applications and beyond."

—James Gosling, father of the Java™ Programming Language

core

SECURITY PATTERNS

Best Practices and Strategies for J2EE™, Web Services, and Identity Management

- A patterns catalog that includes twenty-three new patterns for building end-to-end security
- Security design methodology, patterns, best practices, reality checks, and defensive strategies
- Applied techniques for Web Services security, Identity Management, Service Provisioning, and Personal Identification
- Comprehensive security guide to using J2SE™, J2EE™, J2ME™, and Java Card™

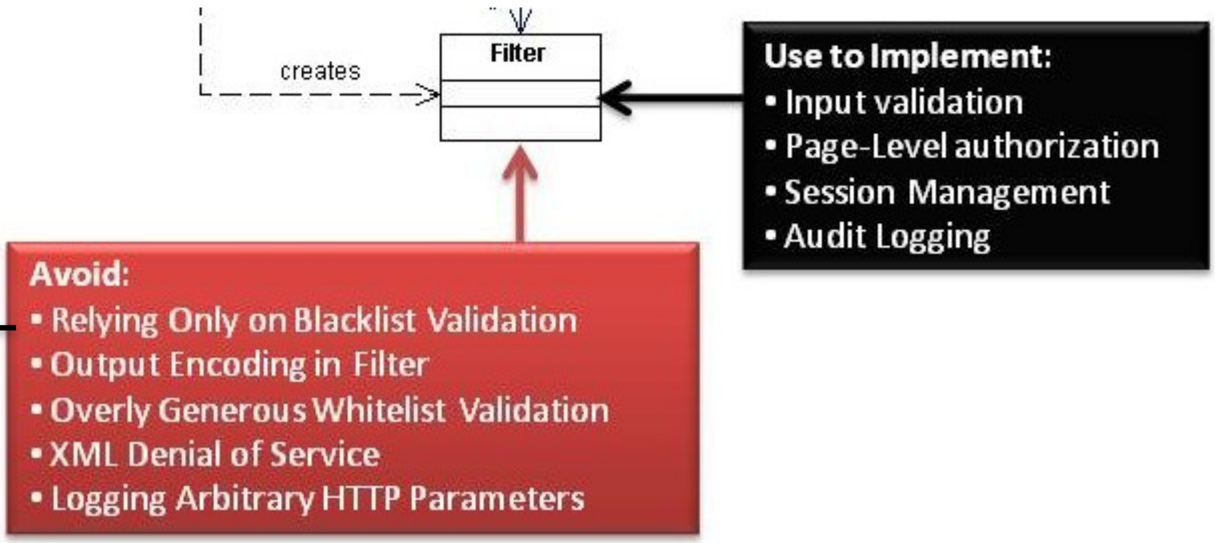
Sun microsystems

CHRISTOPHER STEEL · RAMESH NAGAPPAN · RAY LAI

Forewords by Judy Lin, Executive Vice President, VeriSign, and Joseph Uniejewski, Chief Technology Officer, RSA Security

Uses

- Designing new web application frameworks
- Designing new apps that use the patterns
- Source code review of existing apps
- Runtime assessment of existing apps
- Integrate with threat modeling of new or existing apps

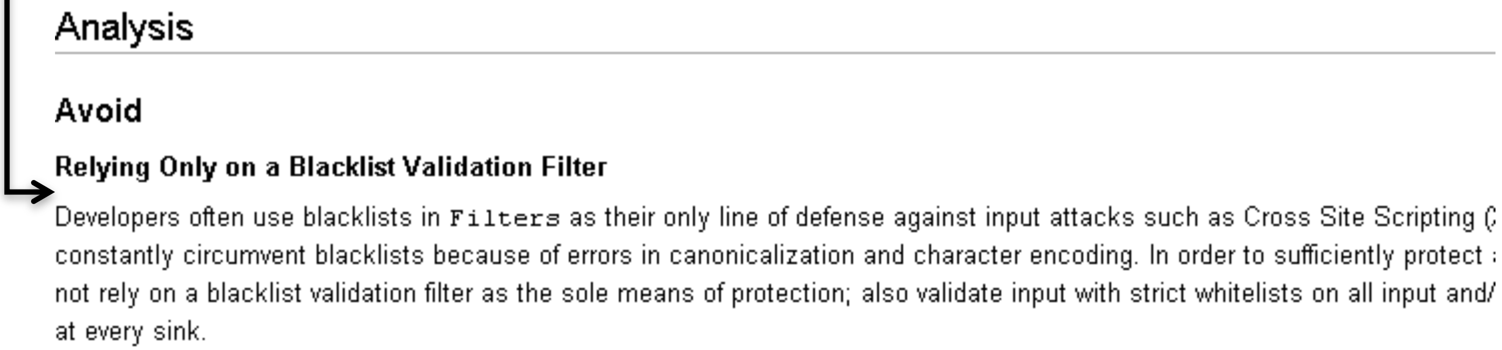


Use to Implement:

- Input validation
- Page-Level authorization
- Session Management
- Audit Logging

Avoid:

- Relying Only on Blacklist Validation
- Output Encoding in Filter
- Overly Generous Whitelist Validation
- XML Denial of Service
- Logging Arbitrary HTTP Parameters

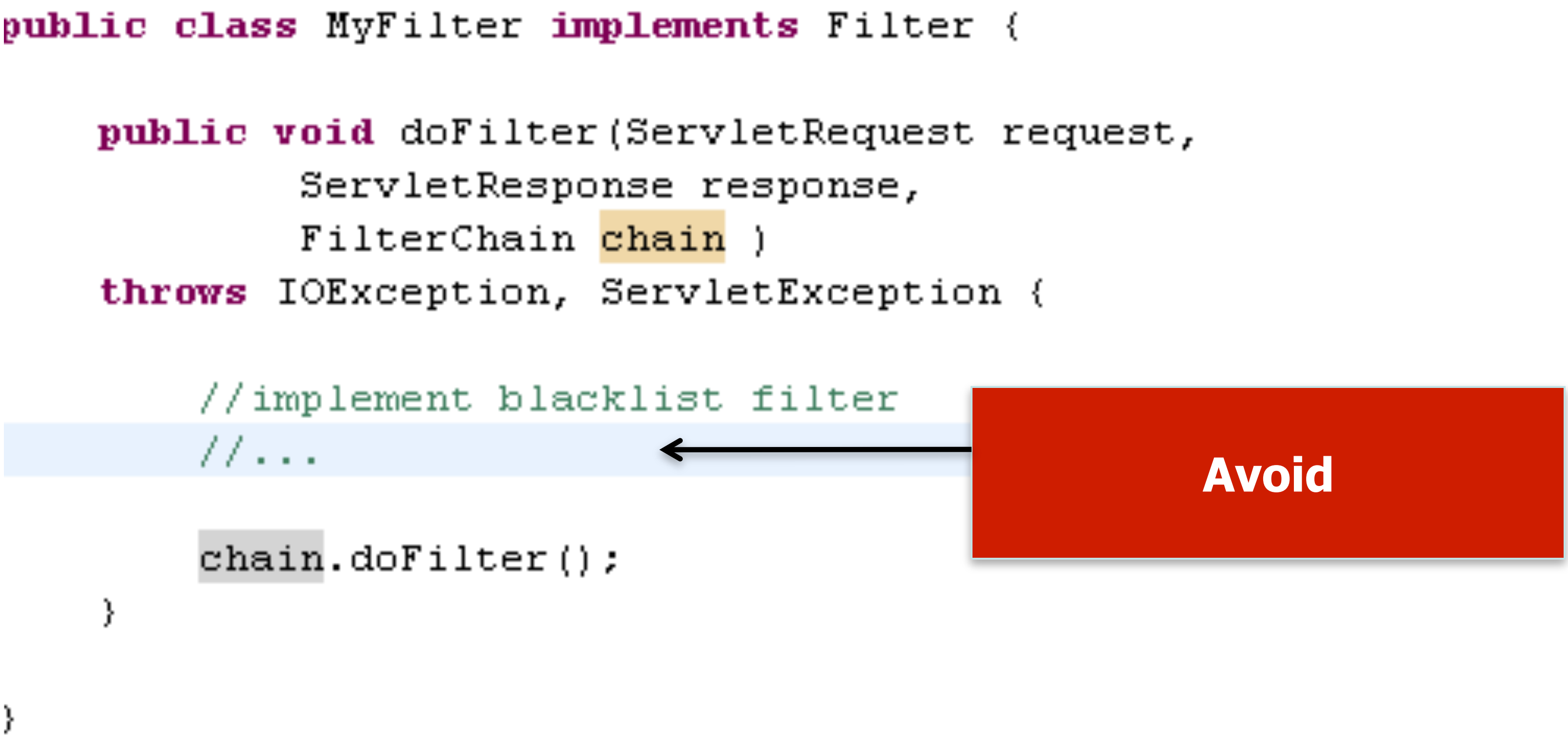


Analysis

Avoid

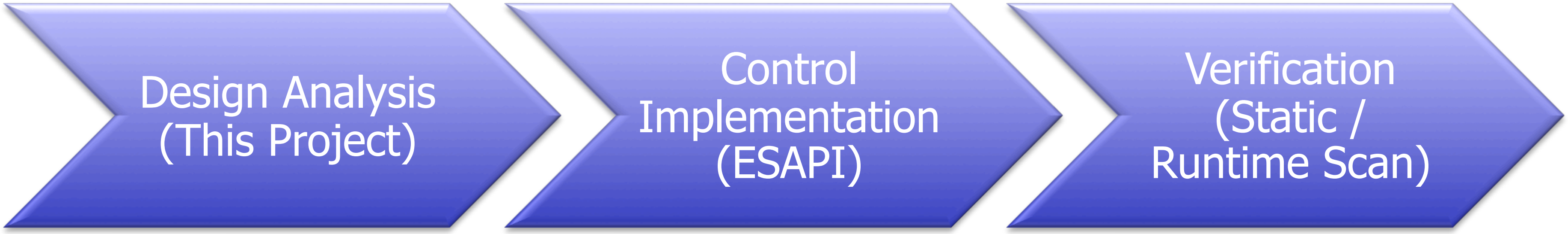
Relying Only on a Blacklist Validation Filter

Developers often use blacklists in `Filters` as their only line of defense against input attacks such as Cross Site Scripting (constantly circumvent blacklists because of errors in canonicalization and character encoding. In order to sufficiently protect not rely on a blacklist validation filter as the sole means of protection; also validate input with strict whitelists on all input and/ at every sink.



```
public class MyFilter implements Filter {

    public void doFilter(ServletRequest request,
            ServletResponse response,
            FilterChain chain )
    throws IOException, ServletException {

        //implement blacklist filter
        //...

        chain.doFilter();
    }

}
```

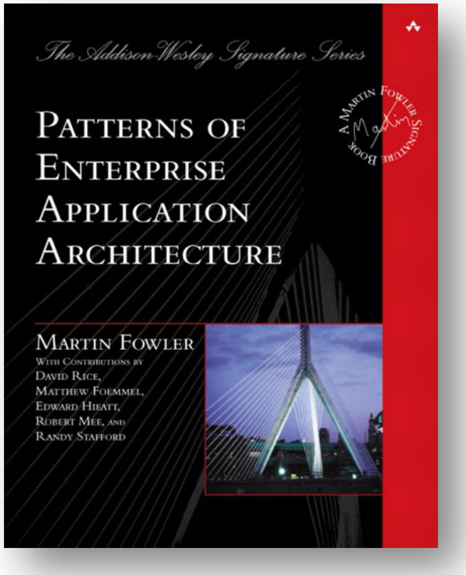
Avoid

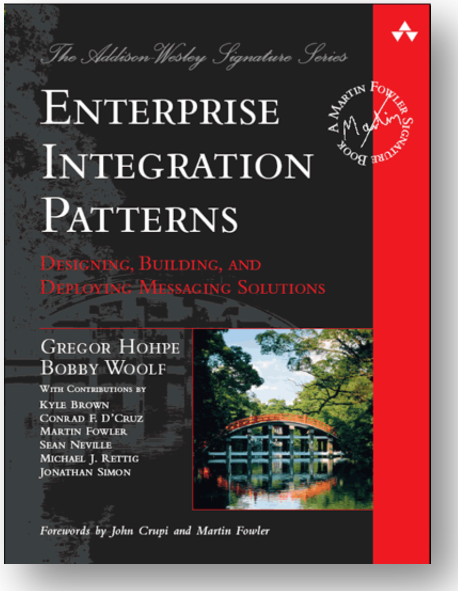

Design Analysis (This Project)
Control Implementation (ESAPI)
Verification (Static / Runtime Scan)

You Can Help ...

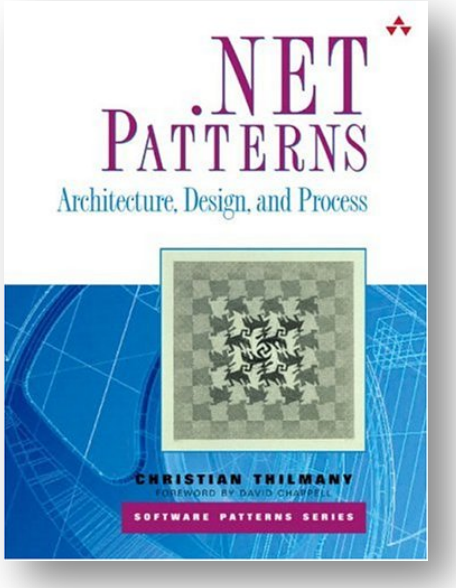
...Tell Developers

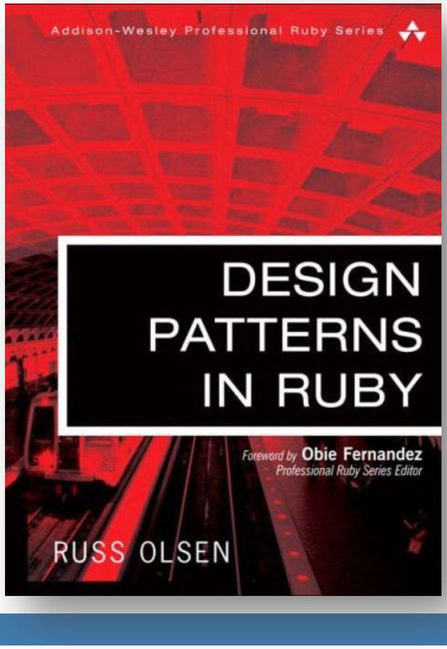
CC Flickr User wili hybrid

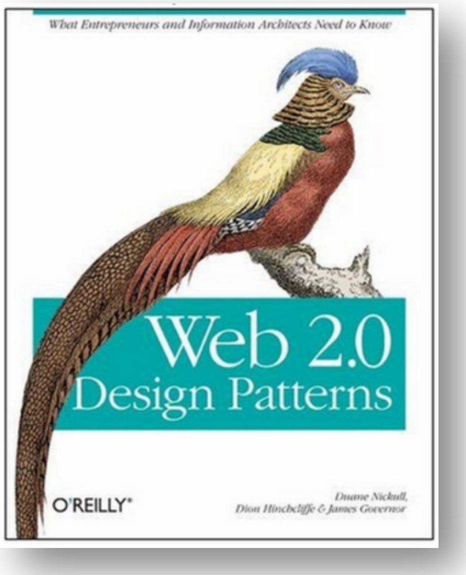

The Addison-Wesley Signature Series
Patterns of Enterprise Application Architecture
A Martin Fowler Signature Book
Martin Fowler
With Contributions by
David Rice,
Matthew Foemmel,
Edward Hieatt,
Robert Mee, and
Randy Stafford


The Addison-Wesley Signature Series
Enterprise Integration Patterns
Designing, Building, and Deploying Messaging Solutions
A Martin Fowler Signature Book
Gregor Hohpe
Bobby Woolf
With Contributions by
Kyle Brown
Conrad F. D'Cruz
Martin Fowler
Sean Neville
Michael J. Rettig
Jonathan Simon
Forewords by John Crupi and Martin Fowler

Next?


.NET Patterns
Architecture, Design, and Process
Christian Thilmany
Foreword by David Chappell
Software Patterns Series


Addison-Wesley Professional Ruby Series
Design Patterns in Ruby
Foreword by Obie Fernandez
Professional Ruby Series Editor
Russ Olsen


What Entrepreneurs and Information Architects Need to Know
Web 2.0 Design Patterns
O'Reilly
Duane Nickull,
Dion Hinchcliffe & James Governor

Our Dream:

+

=

New web application framework idea

Design-time security analysis

Secure-by-default web application framework

CC Flickr User Evan Hunter, NC ND

CC Flickr User IceSabre, NC

CC Flickr User AMagill