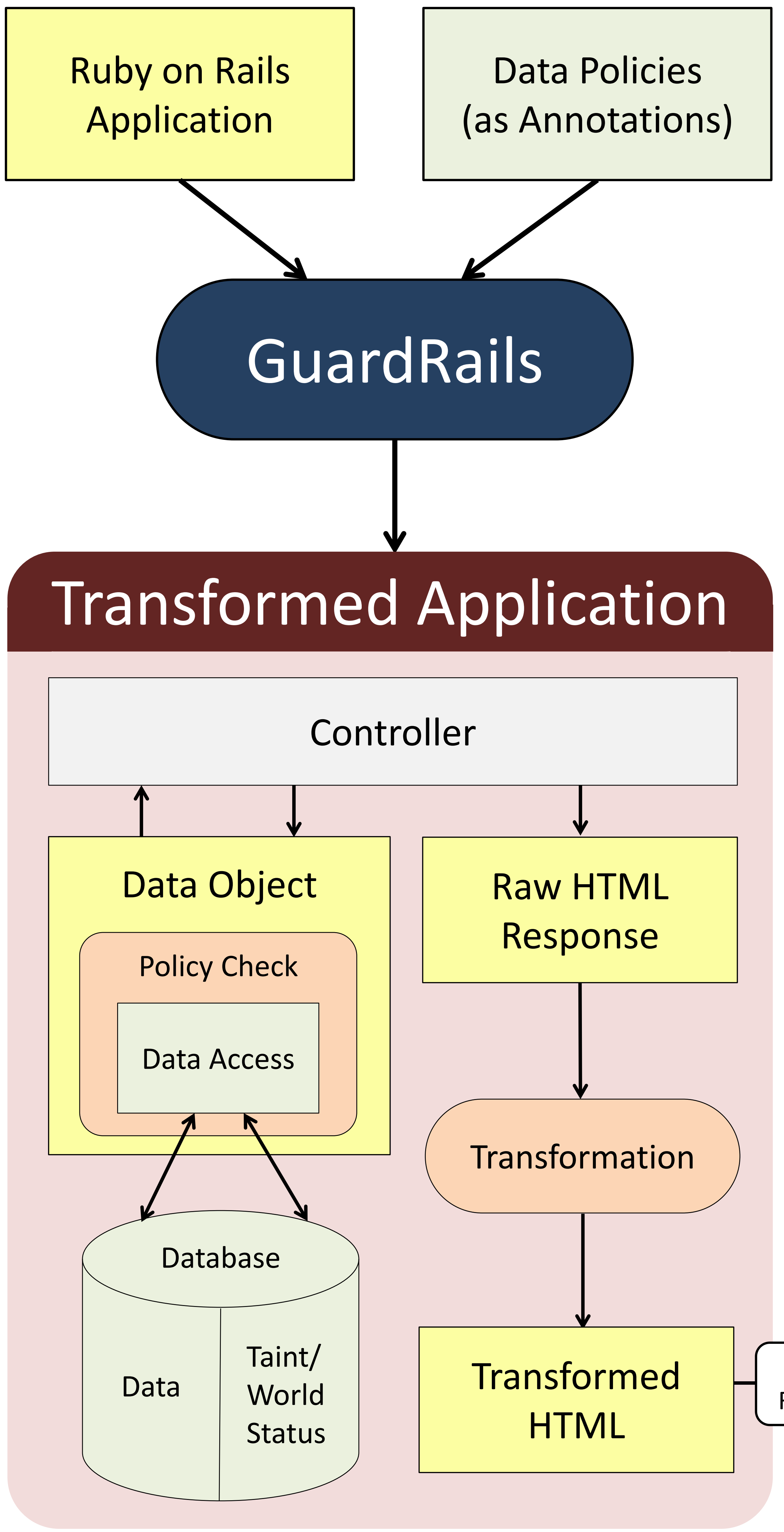
Unifying Data Policies Across the Client and Server

Jonathan Burket, Jenny Cha, Austin DeVinney, Casey Mihaloew, Yuchen Zhou, David Evans

http://guardrails.cs.virginia.edu

Web application security is typically decentralized and *ad hoc*, requiring developers to implement security checks in many different locations. A single missed check can leave an application vulnerable. We explore defining data-centric security policies and propagating them throughout both the client and server.



Privacy Across the Client and Server

Modern web applications often incorporate code from third parties for purposes such as advertising and interacting with social networks. We offer a method to explicitly control what content can be accessed by these third-party scripts by adding annotations to the application code.

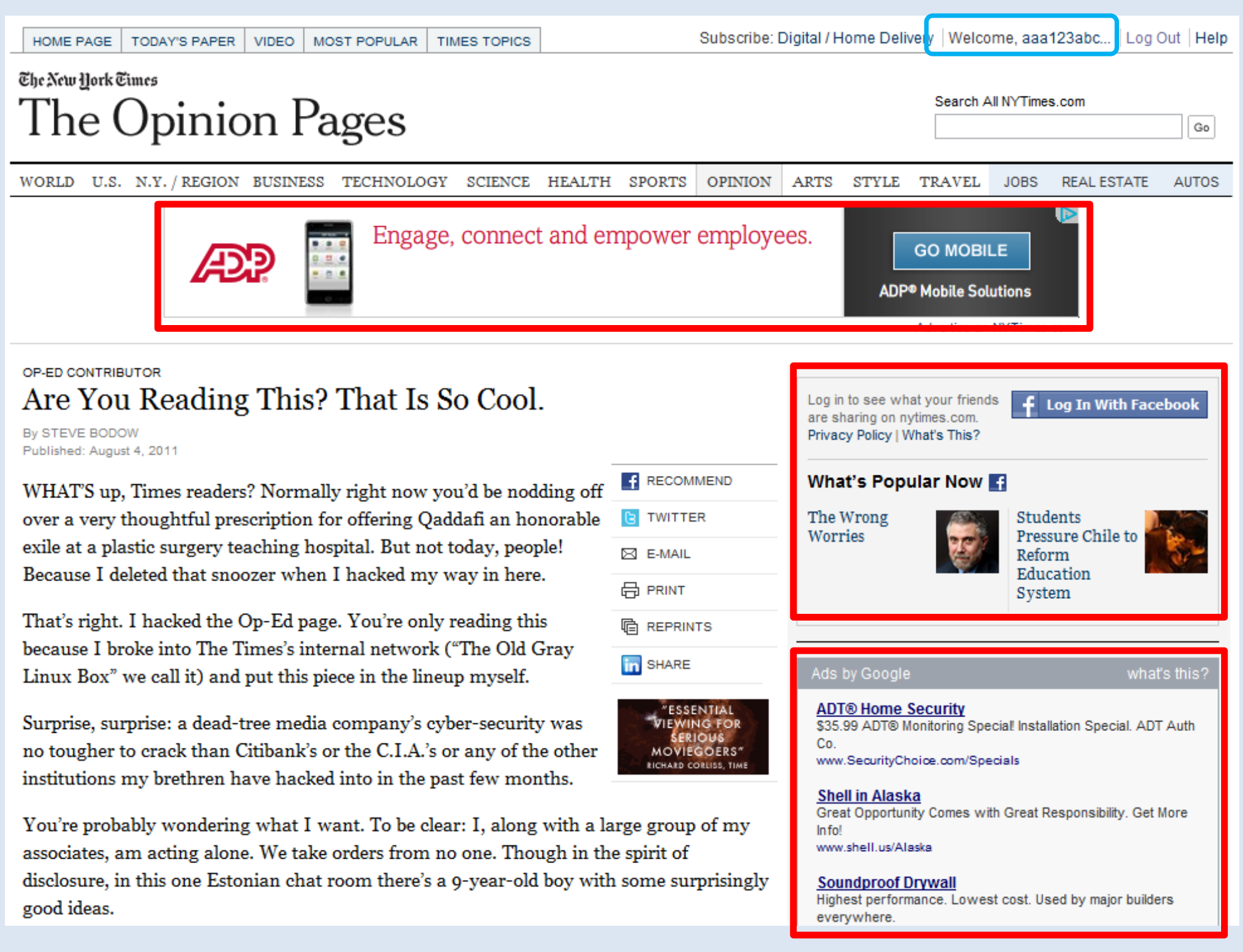
1 Annotate the Data Model

```
# @ read_worlds, :username, :none
class  User < ActiveRecord::Base ...
```

2 GuardRails Marks Sensitive Data in HTML

```
<span RACL="" WACL="">aaa123abc</span>
```

3 Modified Chromium Browser Enforces Script-Access Policies



HOME PAGE | TODAY'S PAPER | VIDEO | MOST POPULAR | TIMES TOPICS — Subscribe: Digital / Home Delivery | Welcome, aaa123abc... | Log Out | Help

The New York Times — The Opinion Pages

Search All NYTimes.com [Go]

WORLD U.S. N.Y. / REGION BUSINESS TECHNOLOGY SCIENCE HEALTH SPORTS OPINION ARTS STYLE TRAVEL JOBS REAL ESTATE AUTOS

ADP — Engage, connect and empower employees. GO MOBILE — ADP® Mobile Solutions

OP-ED CONTRIBUTOR

Are You Reading This? That Is So Cool.

By STEVE BODOW
Published: August 4, 2011

WHAT'S up, Times readers? Normally right now you'd be nodding off over a very thoughtful prescription for offering Qaddafi an honorable exile at a plastic surgery teaching hospital. But not today, people! Because I deleted that snoozer when I hacked my way in here.

That's right. I hacked the Op-Ed page. You're only reading this because I broke into The Times's internal network ("The Old Gray Linux Box" we call it) and put this piece in the lineup myself.

Surprise, surprise: a dead-tree media company's cyber-security was no tougher to crack than Citibank's or the C.I.A.'s or any of the other institutions my brethren have hacked into in the past few months.

You're probably wondering what I want. To be clear: I, along with a large group of my associates, am acting alone. We take orders from no one. Though in the spirit of disclosure, in this one Estonian chat room there's a 9-year-old boy with some surprisingly good ideas.

RECOMMEND | TWITTER | E-MAIL | PRINT | REPRINTS | SHARE

"ESSENTIAL VIEWING FOR SERIOUS MOVIEGOERS" RICHARD CORLISS, TIME

Log in to see what your friends are sharing on nytimes.com. Privacy Policy | What's This? — Log In With Facebook

What's Popular Now — The Wrong Worries — Students Pressure Chile to Reform Education System

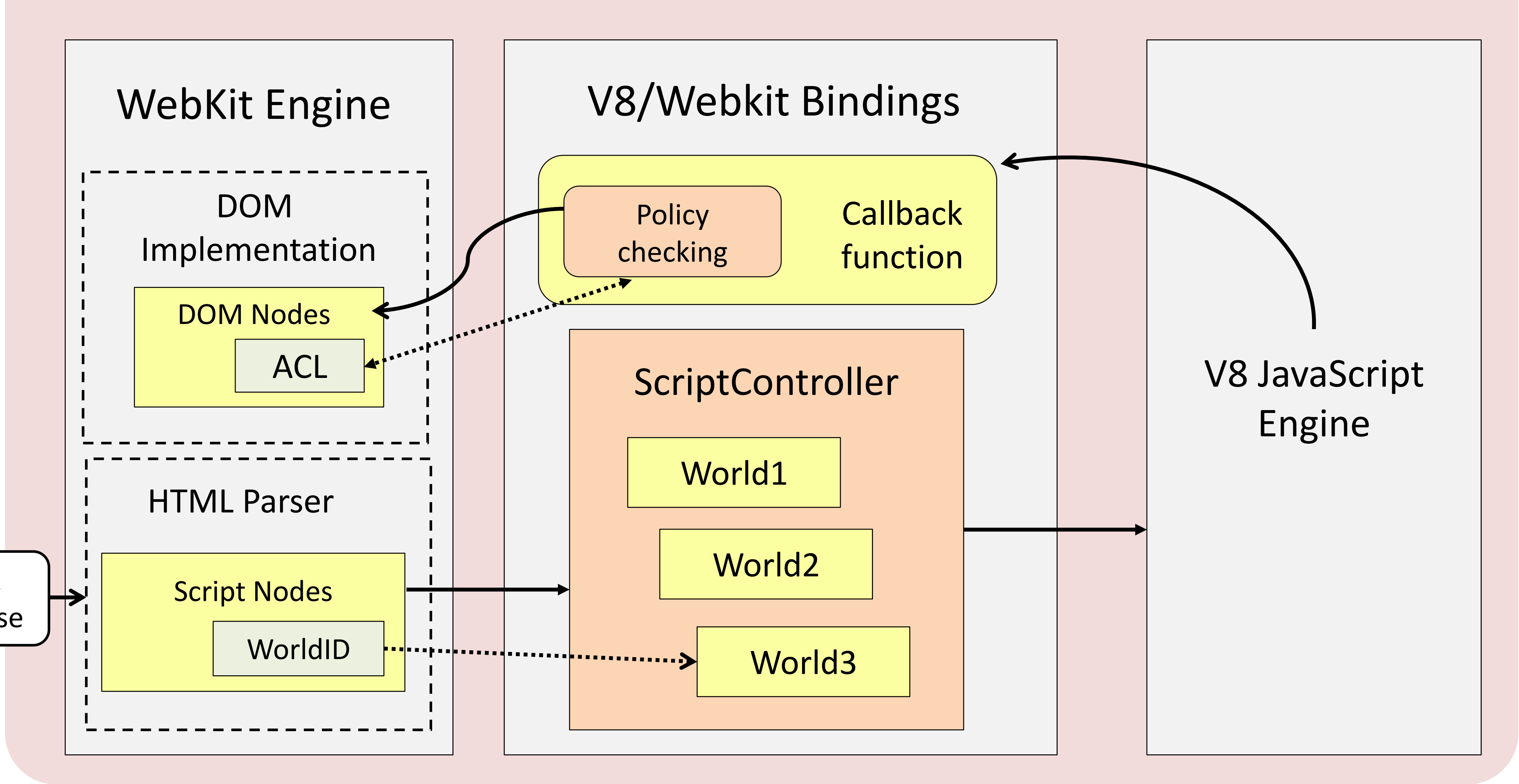
Ads by Google — what's this?

ADT® Home Security — $35.99 ADT® Monitoring Special! Installation Special. ADT Auth Co. www.SecurityChoice.com/Specials

Shell in Alaska — Great Opportunity Comes with Great Responsibility. Get More Info! www.shell.us/Alaska

Soundproof Drywall — Highest performance. Lowest cost. Used by major builders everywhere.

Modified Chromium Architecture



GuardRails Annotations

Annotations let developers specify complex security policies that GuardRails then enforces. Here are some example annotations:

Only friends should be able to see a given user's profile:

```
# @ :read_access, :profile, lambda{|user| self.friends.contains?(user) }
class User...
```

Tags other than links should be removed when the Group's description is used in HTML:

```
# @ :taint, :description, {:HTML => {:DEFAULT => :LinksOnly}}
class Group...
```

An EmailMessage's contents can be read by scripts in *World1* and *World2:*

```
# @ :read_worlds, :contents, ["World1", "World2"]
class EmailMessage...
```

Protecting Content from Scripts

In the modified Chromium, web developers can specify which world a third party script will be executing in by specifying the worldID attribute:

```
<script src="http://somelibrary.com/somelibrary.js" worldId="libraryA"></script>
```

Policies are attached to data using GuardRails and propagated to client side which may look like:

```
Name: University of Virginia<br/>
Description: <span RACL="libraryA, libraryB" WACL="libraryA, libraryB">Professors from
<b RACL="libraryA">Mr. Jefferson's</b> University</span>
```

Only library A can read content inside the <b> tag, but both libraries have full access to other public information.

Jonathan Burket, Patrick Mutchler, Michael Weaver, Muzzammil Zaveri, and David Evans. June 2011. GuardRails: A Data-Centric Web Application Security Framework. In *2nd USENIX Conference on Web Application Development* (WebApps'11).

Yuchen Zhou and David Evans. September 2011. Protecting Private Web Content from Embedded Scripts. In *European Symposium on Research in Computer Security* (ESORICS 2011).

This work is supported by the Air Force Office of Scientific Research through a MURI award.

UNIVERSITY *of* VIRGINIA