



OWASP Enterprise Security API (ESAPI) for C Plus Plus

Dan Amodio

ESAPI for C Project Leader

Dan.Amodio@owasp.org

Dan.Amodio@aspectsecurity.com



April 5th, 2012

Who am I?

- OWASP
 - ▶ ESAPI – C Project leader
 - ▶ ESAPI – C++ Contributor
- Work
 - ▶ Application Security Engineer – Aspect Security
- Experience
 - ▶ Code Reviews
 - ▶ Architecture Reviews
 - ▶ Penetration Testing
 - ▶ Software Development
- Have Wife, Daughter, Hobbies, etc.



You?

- Developers
- Managers
- Security Professionals

This Presentation

- **ESAPI Project Overview**
- **ESAPI for C Plus Plus** (yes... really.)
- **Integrating Security Controls** (DEMO)
- **ESAPI Future** (3.0)



WHAT IS ESAPI?

Free and Open Source (OWASP)

The screenshot shows a web browser window displaying the OWASP Enterprise Security API project page. The browser's address bar shows the URL https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API. The page features the OWASP logo and the text "The Open Web Application Security Project". A navigation menu on the left lists various resources such as "Home", "News", "OWASP Projects", "Downloads", "Local Chapters", "Global Committees", "AppSec Job Board", "AppSec Conferences", "Cheat Sheets", "OWASP Training", "Presentations", "Video", "Press", "Get OWASP Books", "Get OWASP Gear", "Mailing Lists", "About OWASP", and "Membership". A "Reference" section includes "How To...", "Principles", "Threat Agents", "Attacks", "Vulnerabilities", "Controls", and "Activities". The main content area is titled "Category:OWASP Enterprise Security API" and includes a search bar and a table of navigation links. The table lists various languages and frameworks: Home, Downloads, What I did with ESAPI, Glossary, Java EE, Dot NET, Classic ASP, PHP, ColdFusion CFML, Python, JavaScript, Objective C, Force.com, Ruby, Swingset, ESAPI C, ESAPI CPP, ESAPI Perl, and Project Details. The text describes ESAPI as a free, open source, web application security control library. It lists three key features: a set of security control interfaces, a reference implementation for each security control, and optionally your own implementations for each security control. The page also mentions that the project source code is licensed under the BSD license and the Creative Commons license. A list of organizations adopting ESAPI is provided, including American Express, Apache Foundation, Booz Allen Hamilton, Aspect Security, Foundstone(McAfee), The Hartford, Infinite Campus, Lockheed Martin, MITRE, U.S. Navy - SPAWAR, The World Bank, and SANS Institute. A call to action asks users to let the project lead know how their organization is using OWASP ESAPI. At the bottom, there are three sections: "Let's talk here" with a link to "ESAPI Communities", "Got developer cycles?" with a link to "ESAPI Coding", and "Related resources" with a link to "OWASP Cheat Sheet Series". A sponsored advertisement for "ASPECT SECURITY Application Security Experts" is also visible.

Category:OWASP Enterprise Security API

Home Downloads What I did with ESAPI Glossary Java EE Dot NET Classic ASP PHP ColdFusion CFML Python JavaScript Objective C

Force.com Ruby Swingset ESAPI C ESAPI CPP ESAPI Perl Project Details

Sponsored by:

ASPECT SECURITY
Application Security Experts

ESAPI (The OWASP Enterprise Security API) is a free, open source, web application security control library that makes it easier for programmers to write lower-risk applications. The ESAPI libraries are designed to make it easier for programmers to retrofit security into existing applications. The ESAPI libraries also serve as a solid foundation for new development.

Allowing for language-specific differences, all OWASP ESAPI versions have the same basic design:

- There is a set of security control interfaces. They define for example types of parameters that are passed to types of security controls.
- There is a reference implementation for each security control. The logic is not organization-specific and the logic is not application-specific. An example: string-based input validation.
- There are optionally your own implementations for each security control. There may be application logic contained in these classes which may be developed by or for your organization. An example: enterprise authentication.

This project source code is licensed under the BSD license, which is very permissive and about as close to public domain as is possible. The project documentation is licensed under the Creative Commons license. You can use or modify ESAPI however you want, even include it in commercial products.

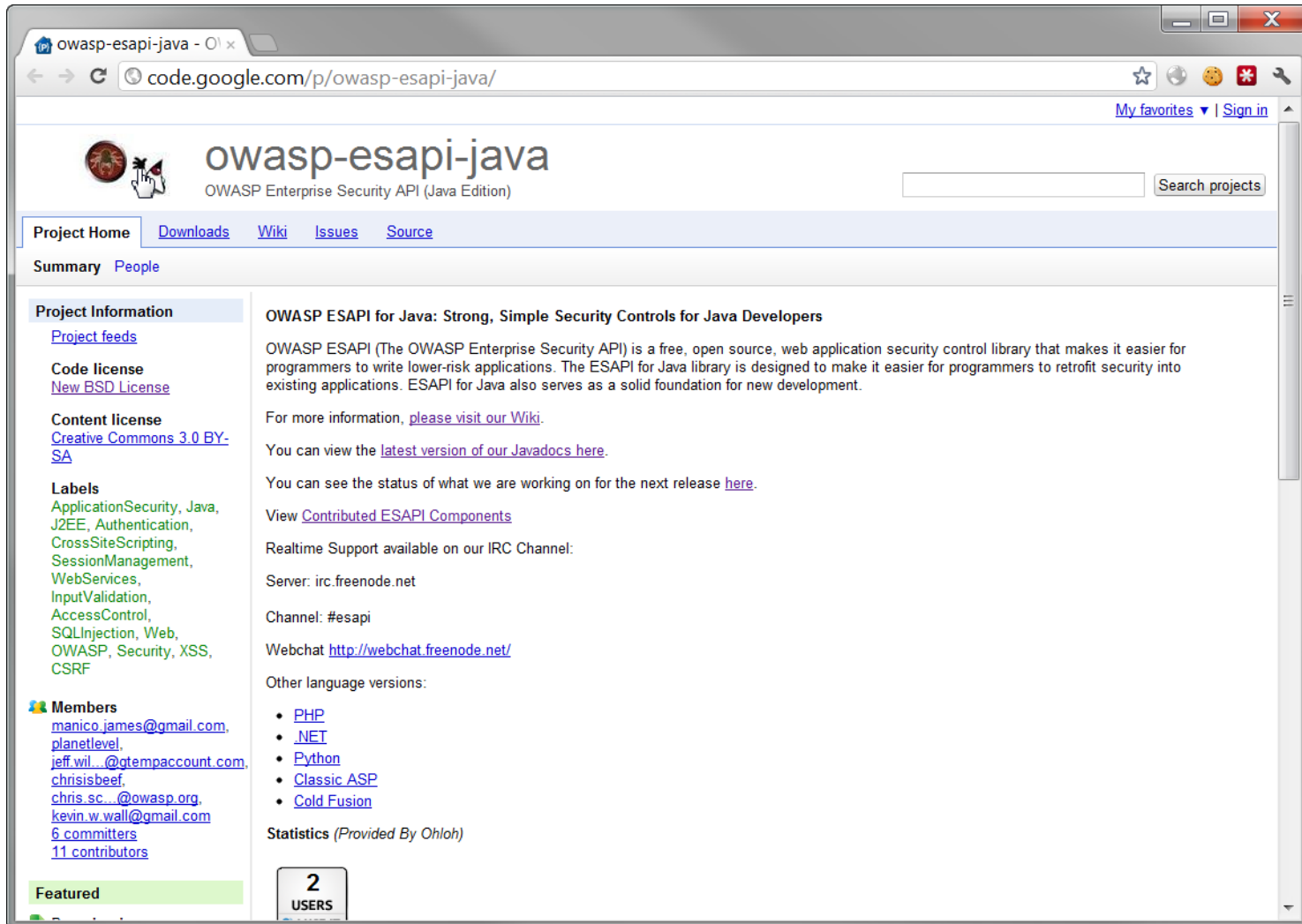
The following organizations are a few of the many organizations that are starting to adopt ESAPI to secure their web applications: American Express, Apache Foundation, Booz Allen Hamilton, Aspect Security, Foundstone(McAfee), The Hartford, Infinite Campus, Lockheed Martin, MITRE, U.S. Navy - SPAWAR, The World Bank, SANS Institute.

Please let us know how your organization is using OWASP ESAPI. Include your name, organization's name, and brief description of how you are using it. The project lead can be reached here. The project maintainer can be reached here.

Let's talk here Got developer cycles? Related resources

ESAPI Communities ESAPI Coding OWASP Cheat Sheet Series

Free and Open Source (OWASP)



The screenshot shows the project page for OWASP ESAPI Java on Code.google.com. The browser address bar shows the URL `code.google.com/p/owasp-esapi-java/`. The page header includes the project name "owasp-esapi-java" and the subtitle "OWASP Enterprise Security API (Java Edition)". Navigation tabs include "Project Home", "Downloads", "Wiki", "Issues", and "Source". The main content area is titled "Summary" and "People".

Project Information

- [Project feeds](#)
- Code license**
[New BSD License](#)
- Content license**
[Creative Commons 3.0 BY-SA](#)
- Labels**
ApplicationSecurity, Java, J2EE, Authentication, CrossSiteScripting, SessionManagement, WebServices, InputValidation, AccessControl, SQLInjection, Web, OWASP, Security, XSS, CSRF

Members

- manico.james@gmail.com
- [planetlevel](#)
- jeff.wil...@gtempaccount.com
- [chrisbeef](#)
- chris.sc...@owasp.org
- kevin.w.wall@gmail.com
- [6 committers](#)
- [11 contributors](#)

Featured

2 USERS

OWASP ESAPI for Java: Strong, Simple Security Controls for Java Developers

OWASP ESAPI (The OWASP Enterprise Security API) is a free, open source, web application security control library that makes it easier for programmers to write lower-risk applications. The ESAPI for Java library is designed to make it easier for programmers to retrofit security into existing applications. ESAPI for Java also serves as a solid foundation for new development.

For more information, [please visit our Wiki](#).

You can view the [latest version of our Javadocs here](#).

You can see the status of what we are working on for the next release [here](#).

View [Contributed ESAPI Components](#)

Realtime Support available on our IRC Channel:

Server: irc.freenode.net

Channel: #esapi

Webchat <http://webchat.freenode.net/>

Other language versions:

- [PHP](#)
- [.NET](#)
- [Python](#)
- [Classic ASP](#)
- [Cold Fusion](#)

Statistics (Provided By Ohloh)

Enhanced Small Arms Protective Insert

esapi - Google Search x

www.google.com/search?hl=en&safe=off&q=esapi&ix=seb&ion=1&bav=on.2,or.r_gc.r_pw.r_qf.,cf.osb&biw=

+You Search Images Maps YouTube News Gmail Documents Calendar More

Google esapi Sign in

Search About 19,300 results (0.09 seconds) Safe Search off

Everything
Images
Maps
Videos
News
Shopping
More

All results
By subject

Any size
Large
Medium
Icon
Larger than...
Exactly...

Any color
Full color
Black and white

U.S. HANDLE WITH CARE

U.S. HANDLE WITH CARE

LARGE STRIKE FACE HANDLE WITH CARE

MEDIUM STRIKE FACE HANDLE WITH CARE

OWASP Top Ten Coverage

OWASP Top Ten	OWASP ESAPI
A1 Cross Site Scripting (XSS)	Validated Request
A2 Broken Access Control	Sanitize
A3 Session Fixation	HTTP Strict Transport Security
A4 Security Misconfigurations	Secure Headers
A5 Cross Site Request Forgery (CSRF)	Secure Cookies
A6 Cryptographic Weaknesses	Secure Randomness
A7 Denial of Service (DoS)	Secure File Upload
A8 Broken Authentication	Secure File Download
A9 Out of Band Authentication	Secure File Access
A10 Unvalidated Redirects and Forwards	Secure File Execution

Enterprise Security API

Existing Security Services/Libraries

ASPECT SECURITY Application Security Experts

Armor for your apps



Custom Enterprise Web Application

OWASP Enterprise Security API

Authenticator

User

AccessController

AccessReferenceMap

Validator

Encoder

HTTPUtilities

Encryptor

EncryptedProperties

Randomizer

Exception Handling

Logger

IntrusionDetector

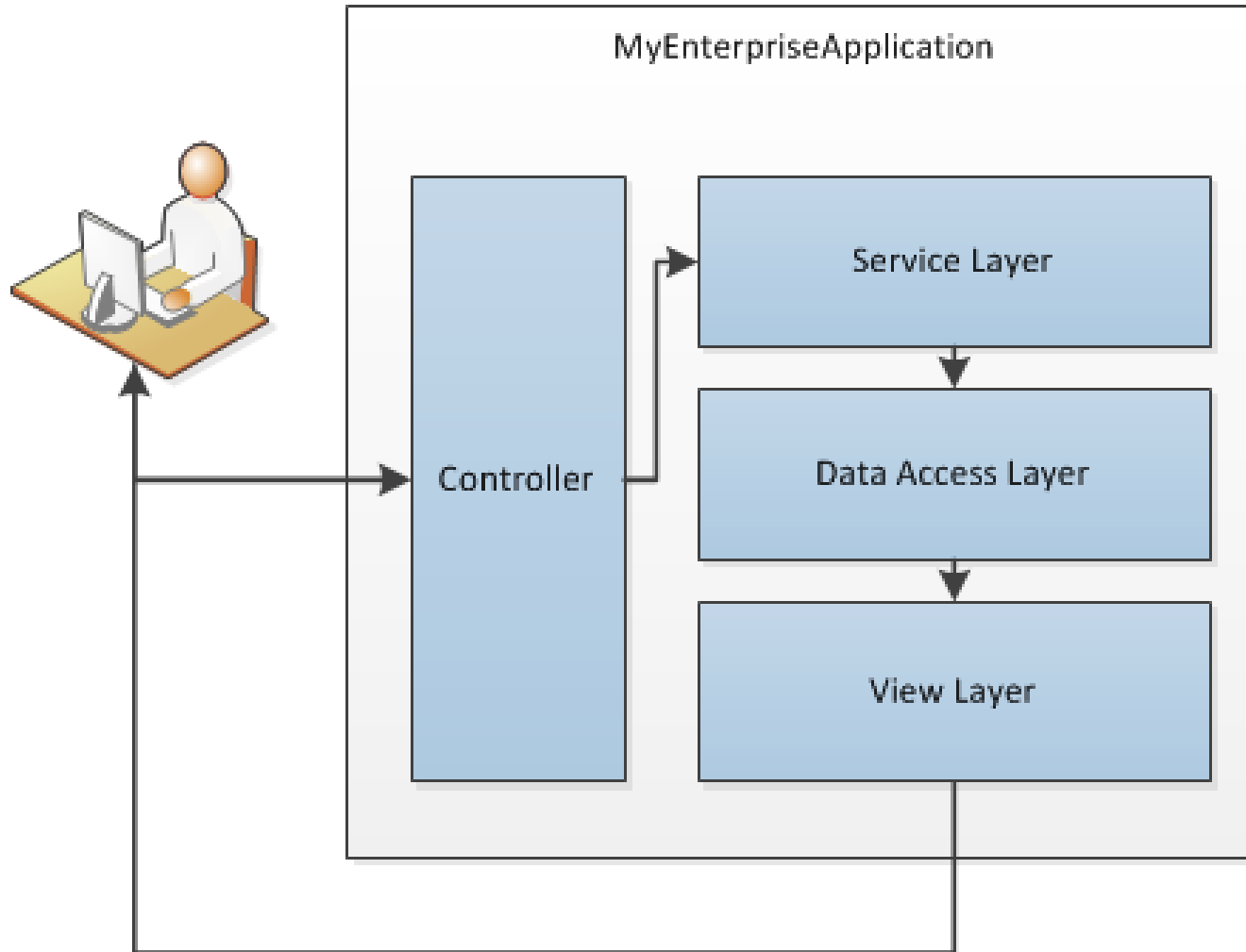
SecurityConfiguration

Your Existing Enterprise Services or Libraries

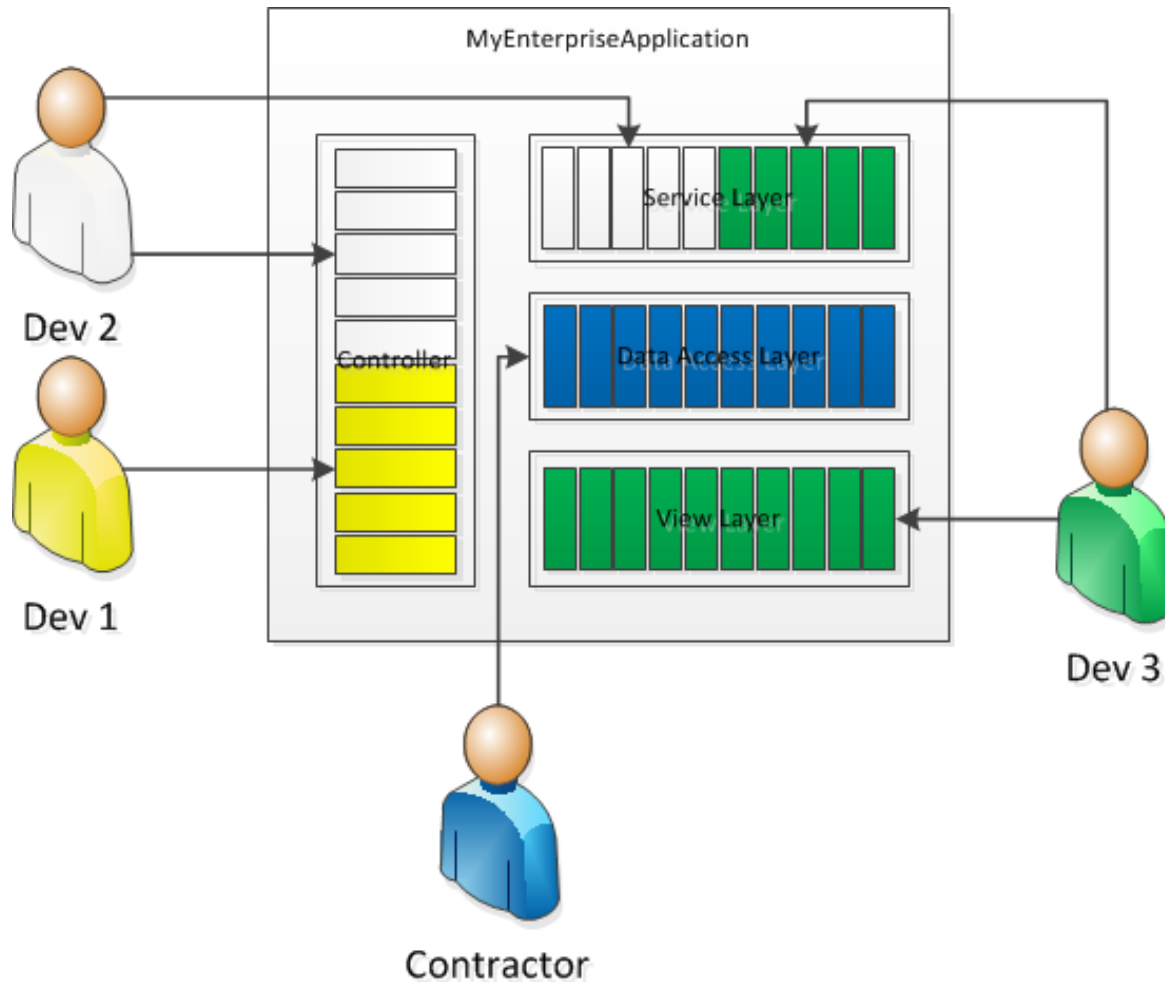
ESAPI Pattern Across Languages

- Security Control Interfaces
- Reference Implementations
- Customizable

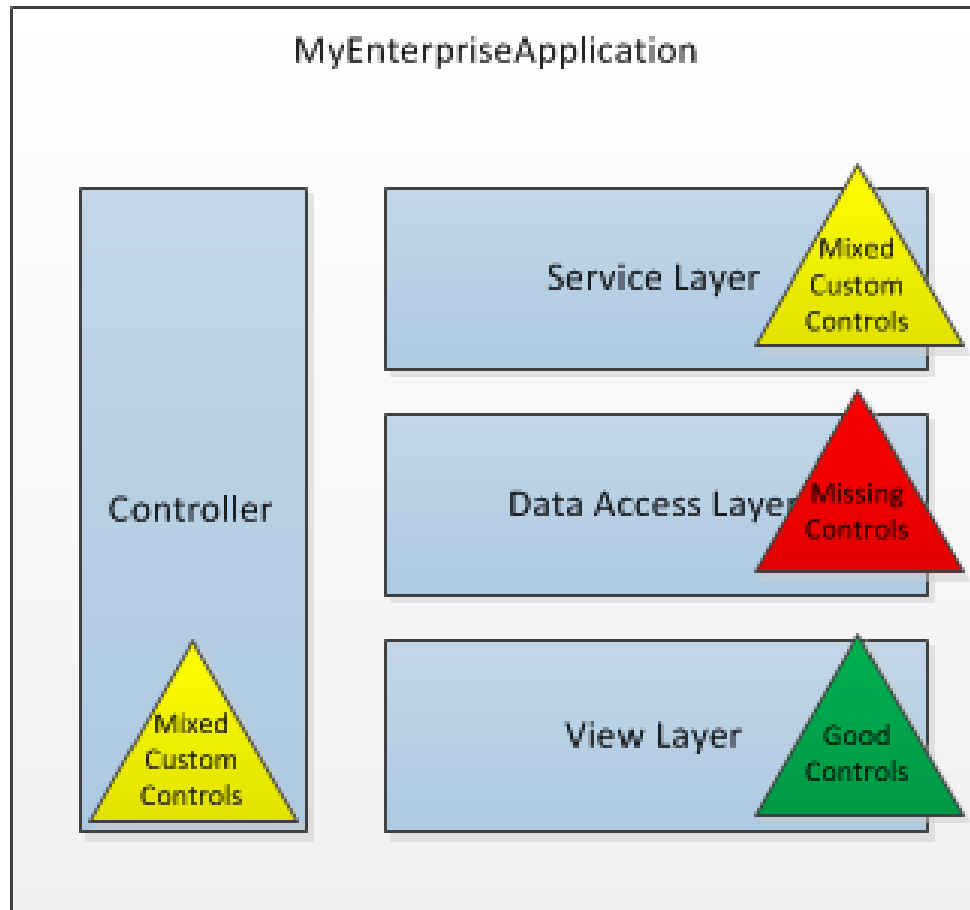
Why Centralized Controls are Important?



Too many cooks in the kitchen!



No Central Controls

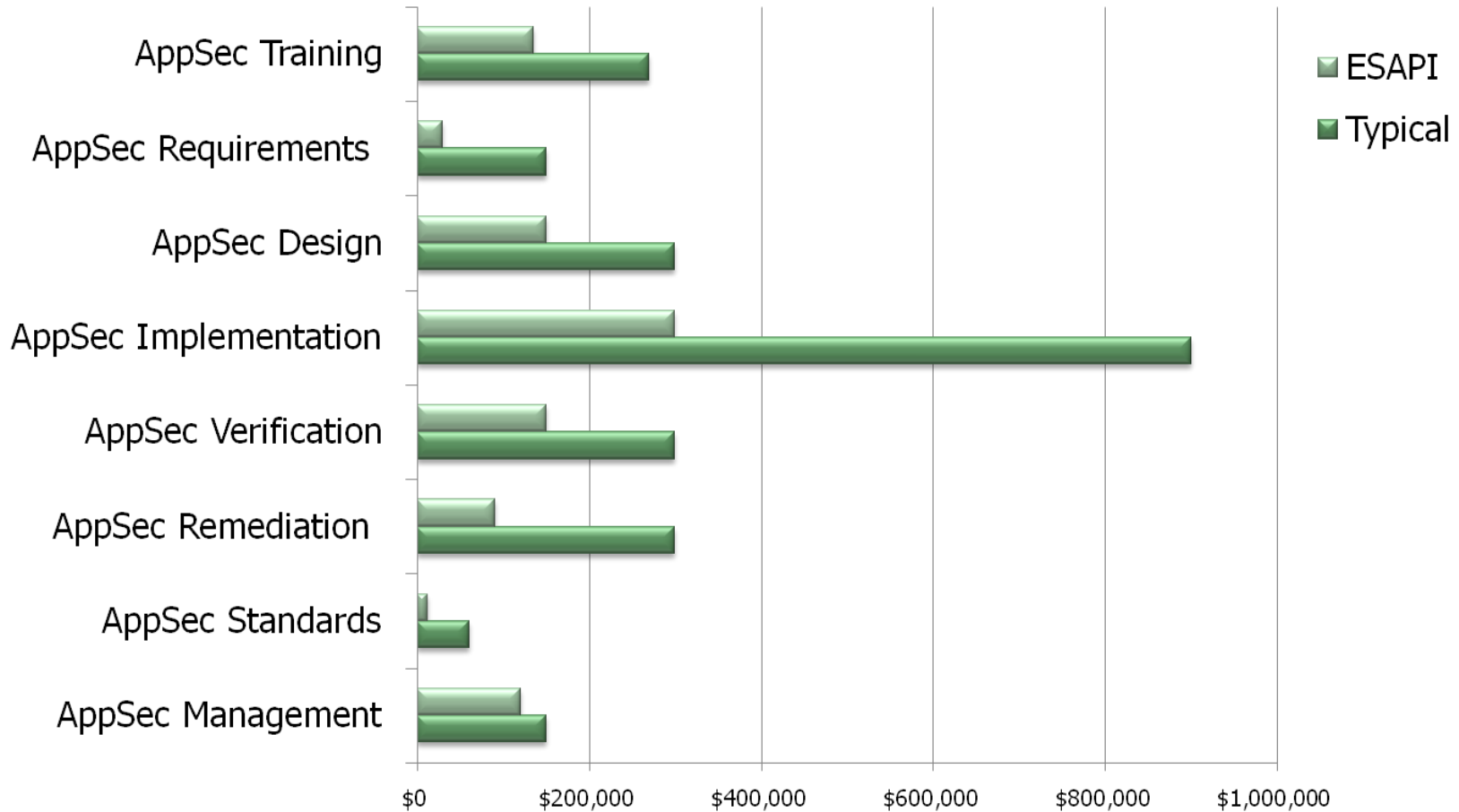


Develop Lower Risk Applications



Vulnerabilities and Security Controls

Potential ESAPI Cost Savings



ESAPI Language Availability

- Java EE
- Dot NET
- ASP
- PHP
- ColdFusion
- Python
- JavaScript
- Objective C
- Force.com
- Ruby
- C
- C++
- Perl

Feature Set vs. Programming Language



	Java	Microsoft .NET	php	ASP.NET	python	JavaScript	C++
Authentication	2.0	1.4			1.4	1.4	2.0 planned
Identity	2.0	1.4			1.4	1.4	2.0 planned
Access Control	2.0	1.4	1.4		1.4	1.4	2.0 planned
Input Validation	2.0	1.4	1.4	1.4	1.4	1.4	2.0
Output Escaping	2.0	1.4		1.4	1.4	1.4	2.0
Canonicalization	2.0	1.4		1.4	1.4	1.4	2.0
Encryption	2.0	1.4	1.4		1.4	1.4	2.0
Random Numbers	2.0	1.4	1.4		1.4	1.4	2.0
Exception Handling	2.0	1.4	1.4	1.4	1.4	1.4	2.0
Logging	2.0	1.4	1.4	1.4	1.4	1.4	2.0
Intrusion Detection	2.0	1.4			1.4	1.4	
Security Configuration	2.0	1.4	1.4	1.4	1.4	1.4	2.0
WAF	2.0						



WHY ESAPI FOR C++?

Reasoning

- Sponsored by Government
- Currently ESAPI for C
- C++ is still popular and used in critical applications

Almost 40k C++ Projects on Sourceforge

The screenshot shows the Sourceforge search interface. At the top, there is a search bar with the text "Search" and an "Advanced" link with a gear icon. Below the search bar, the text "Refine your search" is followed by several filter categories: "Translations", "License", "Programming Language", "Status", "OS", and "Freshness". The "Programming Language" dropdown menu is open, showing a list of languages with their respective project counts: Java (49,269), C++ (39,714), PHP (31,859), C (29,942), Python (14,812), C# (14,625), JavaScript (12,266), Perl (9,654), Unix Shell (4,208), Delphi/Kylix (3,750), Visual Basic (3,305), Visual Basic .NET (3,156), Assembly (2,557), JSP (2,085), and Ruby (1,945). A mouse cursor is pointing at the C++ entry. To the left of the dropdown menu is a "Top Apps" sidebar with categories like "Audio & Video", "Business & Enterprise", "Communications", "Development", "Home & Education", "Games", "Graphics", "Science & Engineering", "Security & Utilities", and "System Administration". To the right of the dropdown menu, there is a "Sort By:" dropdown set to "Most Popular". Below the dropdown menu, there is a preview of a project titled "npppluginmgr" with a description: "Hosting Project for Notepad++ Plugin Manager" and "2,761,955 weekly downloads". The preview also shows a "Download Now" button and a "83.0% RECOMMENDED" badge.

<http://sourceforge.net/directory/>

Over 6k C++ Jobs on Dice

The screenshot shows a web browser window displaying the Dice.com job search results for C++ jobs. The browser's address bar shows the URL: `seeker.dice.com/jobsearch/servlet/JobSearch?op=300&N=0&Hf=0&NUM_PER_PAGE=30&Ntk=JobSearchRan`. The Dice logo is visible in the top left, with the tagline "The career hub for tech". The search results show 1 - 30 of 6273 results. The current search is for "C++". The results table lists several job titles, including "Senior Software Engineer. C / C++, VoIP", "Senior Software Engineer. C or C++, TCP/IP", and "Senior C++ Software Developer". The table columns are Job Title, Company, Location, Date Posted, and View. The View column includes links for Summary and Detail. The page also features a sidebar with "Current Search" and "Refine Results" options, and a "Dice Talent Communities" button at the bottom right.

education connection Your source for accredited online schools.

- ▶ Healthcare
- ▶ Medical Billing
- ▶ Video Game Design
- ▶ Criminal Justice
- ▶ Human Services
- ▶ Computer Science
- ▶ Business
- ▶ Technology
- ▶ Teaching
- ▶ Legal/Paralegal
- ▶ Engineering
- ▶ And More...

Search job title only (e.g. Senior Java Developer) [Advanced Job Search](#)

Search results: 1 - 30 of 6273 [Get new jobs for this search by email](#)

Current Search

Keyword
[Undo](#) C++

Jobs posted within:
 days ago

Refine Results

- + Area Code
- + Country
- + Company
- + Skill
- + City

Results viewable: per page [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [Next](#)

Job Title	Company	Location	Date Posted	View
Senior Software Engineer. C / C++, VoIP	Brains Workgroup, Inc.	Teaneck, NJ	Feb-16-2012	<input checked="" type="radio"/> Summary Detail
Senior Software Engineer. C or C++, TCP/IP	Brains Workgroup, Inc.	Teaneck, NJ	Feb-16-2012	
Senior C++ Software Developer	Brains Workgroup, Inc.	Teaneck, NJ	Feb-16-2012	
Software Engineer - C++	Idea Connectors Inc	San Mateo, CA	Mar-02-2012	

Search By
Company
Metro Area

My Dice
[Create/Edit Profile](#)
[See Saved Jobs](#)
[Upload Your Resume](#)

Dice Talent Communities

Retro-fit Existing Applications

■ Critical Utilities / Systems

- ▶ Telecom
- ▶ Defense
- ▶ Banking / Trading

■ Enterprise Apps

- ▶ Point of Sale
- ▶ Employee Interfaces
- ▶ Airline applications

■ Terminal Systems

■ ???

New Applications

- MMO Games
- Critical Utilities / Systems
- Embedded Applications
- Server Applications
- ???

ESAPI C++ Controls

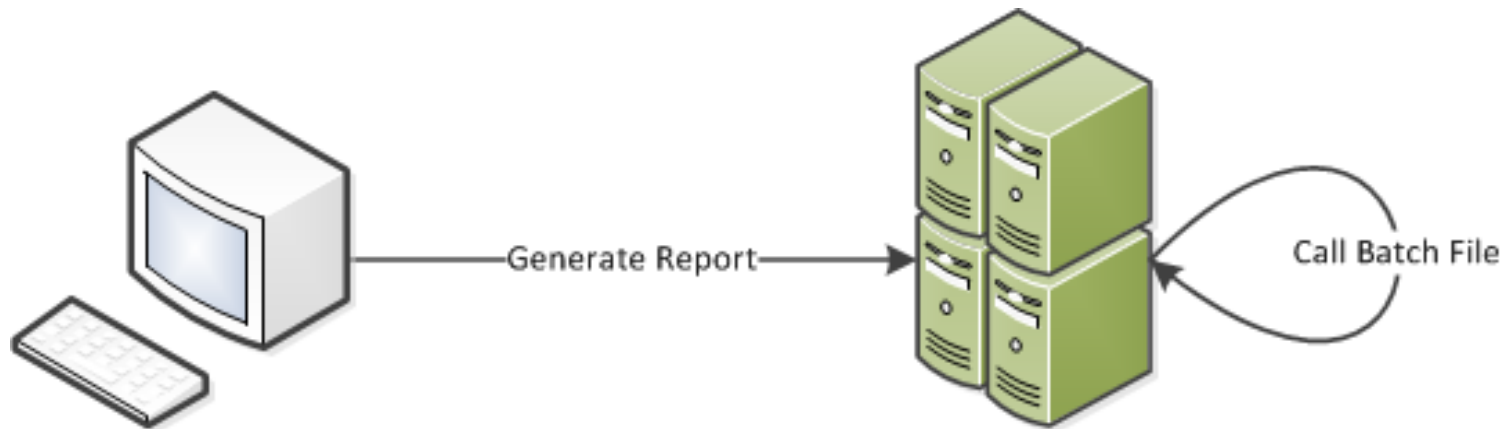
- Authentication
- User
- Access Control
- Validation
- Encoding
- Execution
- Encryption
- Logging



Example ESAPI Integration

DEMO

Example Workflow





Design Choices, Controls, Dependencies

ARCHITECTURE

Design Approach

- Based off Java design
- Removed Web Specifics
- Reached out to the community

ESAPI C++ Controls

Custom Enterprise Application

OWASP Enterprise Security API for C++

Authenticator

User

AccessController

AccessReferenceMap

Validator

Encoder

HTTPUtilities

Encryptor

EncryptedProperties

Randomizer

Exception Handling

Logger

IntrusionDetector

SecurityConfiguration

Your Existing Enterprise Services or Libraries

ESAPI C++ Controls

- Authentication
- User
- Access Control
- Validation
- Encoding
- Execution
- Encryption
- Logging

General Requirements

- Cross-Platform
- Light weight
- Easy to setup and use
- Thread / Memory safe
- Not a memory management solution

Cross-Platform Testing

- Windows / Unix
- Compilers
 - ▶ Visual Studio 2008 / 2010
 - ▶ GCC
 - ▶ Intel ICC
- Unit testing

Light weight

■ Few Dependencies

- ▶ Boost
- ▶ Crypto++

Easy to setup and use

- Documentation
- Few dependencies
- Require as little as possible from the developer

Thread / Memory Safe

- Locking
- Minimal use of pointers
- Code review
- Assertions (nullptr/0/null?)
- SafeInt class written by David LeBlanc
 - ▶ <http://safeint.codeplex.com/>

Memory Management

- Not a memory management solution

- Consistent with Java Implementation
- Requirement - Not broken
 - ▶ Jeff Walton
 - ▶ Kevin Wall (Fixed ESAPI Java crypto)
- Wei Dai's Crypto++
 - ▶ <http://www.cryptopp.com/>

Current Project State

- Not production ready
 - ▶ Some unfinished components and issues
 - Unicode
 - Reference Implementations
- Need contributors and testers

How to get involved (C++)

- <http://www.google.com/search?q=esapi+c%2B%2B>
- Google Code
 - ▶ <http://code.google.com/p/owasp-esapi-cplusplus/>
- OWASP
 - ▶ https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API
- Mailing List
 - ▶ <https://lists.owasp.org/mailman/listinfo/owasp-esapi-c++>
 - ▶ owasp-esapi-c++@lists.owasp.org

How to get involved (C)

■ Google Code

- ▶ <http://code.google.com/p/owasp-esapi-c/>

■ OWASP

- ▶ [https://www.owasp.org/index.php/Category:OWASP Enterprise Security API](https://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API)

■ Mailing List

- ▶ <https://lists.owasp.org/mailman/listinfo/owasp-esapi-c>
- ▶ owasp-esapi-c@lists.owasp.org

ESAPI Project Future

- ESAPI Community
- Pluggable Architecture
 - ▶ Just get what you need
- Lots of Documentation!
 - ▶ Cheat Sheets / Guides
 - ▶ Videos



Dan.Amodio@AspectSecurity.com

QUESTIONS?