OWASP Enterprise Security API (ESAPI) for C Plus Plus

Dan Amodio
ESAPI for C Project Leader
Dan.Amodio@owasp.org
Dan.Amodio@aspectsecurity.com

ASPECT SECURITY
Application Security Experts

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?

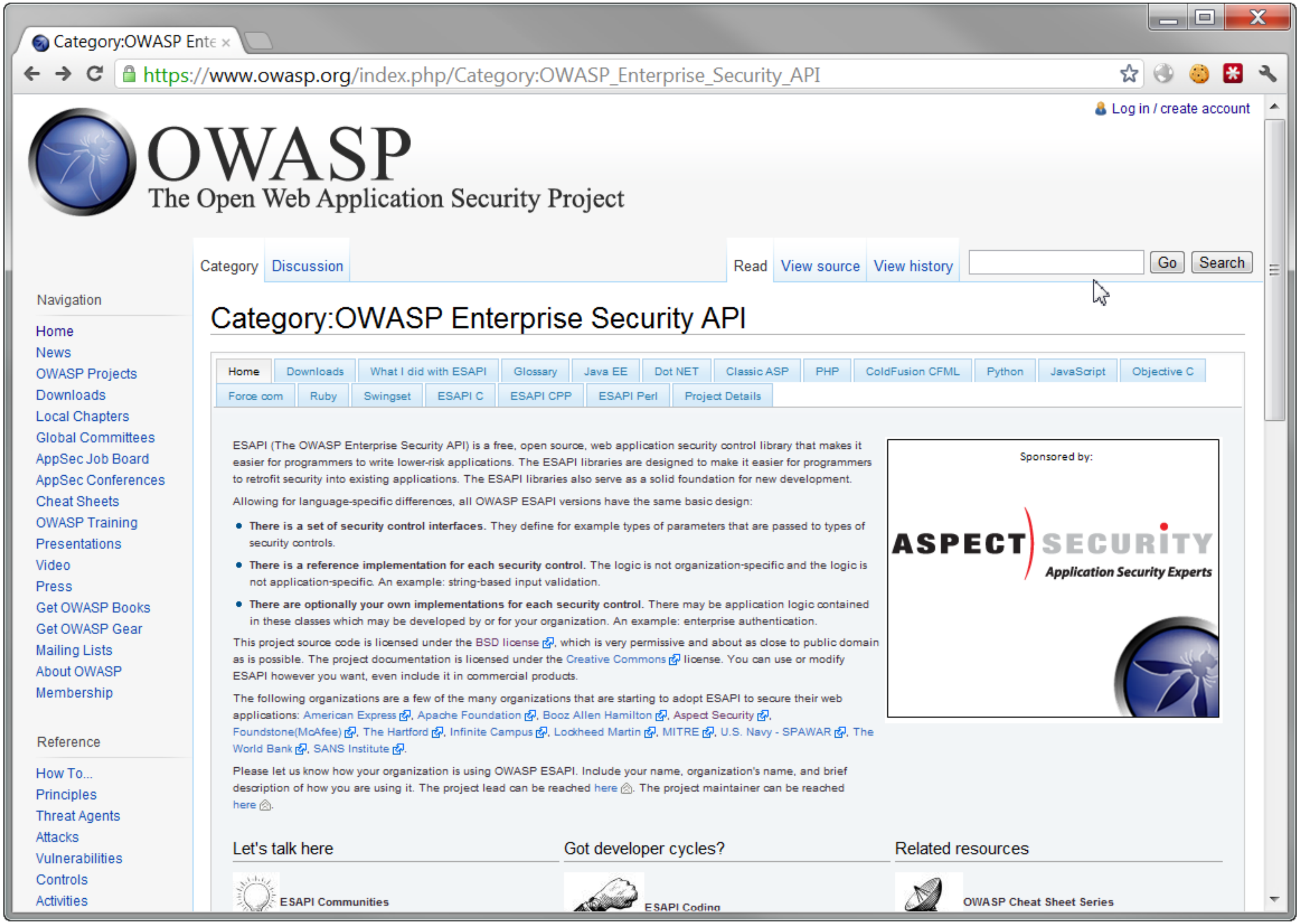
- Developers
- Managers
- Security Professionals

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)



Category:OWASP Enterprise Security API

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:

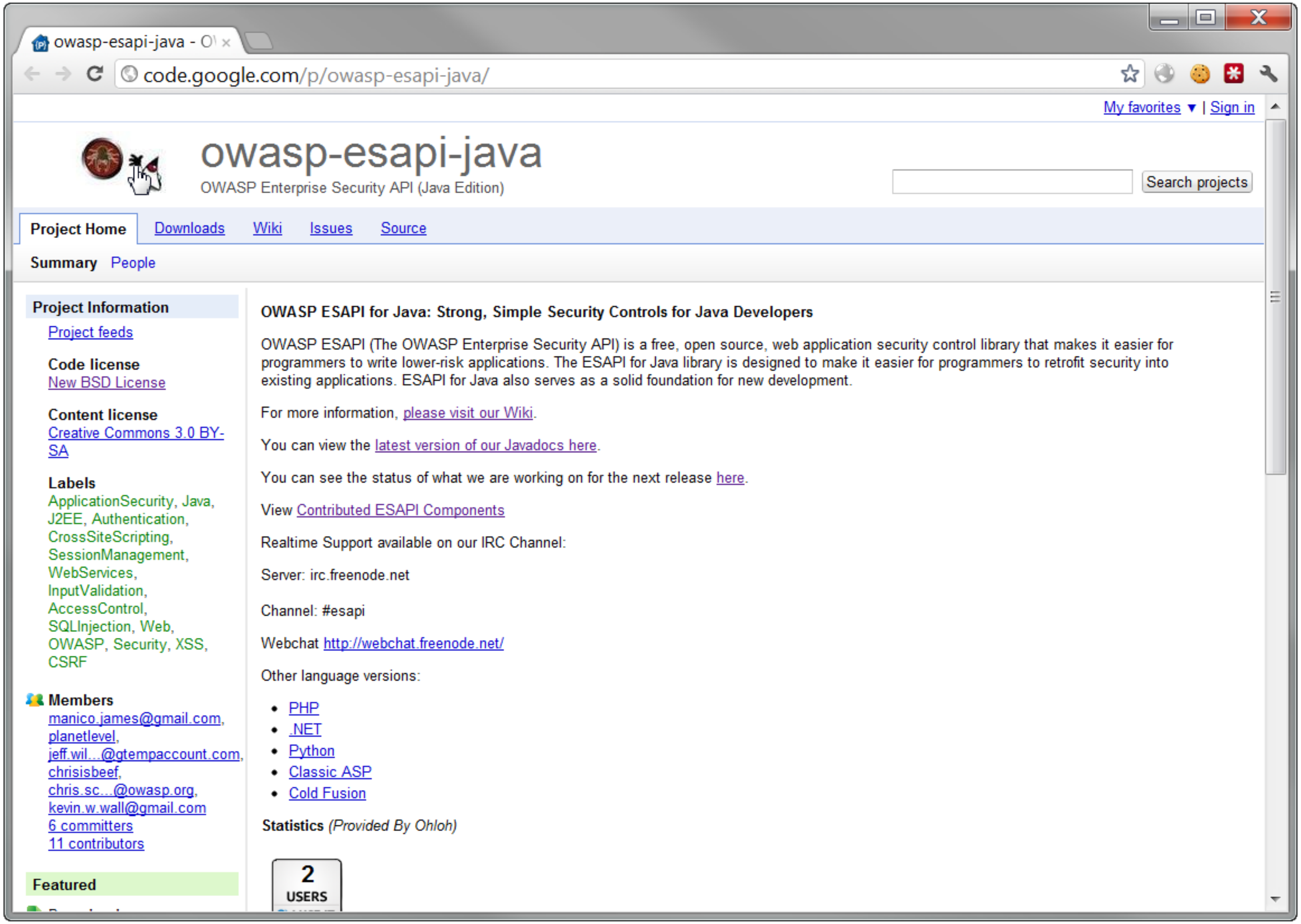
- **There is a set of security control interfaces.** They define for example types of parameters that are passed to types of security controls.
- **There is a reference implementation for each security control.** The logic is not organization-specific and the logic is not application-specific. An example: 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.

Free and Open Source (OWASP)



owasp-esapi-java

OWASP Enterprise Security API (Java Edition)

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, chrisisbeef, chris.sc...@owasp.org, kevin.w.wall@gmail.com
6 committers
11 contributors

Featured

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/

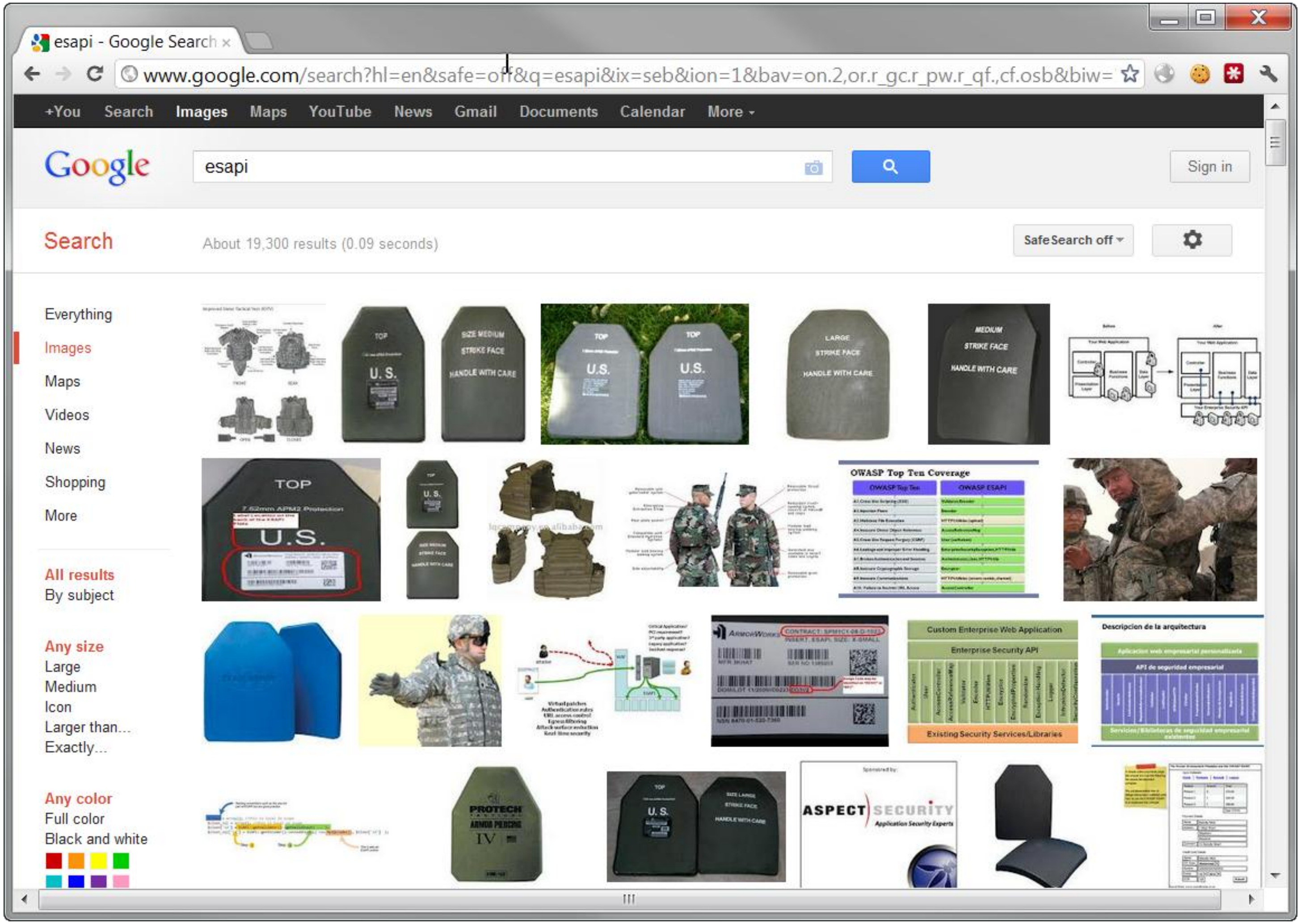
Other language versions:

- PHP
- .NET
- Python
- Classic ASP
- Cold Fusion

Statistics *(Provided By Ohloh)*

2
USERS

Enhanced Small Arms Protective Insert



esapi - Google Search

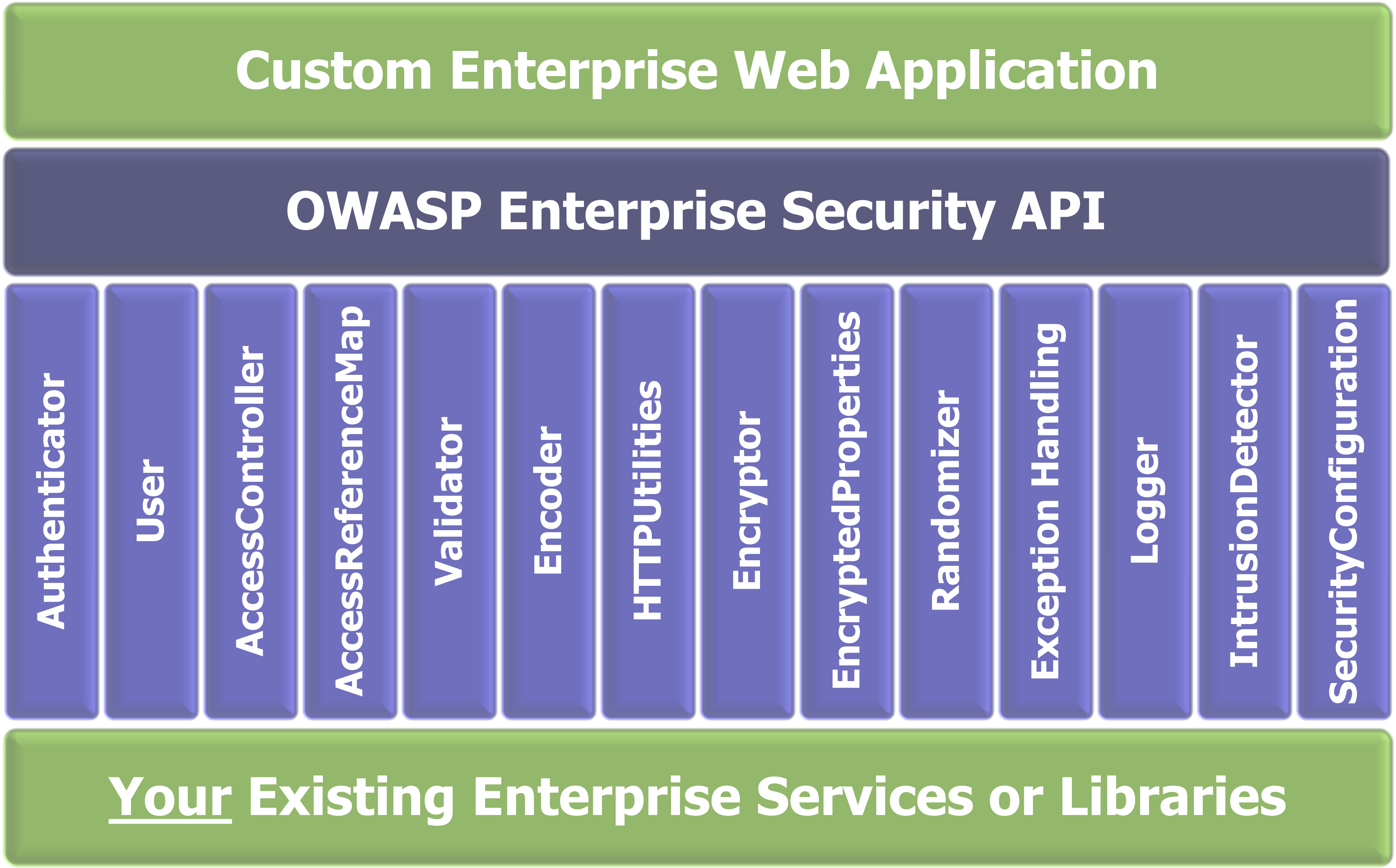
www.google.com/search?hl=en&safe=off&q=esapi&ix=seb&ion=1&bav=on.2,or.r_gc.r_pw.r_qf.,cf.osb&biw=

esapi

About 19,300 results (0.09 seconds)

SafeSearch off

Armor for your apps



Custom Enterprise Web Application

OWASP Enterprise Security API

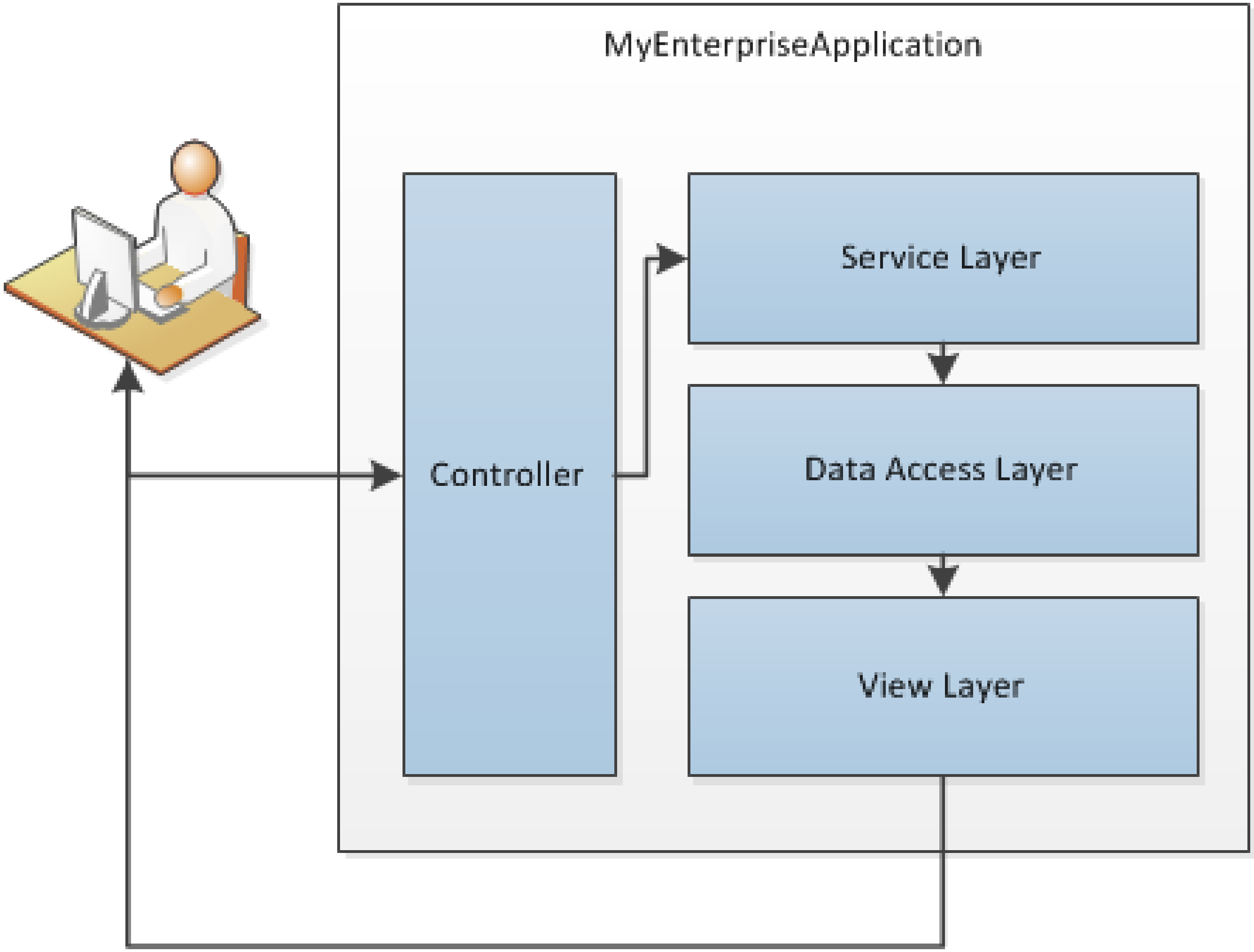
- Authenticator
- User
- AccessController
- AccessReferenceMap
- Validator
- Encoder
- HTTPUtilities
- Encryptor
- EncryptedProperties
- Randomizer
- Exception Handling
- Logger
- IntrusionDetector
- SecurityConfiguration

Your Existing Enterprise Services or Libraries

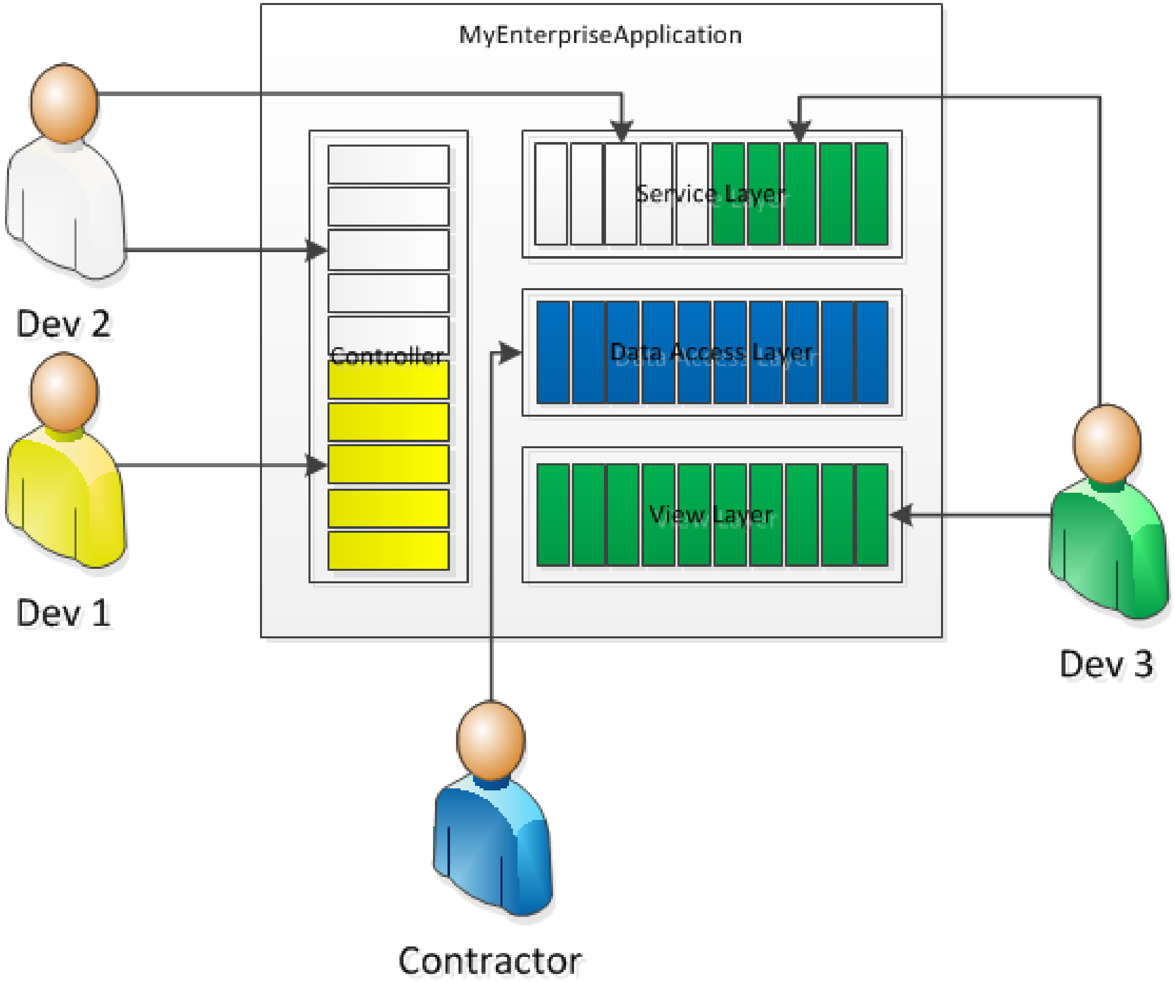
ESAPI Pattern Across Languages

- Security Control Interfaces
- Reference Implementations
- Customizable

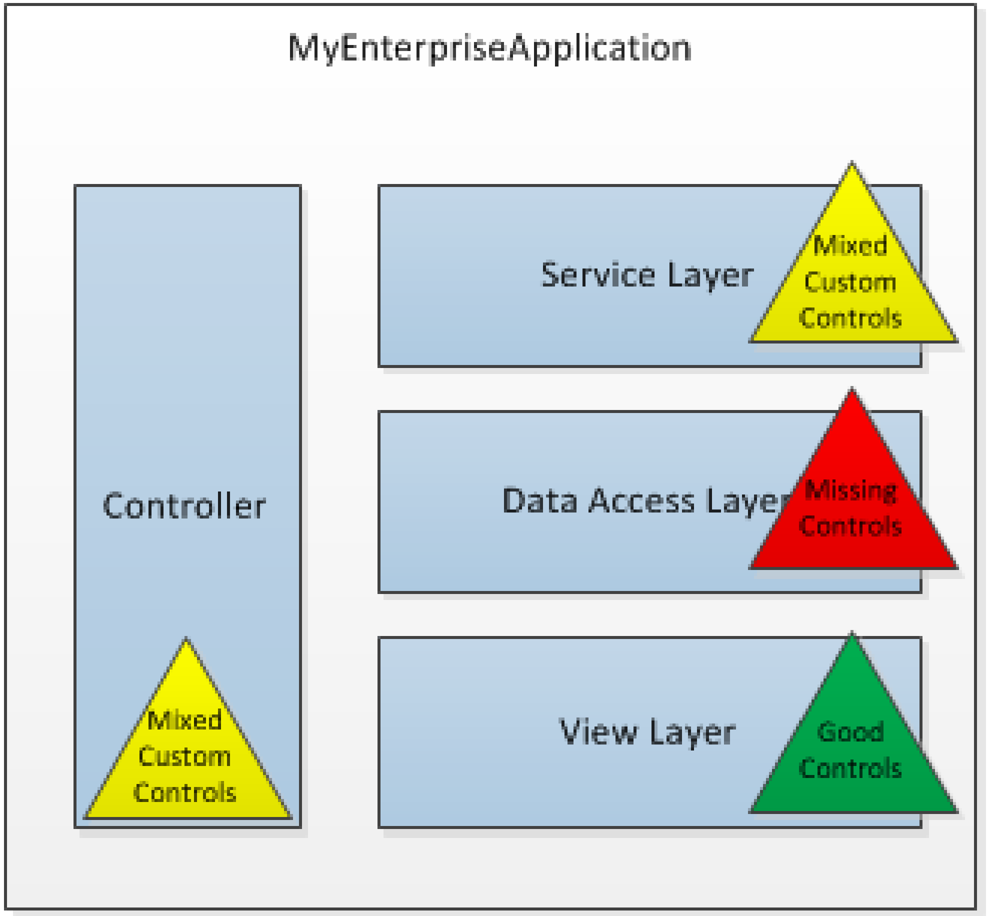
Why Centralized Controls are Important?



Too many cooks in the kitchen!



No Central Controls



MyEnterpriseApplication

Controller

Mixed Custom Controls

Service Layer

Mixed Custom Controls

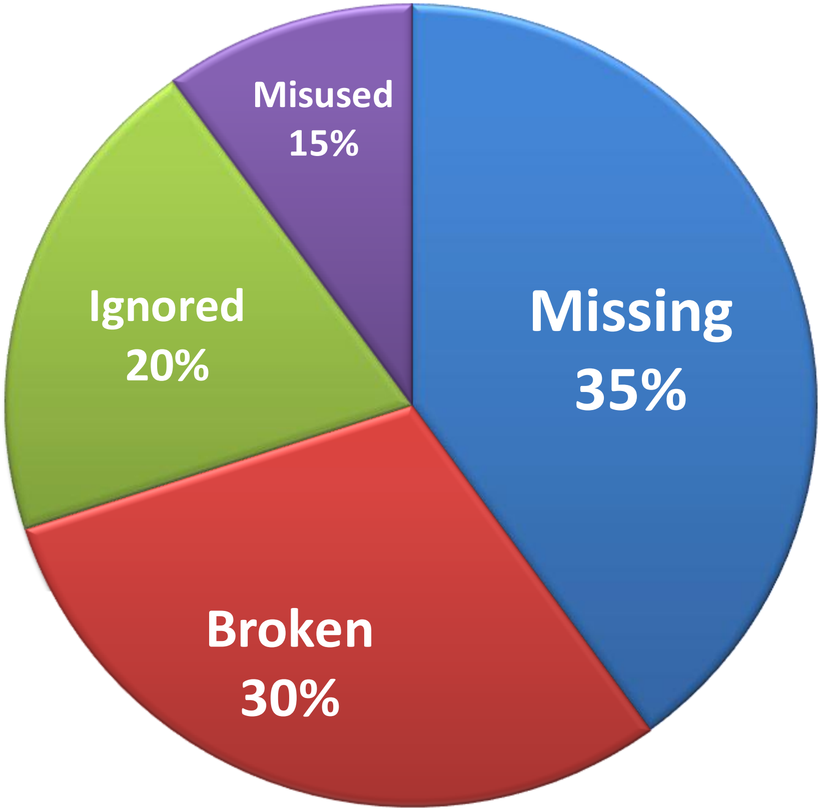
Data Access Layer

Missing Controls

View Layer

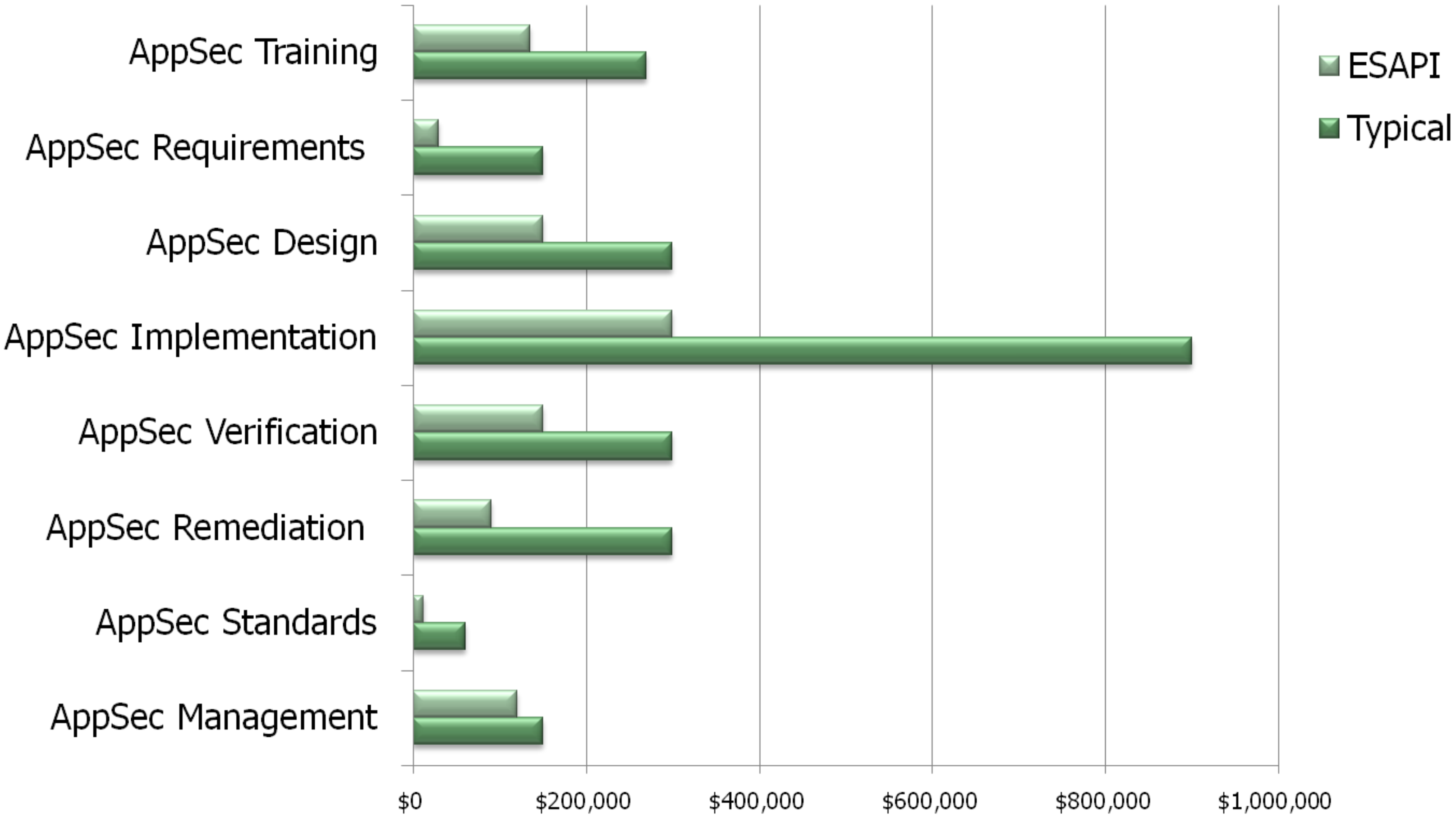
Good Controls

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

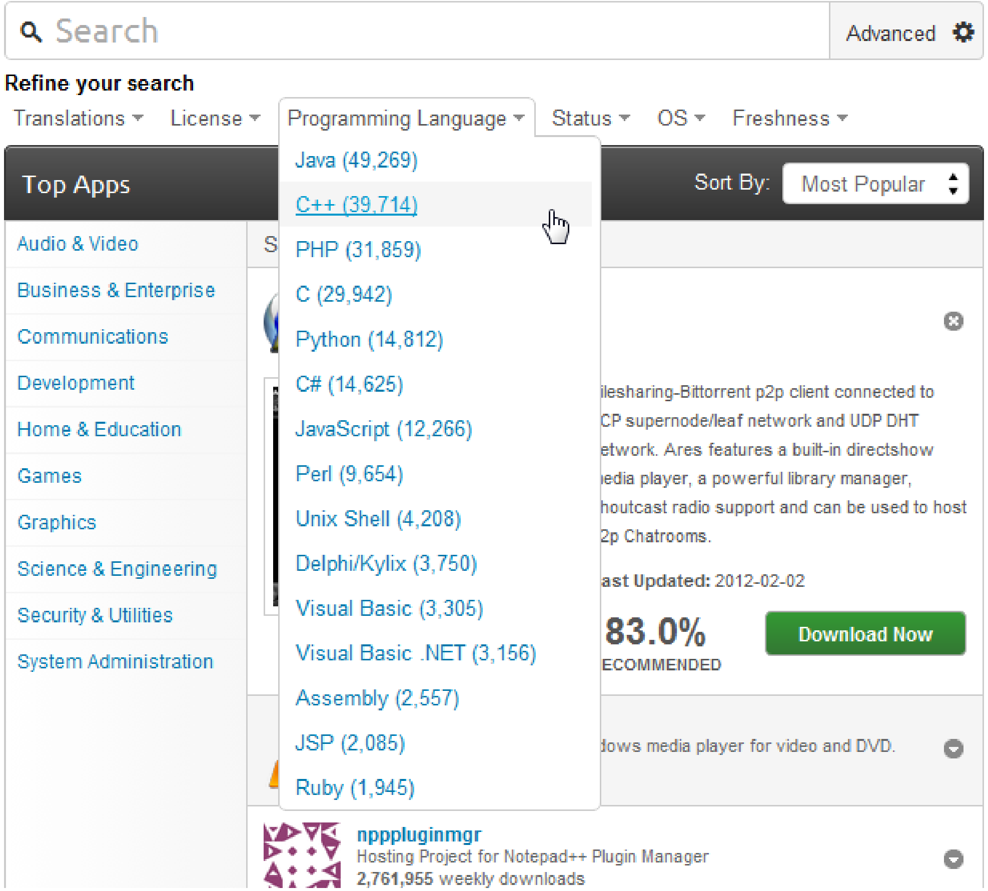
	Java	Microsoft .NET	php	cf	Microsoft ASP.	python	JavaScript	C++
Authentication	2.0	1.4			1.4	1.4		2.0 planned
Identity	2.0	1.4			1.4	1.4		2.0 planned
Access Control	2.0	1.4	1.4		1.4	1.4		2.0 planned
Input Validation	2.0	1.4	1.4	1.4	1.4	1.4	2.0	2.0
Output Escaping	2.0	1.4		1.4	1.4	1.4	2.0	2.0
Canonicalization	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	2.0
Logging	2.0	1.4	1,4	1.4	1.4	1.4	2.0	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	TBD
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



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)
Ruby (1,945)

Audio & Video
Business & Enterprise
Communications
Development
Home & Education
Games
Graphics
Science & Engineering
Security & Utilities
System Administration

ilesharing-Bittorrent p2p client connected to CP supernode/leaf network and UDP DHT etwork. Ares features a built-in directshow iedia player, a powerful library manager, houtcast radio support and can be used to host 2p Chatrooms.

ast Updated: 2012-02-02

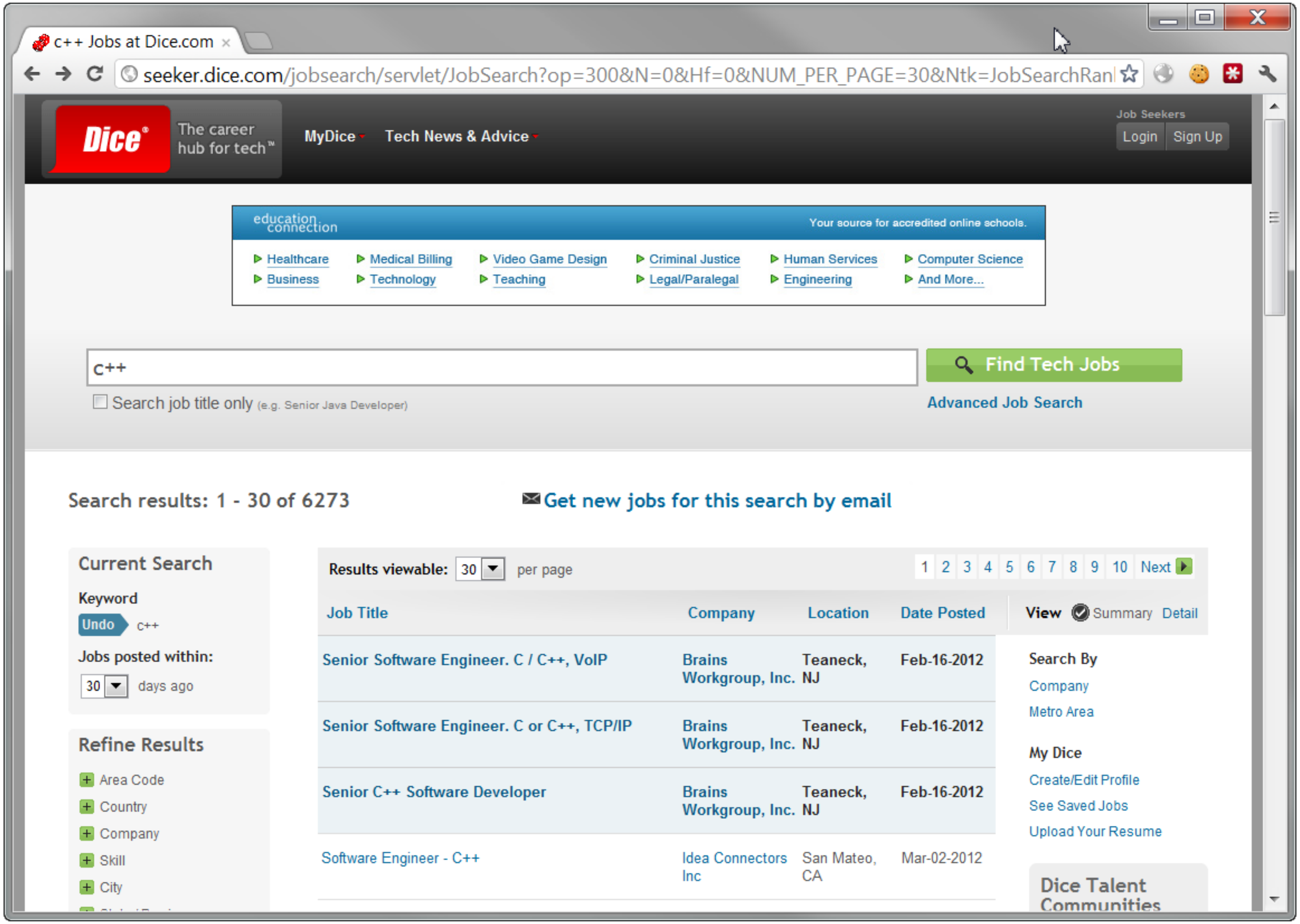
83.0%
ECOMMENDED

dows media player for video and DVD.

nppluginmgr
Hosting Project for Notepad++ Plugin Manager
2,761,955 weekly downloads

http://sourceforge.net/directory/

Over 6k C++ Jobs on Dice



c++ Jobs at Dice.com ×

seeker.dice.com/jobsearch/servlet/JobSearch?op=300&N=0&Hf=0&NUM_PER_PAGE=30&Ntk=JobSearchRan

Dice® The career hub for tech™

MyDice Tech News & Advice

Job Seekers

Login Sign Up

education connection — Your source for accredited online schools.

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

c++

Find Tech Jobs

□ 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:

30 days ago

Refine Results

- Area Code
- Country
- Company
- Skill
- City

Results viewable: 30 per page

1 2 3 4 5 6 7 8 9 10 Next

View ● Summary Detail

Job Title	Company	Location	Date Posted
Senior Software Engineer. C / C++, VoIP	Brains Workgroup, Inc.	Teaneck, NJ	Feb-16-2012
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
- ???

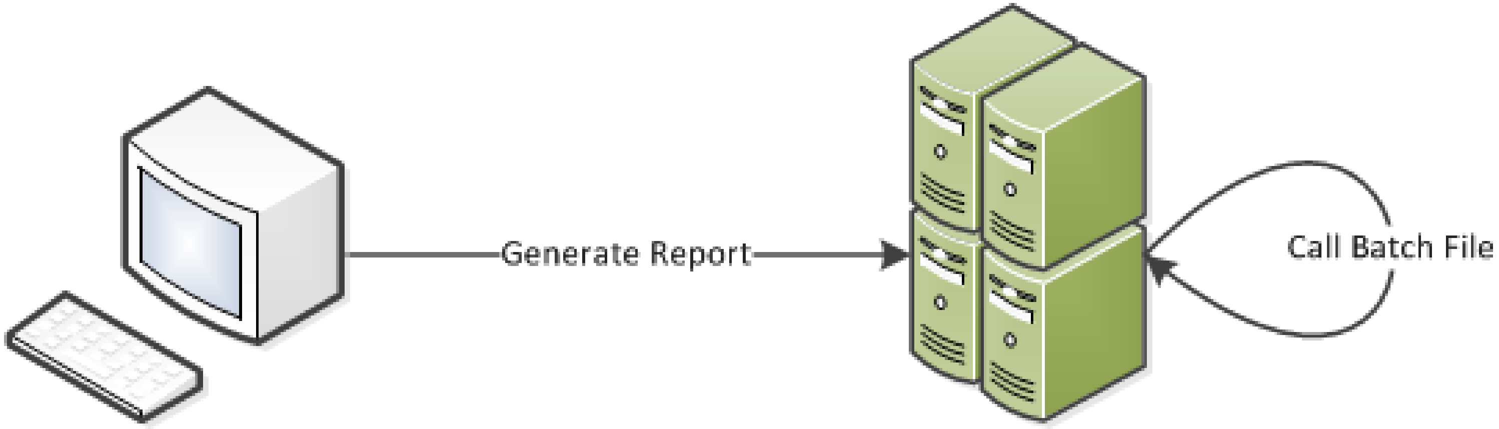
ESAPI C++ Controls

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

Example ESAPI Integration

DEMO

Example Workflow



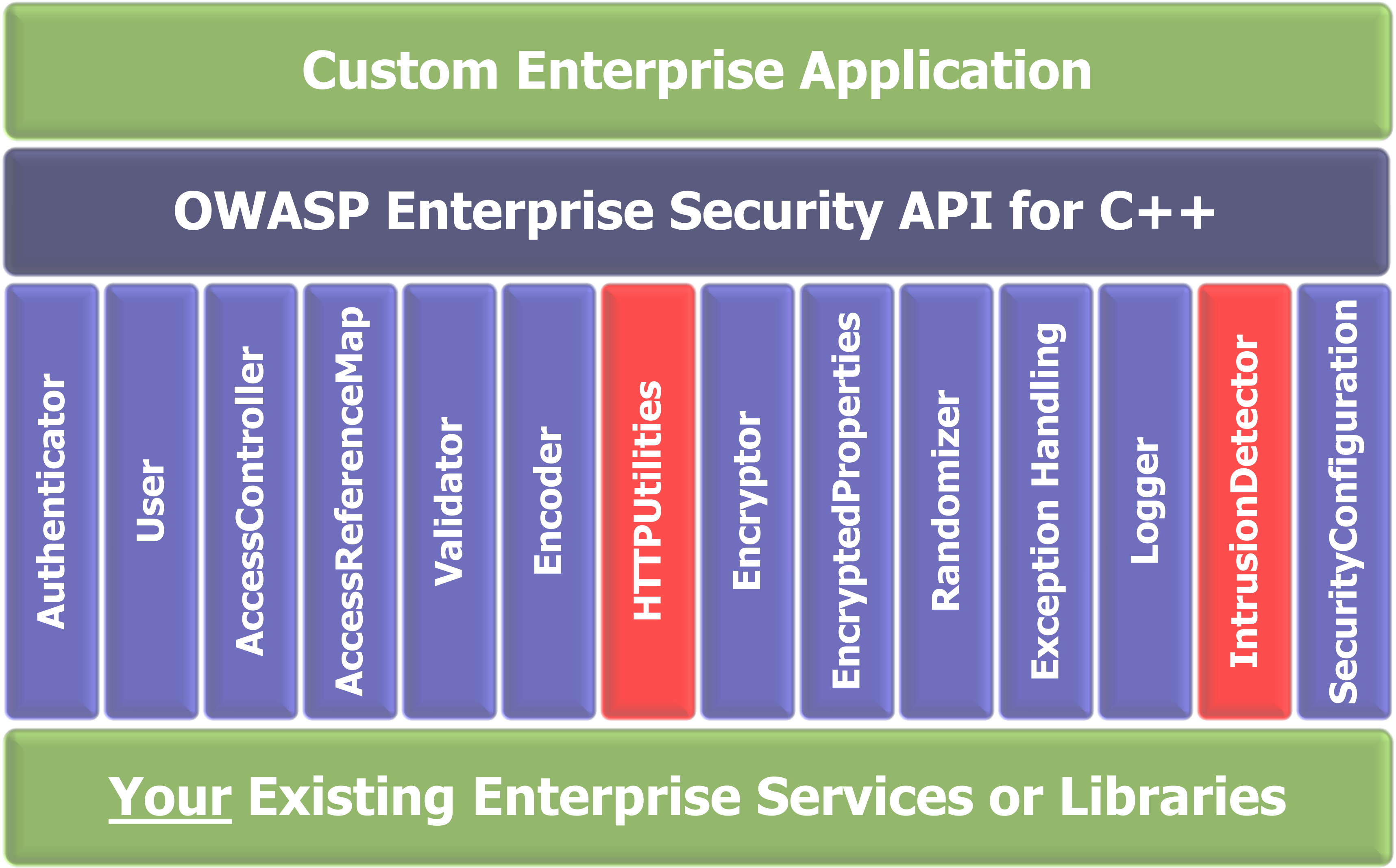
Design Choices, Controls, Dependencies

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

<u>Your</u> 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

Crypto

- 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
- 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?