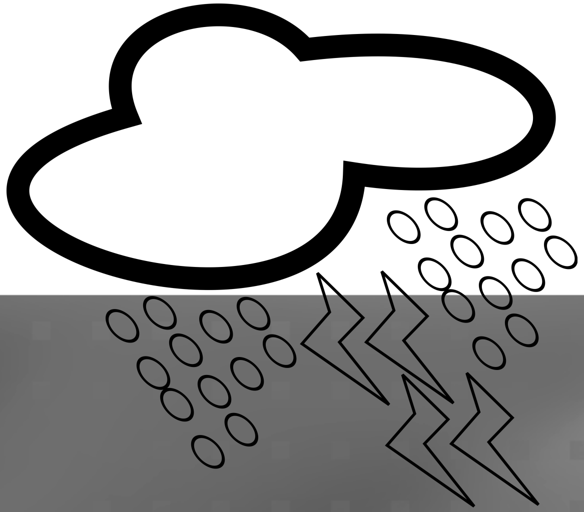


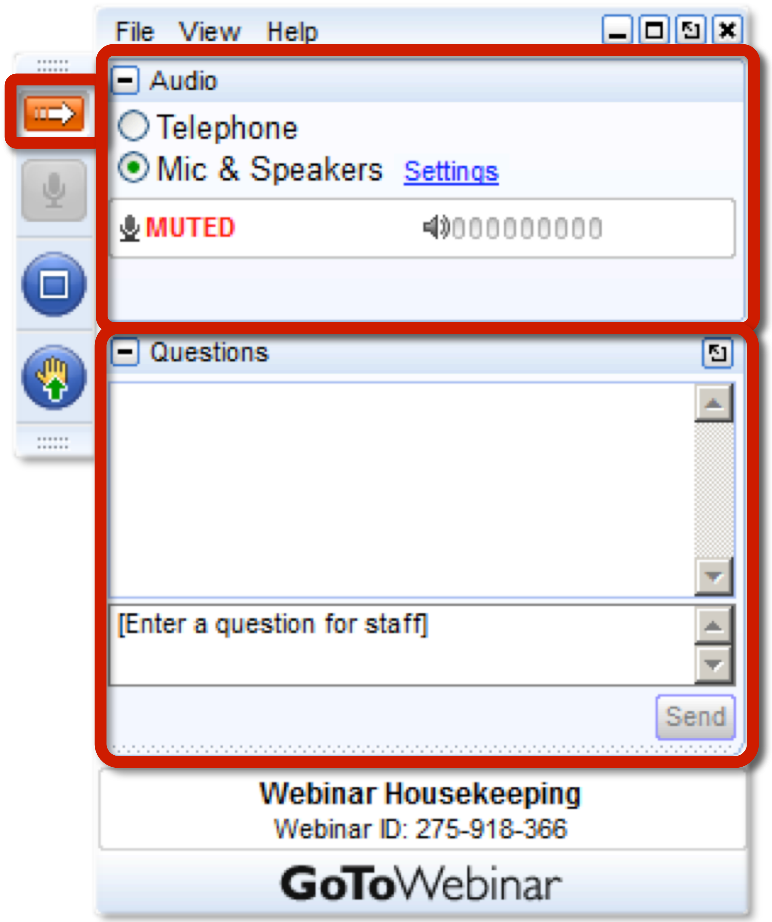
Cloudy With a Chance of Cyber-attacks

Securing Cloud-based Applications

Parasoft

January 2013

GoToWebinar Housekeeping



○ Telephone
● Mic & Speakers

MUTED

[Enter a question for staff]

Webinar Housekeeping
Webinar ID: 275-918-366

Your Participation

Open and hide your control panel

Join audio:

- Choose "Mic & Speakers" to use VoIP
- Choose "Telephone" and dial using the information provided

Submit questions and comments via the Questions panel

Note: Today's presentation is being recorded and will be provided within 48 hours.

In The News

Jan 2013
Restaurant Chain Zaxby's Discloses Security Breach

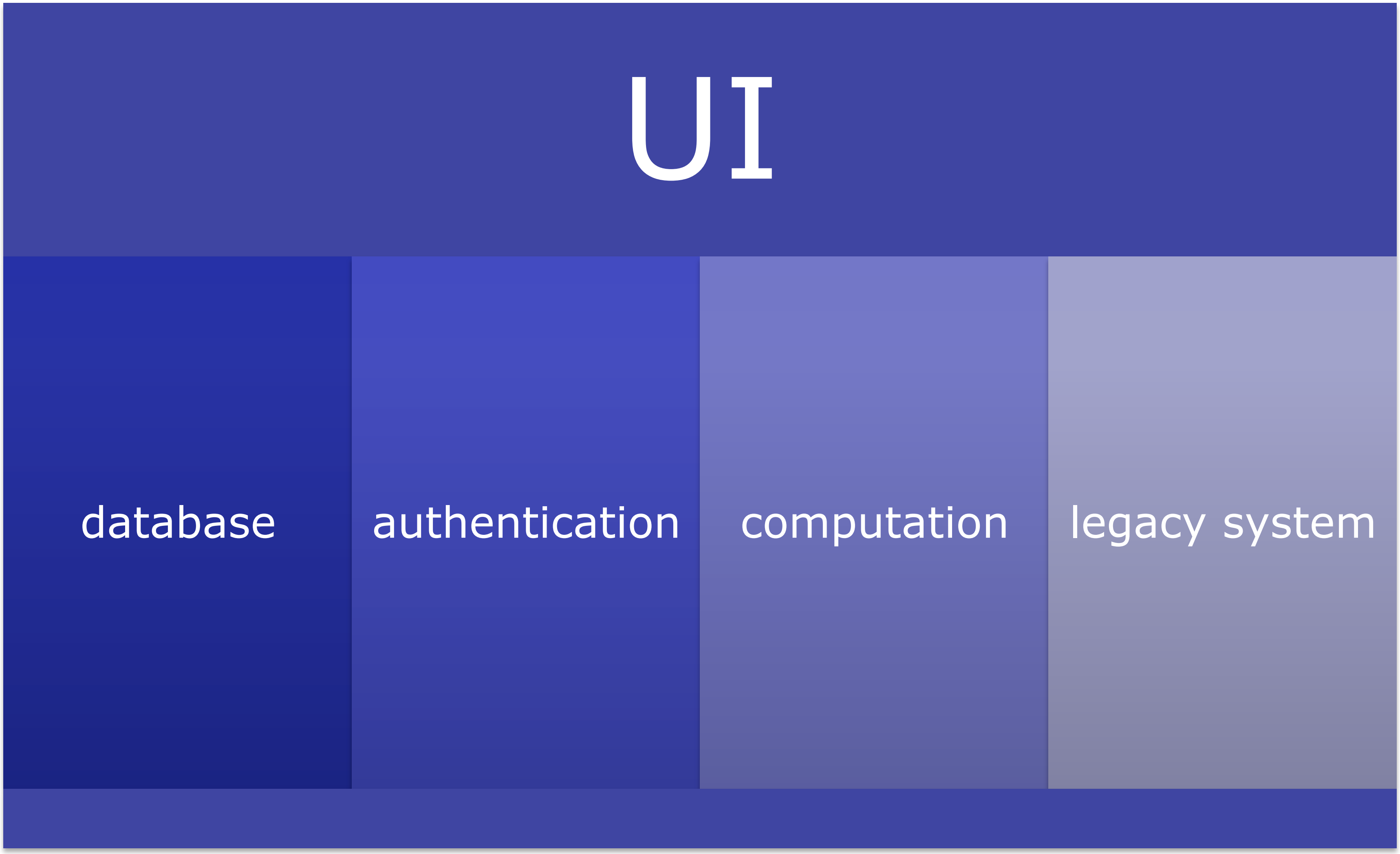
Jan 2013
Utah Health Department Acknowledges New Security Breach

Jan 2013
Cumberland investigates website security breach

Jan 2013
Florida Department of Juvenile Justice Suffers Security Breach

December 2012
Breach of 1.6M accounts at FBI, NASA, and more

Attack Surfaces – Traditional Application



UI

database

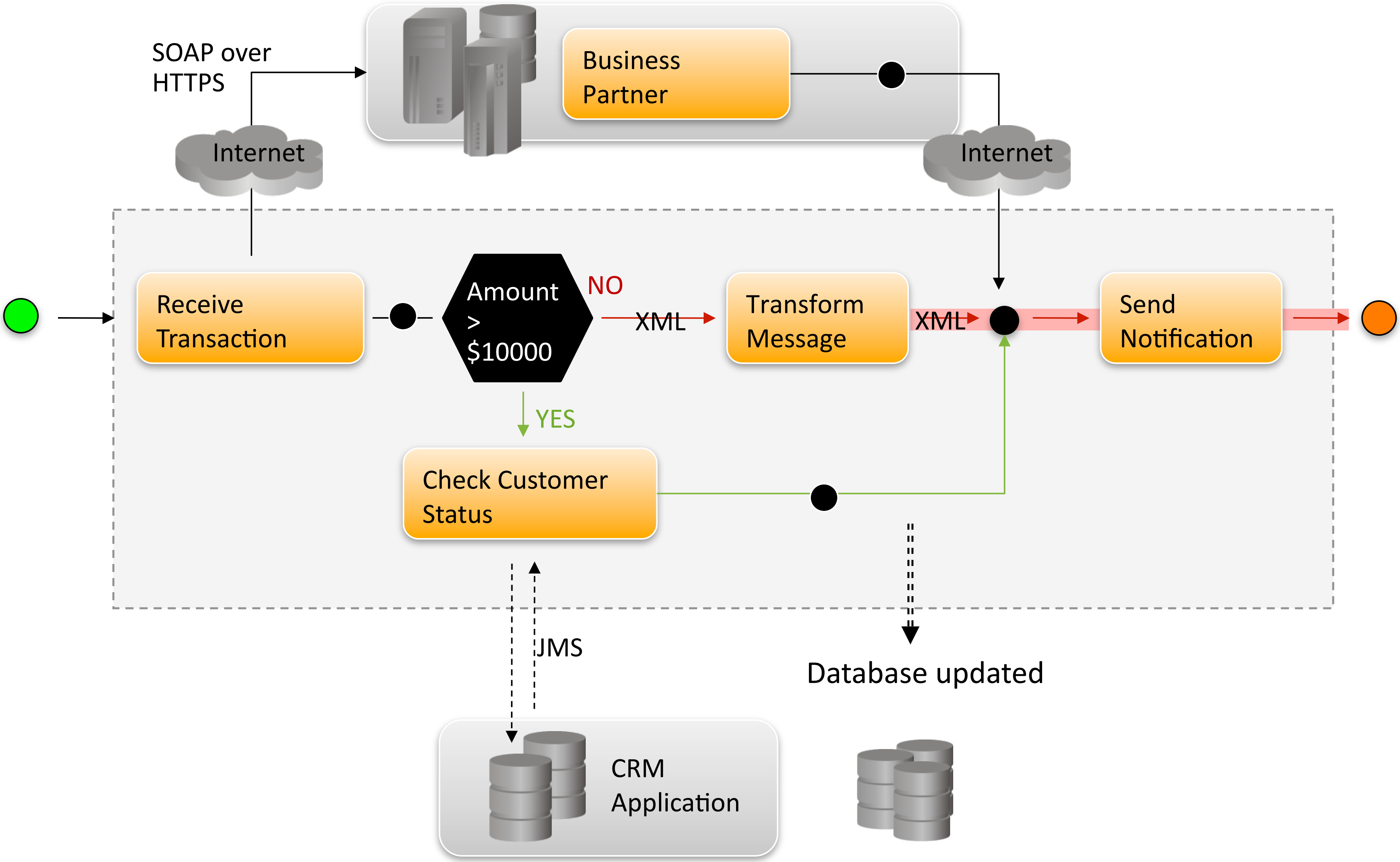
authentication

computation

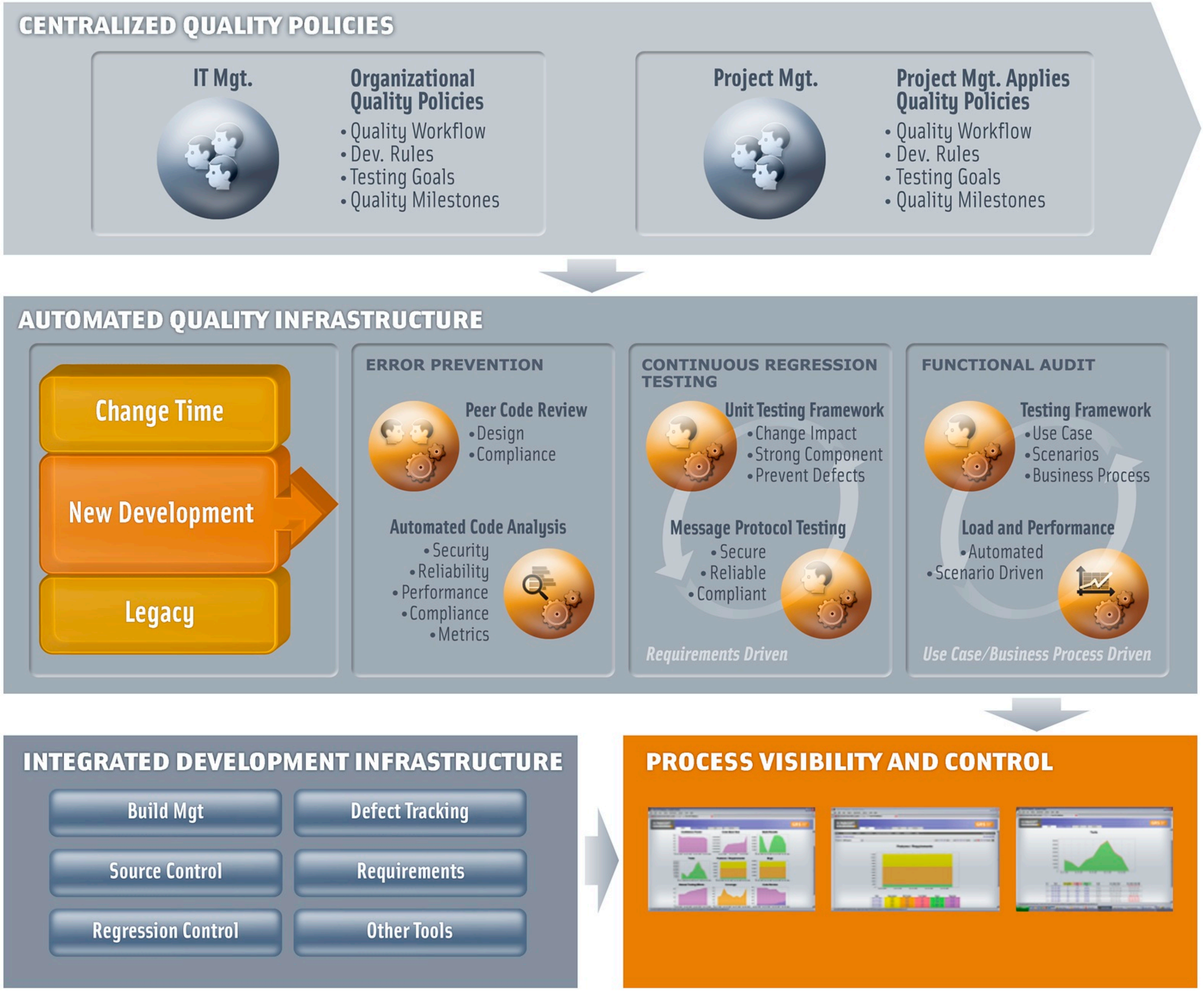
legacy system

Attack Surfaces in the Cloud

PARASOFT



Comprehensive Solution Required



CENTRALIZED QUALITY POLICIES

IT Mgt.

Organizational Quality Policies
- Quality Workflow
- Dev. Rules
- Testing Goals
- Quality Milestones

Project Mgt.

Project Mgt. Applies Quality Policies
- Quality Workflow
- Dev. Rules
- Testing Goals
- Quality Milestones

AUTOMATED QUALITY INFRASTRUCTURE

Change Time

New Development

Legacy

ERROR PREVENTION

Peer Code Review
- Design
- Compliance

Automated Code Analysis
- Security
- Reliability
- Performance
- Compliance
- Metrics

CONTINUOUS REGRESSION TESTING

Unit Testing Framework
- Change Impact
- Strong Component
- Prevent Defects

Message Protocol Testing
- Secure
- Reliable
- Compliant

Requirements Driven

FUNCTIONAL AUDIT

Testing Framework
- Use Case
- Scenarios
- Business Process

Load and Performance
- Automated
- Scenario Driven

Use Case/Business Process Driven

INTEGRATED DEVELOPMENT INFRASTRUCTURE

Build Mgt

Defect Tracking

Source Control

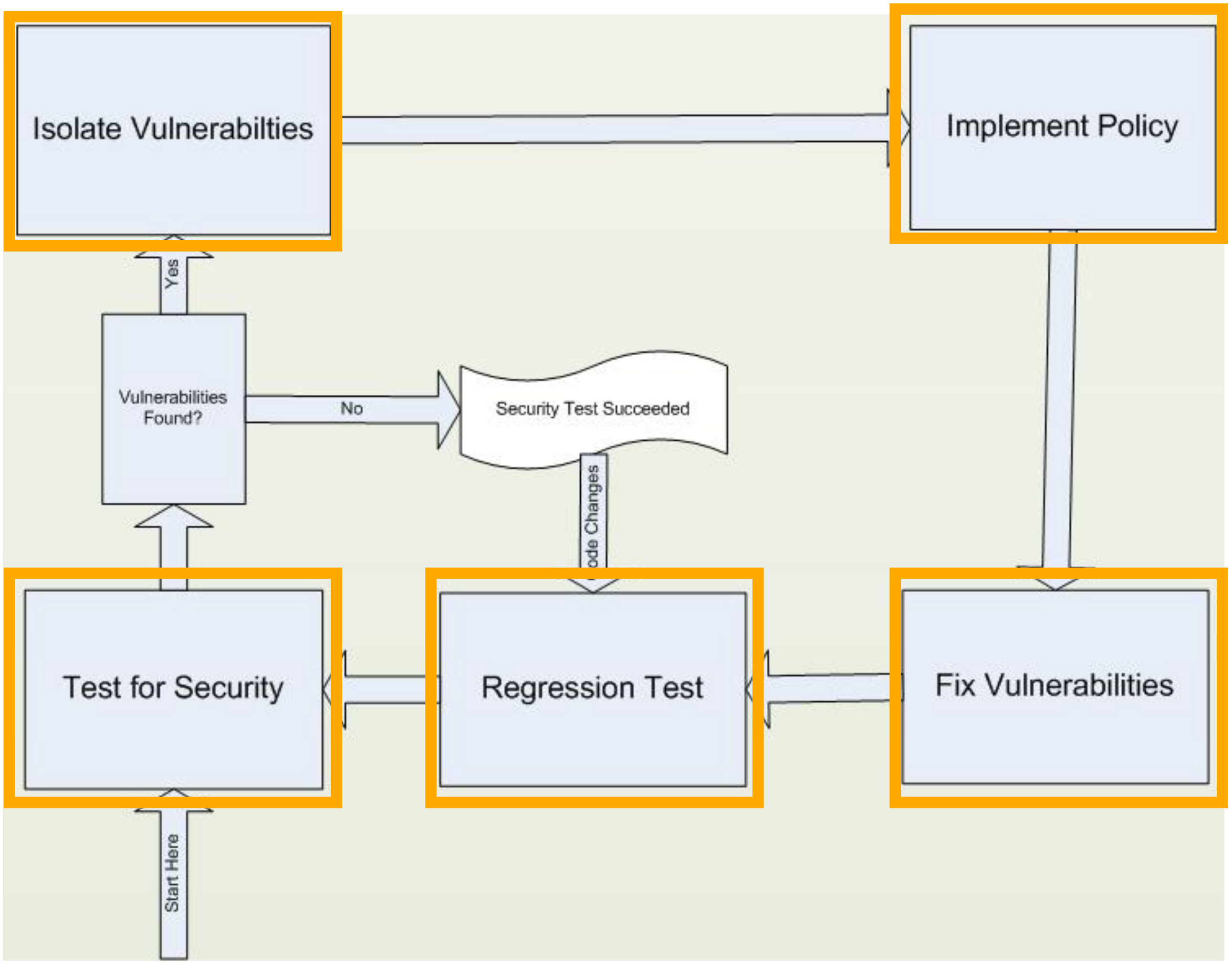
Requirements

Regression Control

Other Tools

PROCESS VISIBILITY AND CONTROL

Securing An Application



Policy Management

- Capabilities
  - Centralized management and reporting of “expectations”
  - Knowledgebase
- Benefits
  - Globally accessible
  - Promotes predictable results
- Drawbacks
  - Must invest time to develop and evolve

Static Analysis

- Capabilities
  - Find real security bugs
  - Low cost method
- Benefits
  - Detects problems early
  - Trains developers by pointing out problematic code
- Drawbacks
  - Must be properly configured
  - Flow-analysis alone cannot prevent

Peer Code Review

- Capabilities
  - Facilitates high-level analysis of security and design

- Benefits
  - Identifies complex vulnerabilities
  - Keeps team in sync

- Drawbacks
  - Peer code review is mostly talked about and easily delayed

Unit Testing

- Capabilities
  - Starts testing validation methods and verifying security functionality before the system is complete
- Benefits
  - Reduces the time required for validation
  - Can expose potential vulnerabilities earlier than pre-production
- Drawbacks
  - Test cases must be kept in sync with evolving application

Continuous Regression Testing

- Capabilities
  - Runs all existing test on a continuous basis
  - Alerts team of failures
- Benefits
  - Ensures that the application remains secure
  - Ensures stability during change
- Drawbacks
  - Must keep test cases in sync

Penetration Testing

- Capabilities
  - Should verify that the security policy is operates correctly
  - Outside-in testing
- Benefits
  - Validates against known attack scenarios
- Drawbacks
  - Not a complete system
  - Late stage technology
  - Reactive

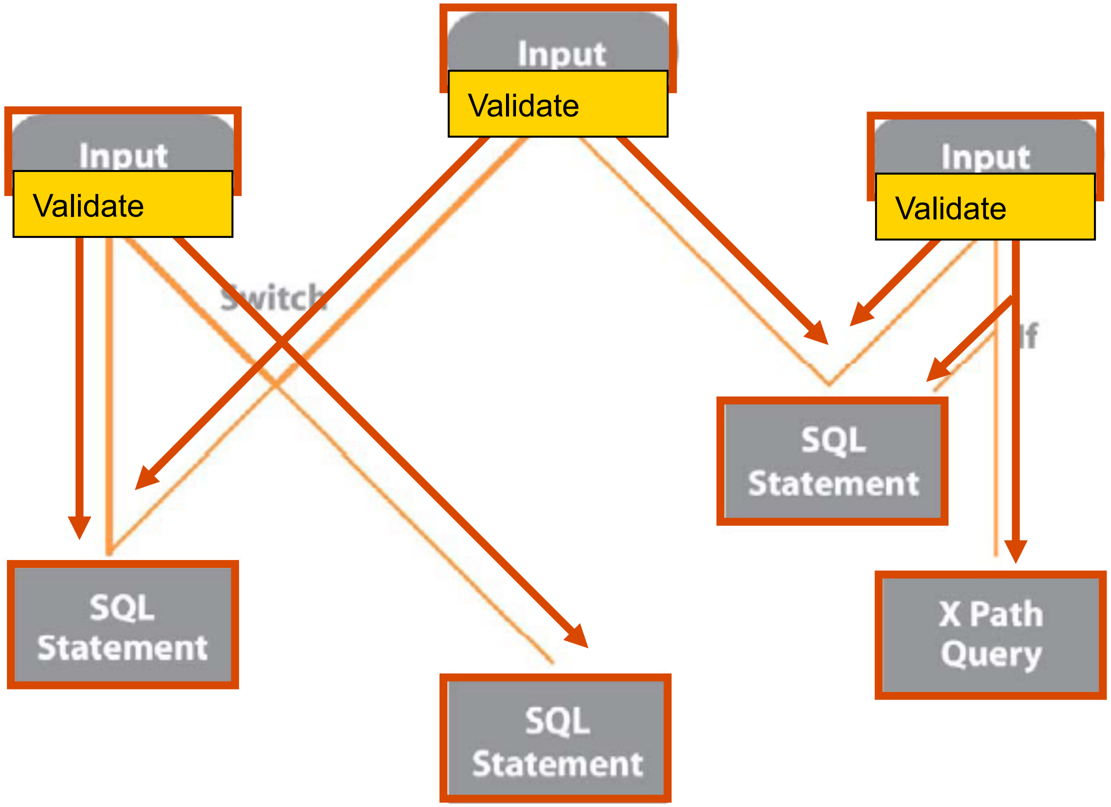
Coding Defensively: Validating inputs

The Solution = validate inputs upon entry

3 entry points

9 paths through the code

4 potential vulnerabilities



Input Validation Approach

- Validate every input immediately after it is received
- Input validation prevents attacks on the application
- Prevents over half of the most common web application vulnerabilities
  - Cross-site scripting
  - Injection flaws
  - Misc file execution
  - Cross site request forgery
  - Failure or restrict URL access

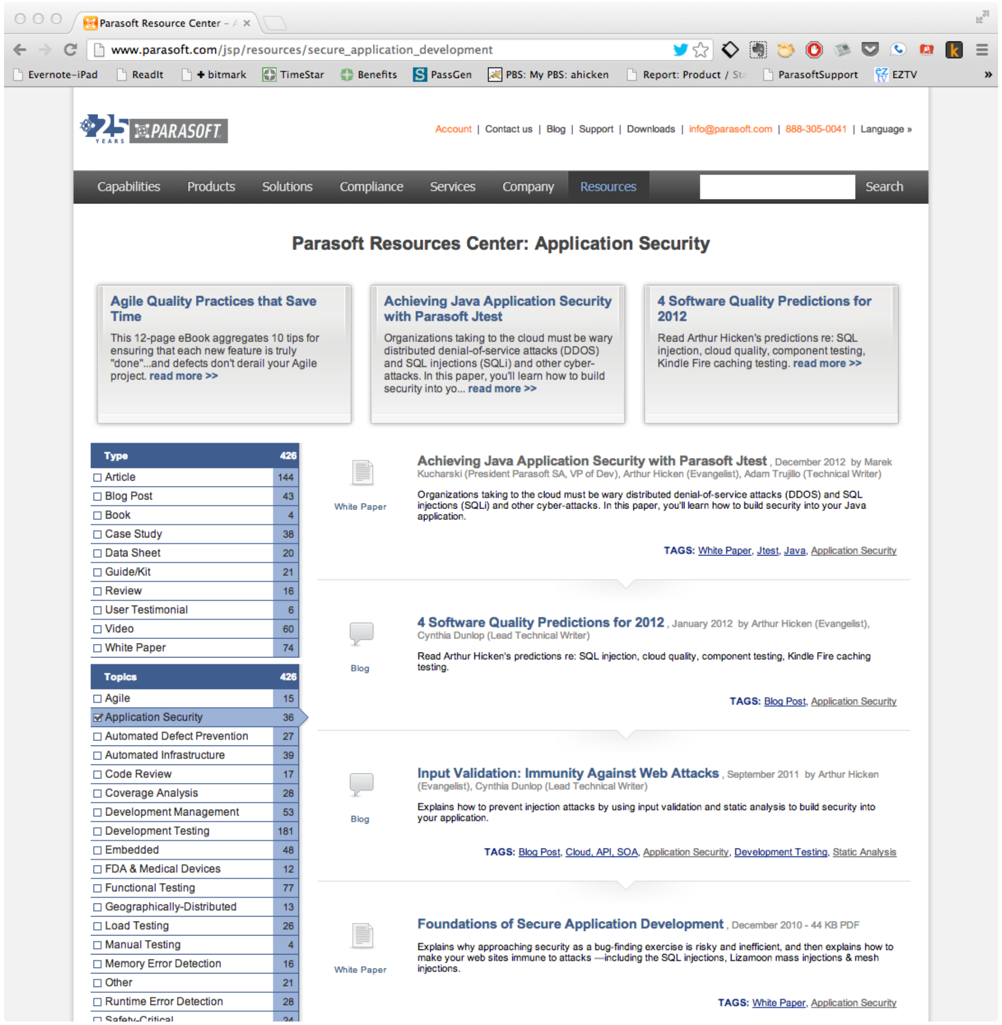
Security Resources

PARASOFT®

- CWE – Common Weakness Enumeration
  - http://cwe.mitre.org
- OWASP - Open Web Application Security Project
  - http://www.owasp.org
- PCI – Payment Card Industry Security Standards
  - https://www.pcisecuritystandards.org
- Hack.me – Community based security learning project
  - https://hack.me
- SAMATE - Software Assurance Metrics And Tool Evaluation
  - http://samate.nist.gov
- Build Security In – Collaborative security effort
  - https://buildsecurityin.us-cert.gov

Resources

- info@parasoft.com webinar@parasoft.com



Parasoft Resources Center: Application Security

Agile Quality Practices that Save Time

This 12-page eBook aggregates 10 tips for ensuring that each new feature is truly "done"...and defects don't derail your Agile project. **read more >>**

Achieving Java Application Security with Parasoft Jtest

Organizations taking to the cloud must be wary distributed denial-of-service attacks (DDOS) and SQL injections (SQLi) and other cyber-attacks. In this paper, you'll learn how to build security into yo... **read more >>**

4 Software Quality Predictions for 2012

Read Arthur Hicken's predictions re: SQL injection, cloud quality, component testing, Kindle Fire caching testing. **read more >>**

Type	426
□ Article	144
□ Blog Post	43
□ Book	4
□ Case Study	38
□ Data Sheet	20
□ Guide/Kit	21
□ Review	16
□ User Testimonial	6
□ Video	60
□ White Paper	74

Topics	426
□ Agile	15
☑ Application Security	36
□ Automated Defect Prevention	27
□ Automated Infrastructure	39
□ Code Review	17
□ Coverage Analysis	28
□ Development Management	53
□ Development Testing	181
□ Embedded	48
□ FDA & Medical Devices	12
□ Functional Testing	77
□ Geographically-Distributed	13
□ Load Testing	26
□ Manual Testing	4
□ Memory Error Detection	16
□ Other	21
□ Runtime Error Detection	28
□ Safety-Critical	24

White Paper

Achieving Java Application Security with Parasoft Jtest , December 2012 by Marek Kucharski (President Parasoft SA, VP of Dev), Arthur Hicken (Evangelist), Adam Trujillo (Technical Writer)

Organizations taking to the cloud must be wary distributed denial-of-service attacks (DDOS) and SQL injections (SQLi) and other cyber-attacks. In this paper, you'll learn how to build security into your Java application.

TAGS: White Paper, Jtest, Java, Application Security

Blog

4 Software Quality Predictions for 2012 , January 2012 by Arthur Hicken (Evangelist), Cynthia Dunlop (Lead Technical Writer)

Read Arthur Hicken's predictions re: SQL injection, cloud quality, component testing, Kindle Fire caching testing.

TAGS: Blog Post, Application Security

Blog

Input Validation: Immunity Against Web Attacks , September 2011 by Arthur Hicken (Evangelist), Cynthia Dunlop (Lead Technical Writer)

Explains how to prevent injection attacks by using input validation and static analysis to build security into your application.

TAGS: Blog Post, Cloud, API, SOA, Application Security, Development Testing, Static Analysis

White Paper

Foundations of Secure Application Development , December 2010 - 44 KB PDF

Explains why approaching security as a bug-finding exercise is risky and inefficient, and then explains how to make your web sites immune to attacks —including the SQL injections, Lizamoon mass injections & mesh injections.

TAGS: White Paper, Application Security