

Secure Software Purchasing

Matthew Moynahan, CEO, Veracode

Jim Routh, CISO, Depository Trust Corporation

VERACODE

The Problem with My Jeep...



The World's Next Big Problem is Our Insecure Software Infrastructure – And It Is A Global Problem

- The software industry is the world's largest manufacturing industry (\$235B) with **NO** notion of security quality. It forms the fabric of our modern infrastructure.
- 7,000 new security vulnerabilities in 2007 and over \$117B in losses from identity theft alone...and things are getting worse.

2007

America's Hackable Backbone

Researchers hack into and take control over a nuclear power plant



2007

iPhone hacked in minutes after launch; multiple vulnerabilities found, Apple discloses backdoor "feature" on iPhone



2007

45.7M credit card numbers stolen by largest cyber criminal ring yet from TJX, costing TJX \$256M, stock drops 8%



2007

Experimental cyber attack causes generator to self-destruct. Could cause \$700B in damage on mass scale



2008

FAA announces New Boeing 787 plane controls could be taken over by hackers during flight



2008

Multiple cross-site scripting (XSS) vulnerabilities discovered in Google, Facebook and MySpace. Backdoors found in Gmail



How Did the Software Industry Get So Insecure?

Software Buyers



- Unable to “test-before-buy” - no source code
- No legal recourse
- Time-consuming and expensive to test
- Limited security expertise

Software Manufacturers

ISV

- Focus on minimizing cost and maximizing features
- Too time consuming to conduct proper testing
- Limited security expertise
- Minimal incentives

Code Complexity



- Modern software development creates mixed code bases
- Software of Unknown Pedigree (“SOUP”)
- Increasing frequency of change from Web 2.0

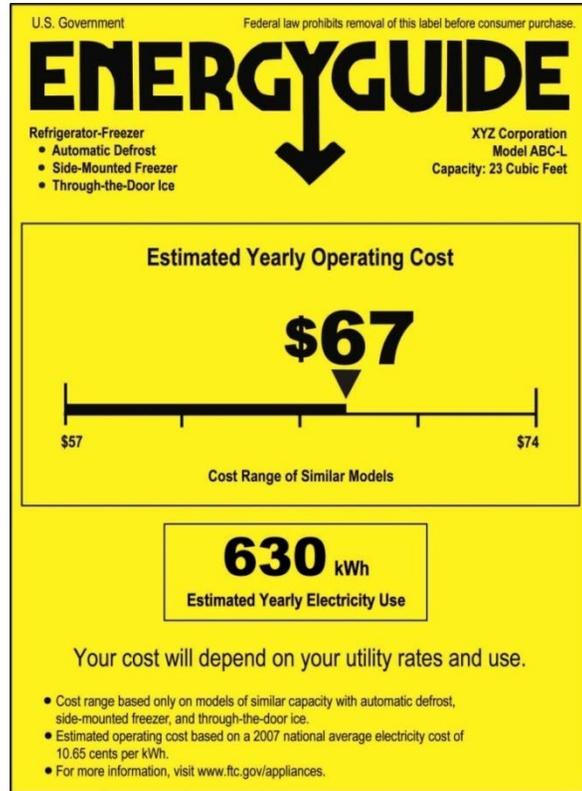
All Application Security Risk Has Two Root Causes



Application Development and Procurement Have Become Increasingly Distributed and Complex



Why Have Independent Assessments of Commercial Software Been So Elusive?



Would you purchase a hot water heater without knowing how much it would cost to operate?



Would Coke and Pepsi agree to a taste test in a grocery store if they had to give you their secret formulas (e.g. source code)?

Other Industries Have Been Successful in Creating Demand for Security in Products

Auto Safety

Prior Status

- Limited visibility into car safety
- No benchmark or consistent safety measurement
- Focus on end-point (driver behavior), not source (car manufacturer)
- Result: high insurance rates, unbounded risk

Industry Initiative

**INSURANCE INSTITUTE
FOR HIGHWAY SAFETY**

Results

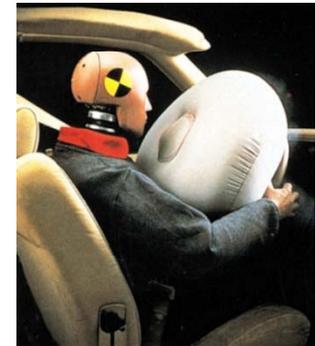
- Shift to source of risk
- Safety improvements (seat belts, air bags, crumple zones, stability control) built into cars
- Objective benchmark for auto safety

Software Security

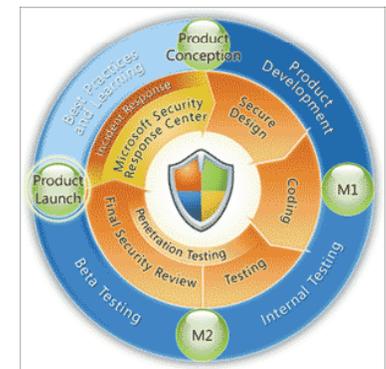
- Limited visibility into safety of COTS
- No benchmark or consistent security measurement
- Focus on end-point (enterprise), not source (software vendor)
- Result: high operational cost, unbounded risk

Pressure from Software Buyer Community

- Shift to source of risk
- Security built into the SDLC
- Objective benchmarking and reasonable security acceptance criteria



Microsoft



Microsoft SDL

Momentum Began with Secure Software Purchasing Coalition of Early Adopter Financial Service Institutions

Key Coalition Objectives

- » Shifts responsibility and operational cost of application security from enterprise to ISV (or shared initially)
- » Minimizes current unbounded risk with 3rd Party software
- » Establishes mitigating controls by creating “acceptance criteria” for purchased software, before it is deployed in-house
- » Develops a security procurement governance model that delivers permanent and persistent success from procurement best practices
- » Provides major efficiencies and cost savings by eliminating redundant testing; reducing patch and customer support costs and development rework

What would a service look like to rate COTS software?

VERACODE

Any New Model Must Look at Strengths and Weaknesses of Current Approaches



Security Consultants

- Expensive
- Do not scale
- Inconsistent
- In short supply



Analysis Tools

- High FP & FN rates
- Islands of information
- Disparate output formats
- Long learning curves

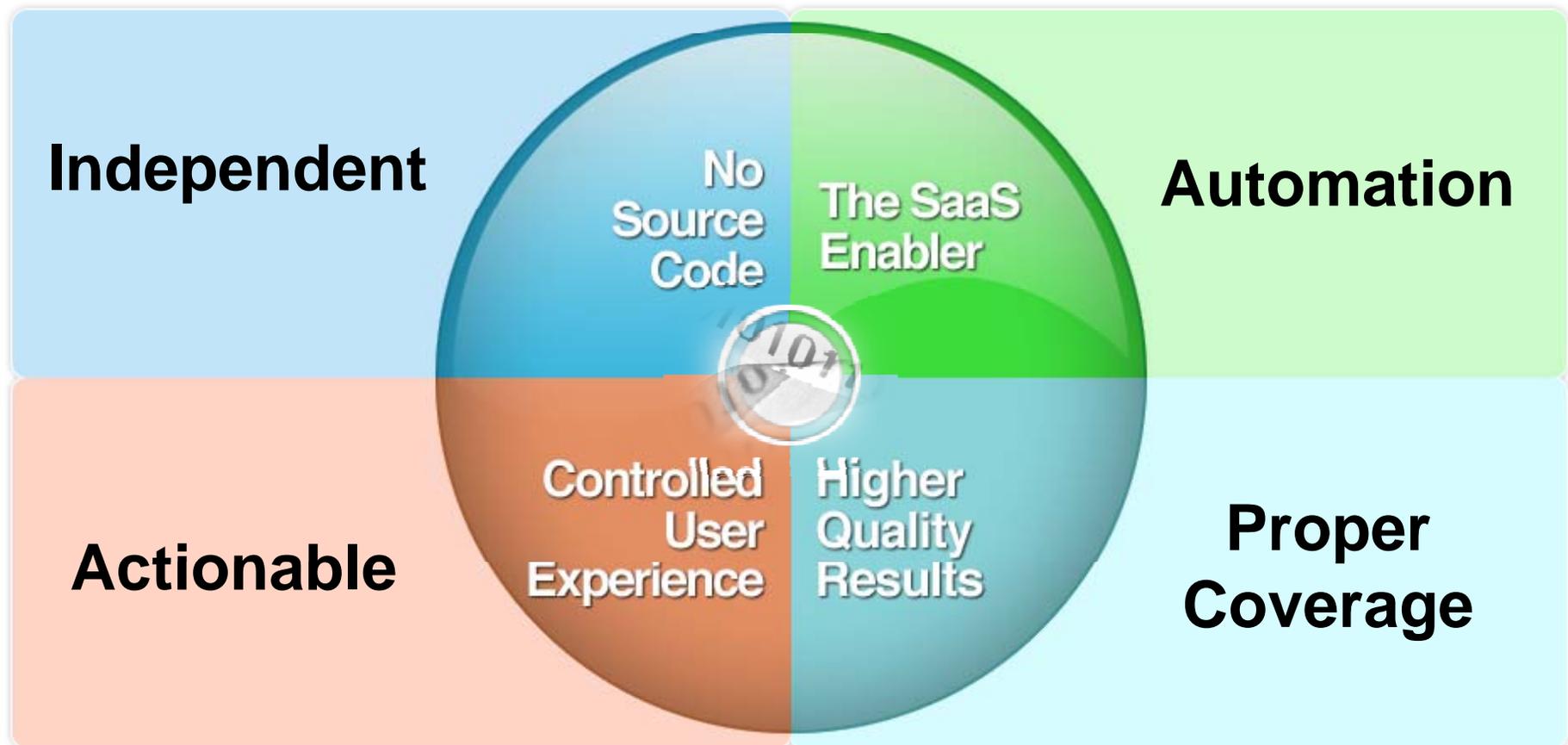


Processes

- Complex development and supply chain relationships
- No separation of duties
- Increased requirement for IV&V

Veracode was created to overcome these limitations

Four Requirements Necessary for Effective Vendor Software Security Assessments



Veracode's Software Assurance Center

Veracode Software Assurance Center

Login

Enter Username, Password and Token Passcode below.

Username:

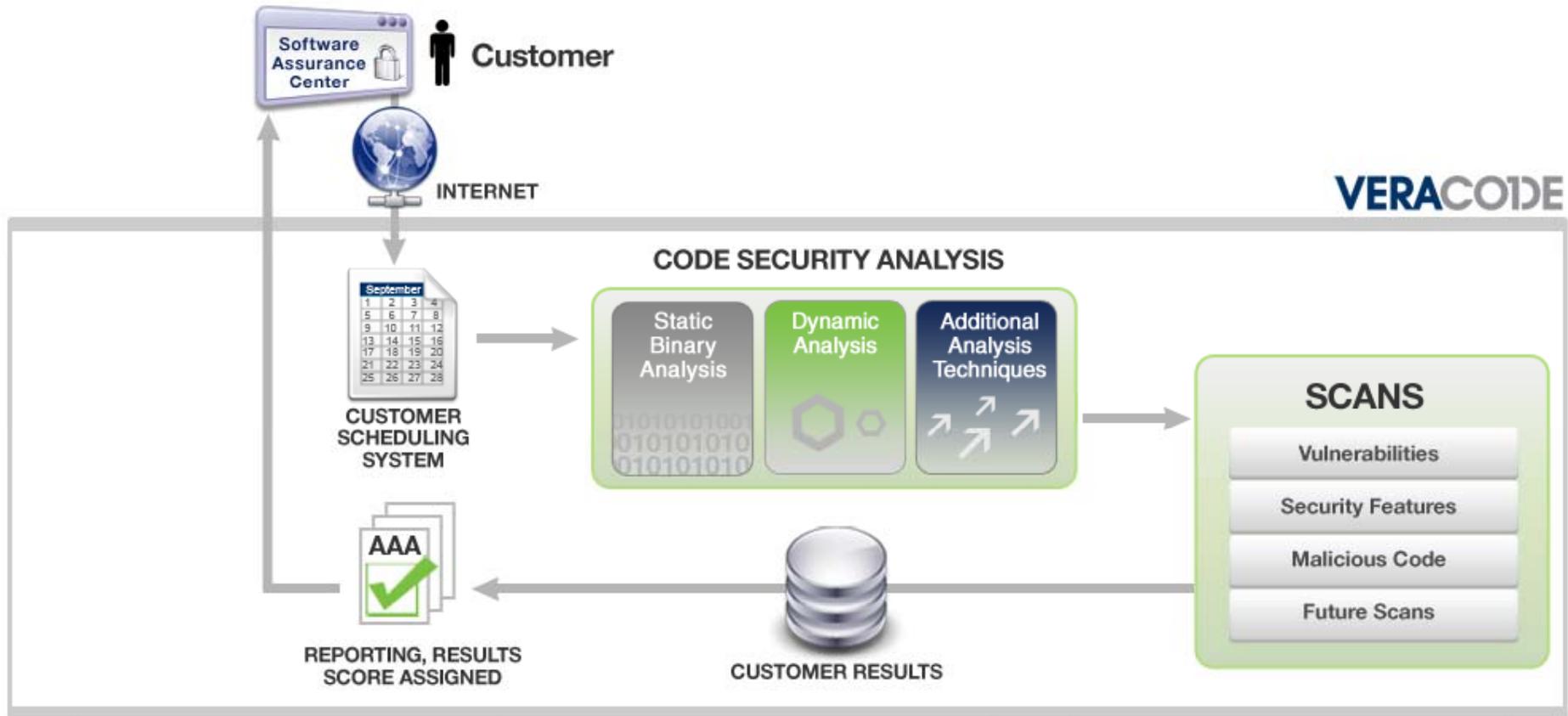
Password:

Passcode:

[Verify Browser](#) | [Forgot Password ?](#)

Copyright Veracode, Inc., 2008

Veracode's "In-the-Cloud" Software Assessment Factory



1 Simply upload application & schedule tests. Results within 24-72 hours.

2 Results include security rating & advice to easily fix security vulnerabilities.

3 Powerful data analysis enable trending and more informed decision-making.

Case Study: DTCC

Depository Trust Clearing Corporation

VERACODE



DTCC Software Security Program

Jim Routh, CISM
CISO
DTCC

Jrouth@dtcc.com



About DTCC

DTCC, through its subsidiaries, provides clearance, settlement and information services for equities, corporate and municipal bonds, government and mortgage-backed securities, money market instruments and over-the-counter derivatives. In addition, DTCC is a leading processor of mutual funds and insurance transactions, linking funds and carriers with their distribution networks. DTCC's depository provides custody and asset servicing for more than 3.5 million securities issues from the United States and 110 other countries and territories, valued at \$40 trillion.

In 2007, DTCC settled more than \$1.8 quadrillion in securities transactions

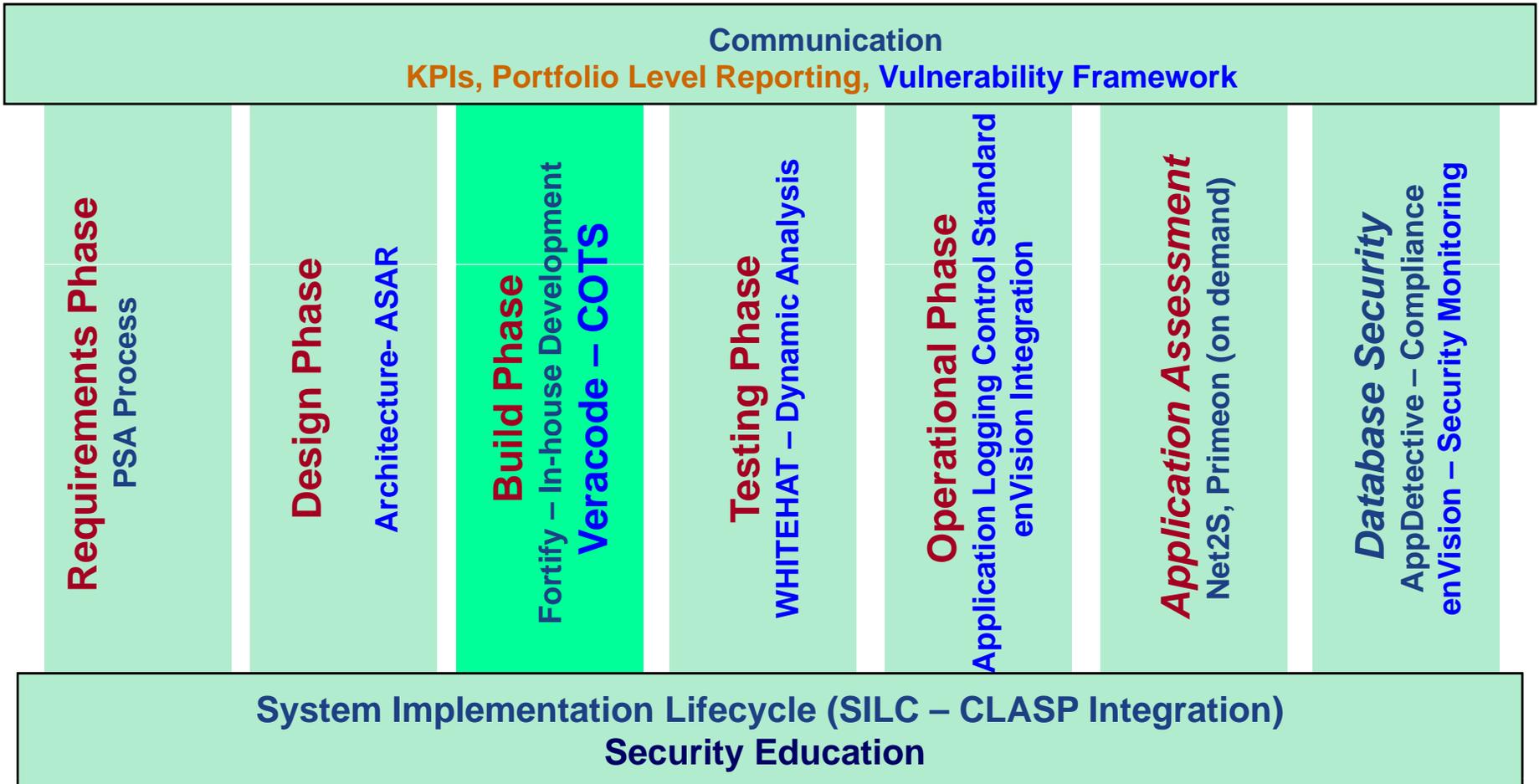


Challenge: COTS Security

- DTCC sought a viable approach to conducting security assessments of commercial off the shelf software that represented a potential risk to institutional customers
- DTCC chose to integrate a Veracode scan into the requirements for high risk software products
- This control fits into a comprehensive program for software security



DTCC's Software Security Program





DTCC COTS Security Process

Software Request

Static Code Analysis

Dynamic Analysis

Manual

Requirements Contract

1.

“White Box” Testing

“Black Box” Testing

Pen Tests End-to-end



Vulnerabilities by project, portfolio and across portfolios



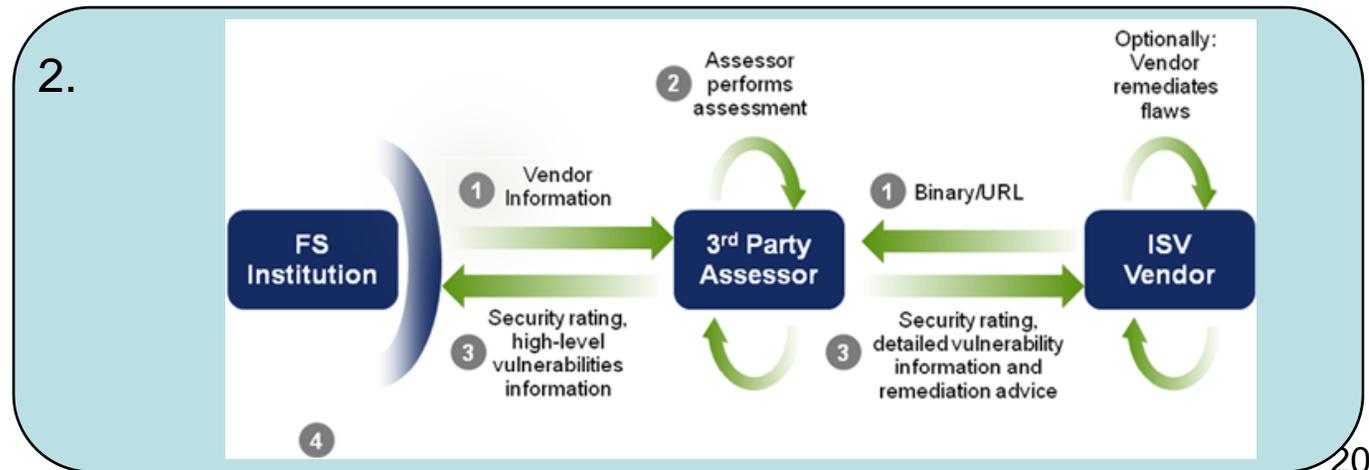
Vulnerabilities by project, portfolio and across portfolios



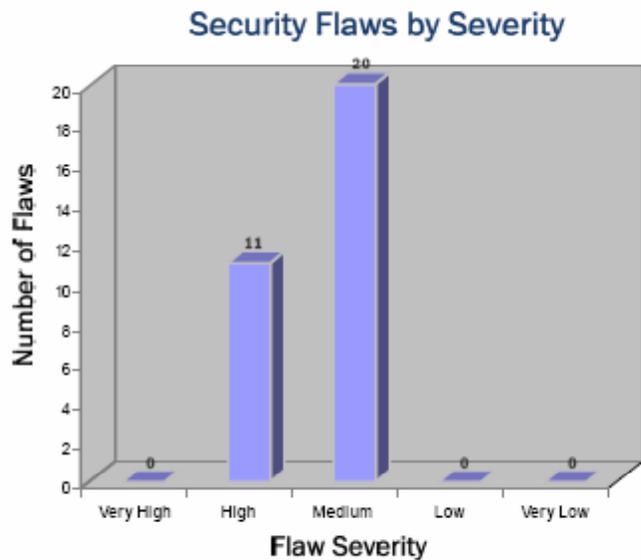
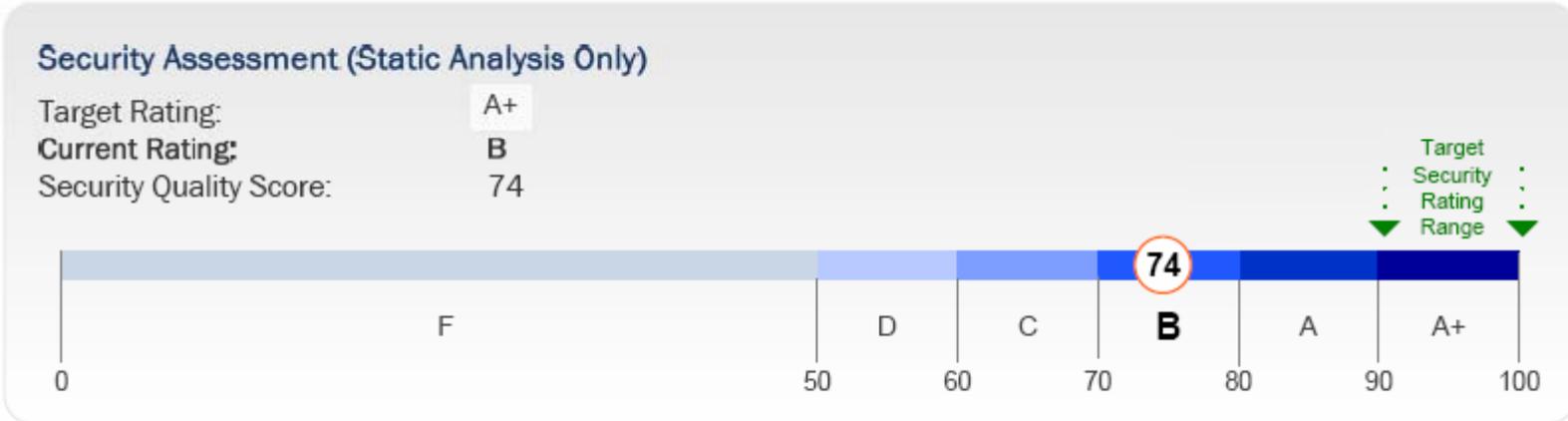
Remediation List	
1. High	Closed
2. Med	Closed
3. Low	Open
4. Med	Closed
5. High	Closed
6. Med	Open

Remediation List

2.



DTCC Received High Level AppSec Report to Make More Informed Business Decisions



Top Risks

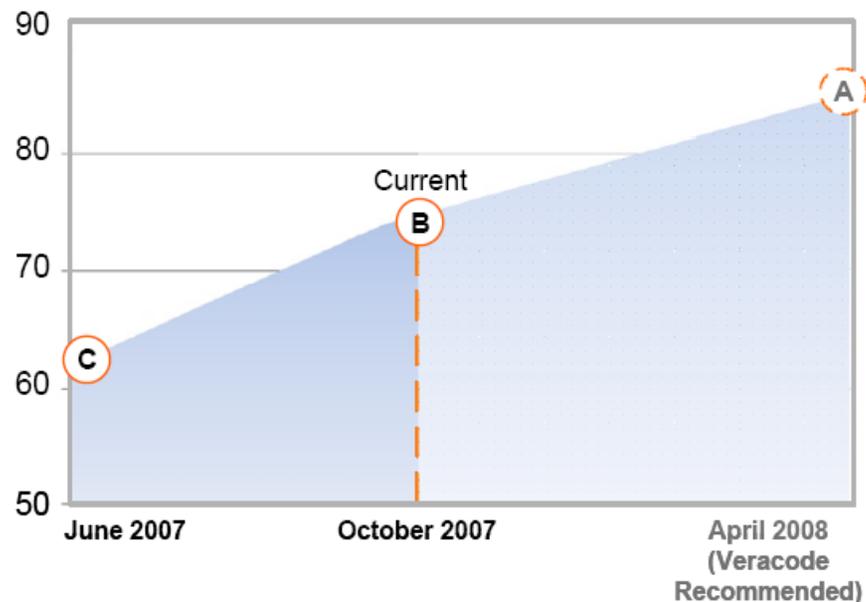
Top security flaws detected in the application included:

Flaw Category	Severity	Count
Leftover Debug Code	High	6
Unchecked Error Condition	High	5
Insufficient Entropy in PRNG	Medium	7
Often Misused: Authentication	Medium	3
Basic XSS	Medium	2

Total Flaws detected in application: 31

COTS SecurityReview Remediation Roadmap Report

Application Ratings Trend



- In June 2007, Veracode analyzed, scored and rated Application version 1.0. It received a security quality score of 62, corresponding to a C rating.
- In October 2007, Veracode analyzed, scored and rated Application version 2.0. The security quality score was 74, corresponding to a B rating.
- The Security Improvement Roadmap (below) outlines what actions Independent Software can take to increase the rating to A by April of 2008.

ISV Received Detailed Vulnerability Information to Remediation Platform

Veracode Scan Review: Apache IHTTP Server

Overall Rating: **D**

Scan Type: **Static Analysis** | Dynamic Analysis

Show: Fix First Analyzer Source Code Viewer None

"Fix First" Analyzer

Veracode recommends that developers prioritize remediation efforts in terms of a combination of flaw severity and effort, with high severity/low effort flaws being prioritized to "fix first".

Click on the red circles to the left to browse your application flaws by their "fix first" status.

ALL FLAWS | BY FOLLOW-UP | BY ANNOTATIONS

Total Flaws: 37 Selected Flaw: Search: ID

ID	Severity	Exploitability	Category	Type	CWE ID	Module	Source
8	High	-	Stack-based Buffer Overflow	fgets	121	httpd	
13	High	-	Stack-based Buffer Overflow	fgets	121	httpd	
26	High	-	Use of inherently dangerous function	getenv	242	httpd	
27	High	-	Use of inherently dangerous function	getenv	242	httpd	
41	High	-	Stack-based Buffer Overflow	strcpy	121	httpd	
52	High	-	Use of inherently dangerous function	getenv	242	httpd	
65	High	-	Stack-based Buffer Overflow	strcpy	121	httpd	
31	High	-	Unchecked Error Condition	strlen	381	httpd	
35	High	-	Externalization of Insecure Variables	getopt	414	httpd	

Flaws Call Stack

Vulnerability "Fix First" Chart

Results Stitch Directly to Line of Source Code for Remediation

Veracode Scan Review: Apache HTTP Server

Overall Rating: **D**

Scan Type: **Static Analysis** | Dynamic Analysis

Show: Fix First Analyzer Source Code Viewer None

Source Code View: *util_script.c*

```

583 }
584
585 static int getfunf_FILE(char *buf, int len, void *f)
586 {
587     return fgsets(buf, len, (FILE *) f) != NULL;
588 }
589
590 int ap_scan_script_header_err(request_rec *r, FILE *f,
591                             char *buffer)
592 {
593     return ap_scan_script_header_err_core(r, buffer, getfunf_FILE, f);
594 }
595
596 static int getfunf_BUFF(char *v, int len, void *fb)
597 {
598     return ap_bgets(v, len, (BUFF *) fb) > 0;
599 }
600
    
```

ALL FLAWS | BY FOLLOW-UP | BY ANNOTATIONS

Total Flaws: 37 Selected Flaw: Search: ID

ID	Severity	Category	Type	CWE ID	Module	Source	Line #	Status
8	High	Stack-based Buffer Overflow	fgets	121	httpd	util.c	818	open
13	High	Stack-based Buffer Overflow	fgets	121	httpd	util_script.c	587	open

Description: This call to fgsets() contains a buffer overflow. The source string has a size (excluding termination) of (unavailable) bytes, and the destination buffer is (unavailable) bytes. If an attacker can control the data written into the buffer, the overflow may result in execution of arbitrary code. [Show Remediation](#)

Date	Review	Comment
10/16/07 14:53:32	test	
11/07/07 14:20:42		This needs to be fixed
02/01/08 11:14:40		This has been resolved
02/07/08 16:06:48		ok'd
02/09/08 12:38:11		Security OK
02/28/08 15:33:15		ok
03/20/08 16:37:59		reopening

Flaws Call Stack



ISVs May Choose 1 or 2

- Vendors are encouraged to either provide artifacts of controls or work with Veracode
- Once security assessment results are available, ISVs and DTCC agree on remediation priorities captured as Action Items in the Vendor Management section of the CIS Portal

The screenshot shows the CIS Portal interface in Microsoft Internet Explorer. The browser address bar displays a URL starting with 'https://www.dtcc.com/cisportal/'. The page title is 'CIS Portal'. The navigation menu on the left includes 'Vendor Management' and 'Vendor Profile: Sigertan'. The main content area shows the 'Assessments' section for the vendor 'Sigertan'. It includes a table for 'Action Items' with columns for 'Action Item ID', 'Action Required', and 'Vendor Name'. Below this, there are sections for 'Assessment Kickoff' and 'Onsite Assessment', each with a 'Tracking ID' field and a 'Vendor Name' field. The 'Assessment Status' is set to 'Completed'. The page footer contains copyright information for 2008 The Depository Trust & Clearing Corporation.



Lessons Learned

- Most software firms have limited or no security controls within the development process
- The Veracode service offers an easy way for these firms to both comply with DTCC requirements and build security into their software over time
- Almost 50% of the software vendors chose to use Veracode beyond the requirements as a core control for their development process
- DTCC's initial investment in the Veracode scanning process has been very successful and DTCC is using this process for selected internal applications as well

Veracode's Mission and Background

Veracode's mission is to make it easy and cost-effective for organizations to produce and purchase secure code.

2002 - 2004

- Application security consulting firm @stake develops technology to automate manual code reviews.
- SYMC acquires @stake to bolster AppSec expertise.

2006

- Founders/technology/patents spun-out of SYMC to create Veracode. \$19.5M secured from leading VCs and strategic investors.

2007

- Key patents filed for on-demand application security testing platform, ratings system, and business model.
- Commercial service launched at RSA 2007 and Delta, Cisco and Barclays sign as first enterprise customers.

2008

- Veracode becomes the industry's first provider of complete application security testing solution by combining static binary and dynamic analysis.
- Veracode gains major traction signing 60+ customers and obtaining industry recognition with 12 awards (e.g. Wall Street Journal Technology Award)

Any Questions?

Matthew Moynahan, CEO, Veracode
mmoynahan@veracode.com

VERACODE