David Mortman

CSO-in-Residence, Echelon One, LLC

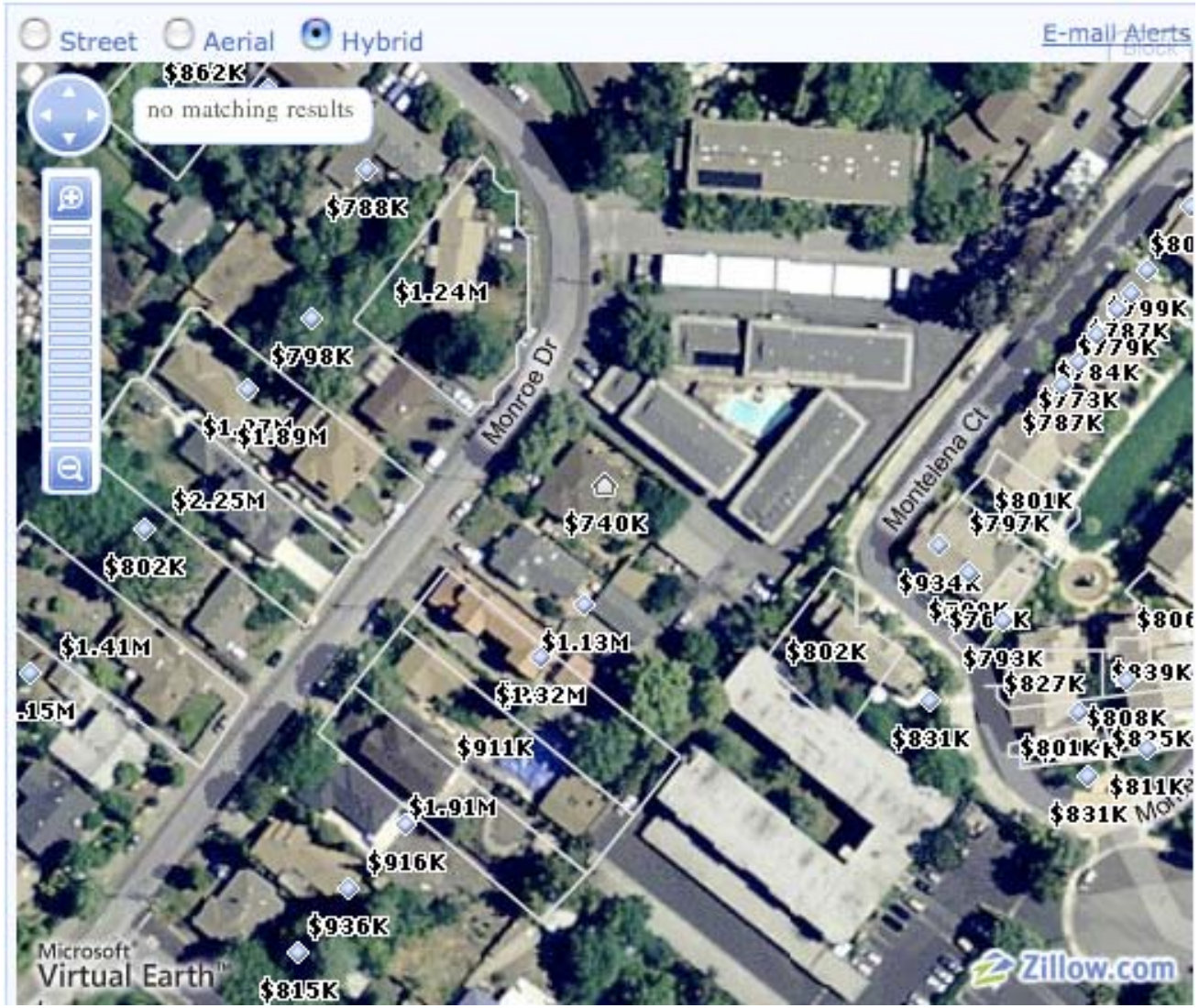
A Tale of 2.0 Webs

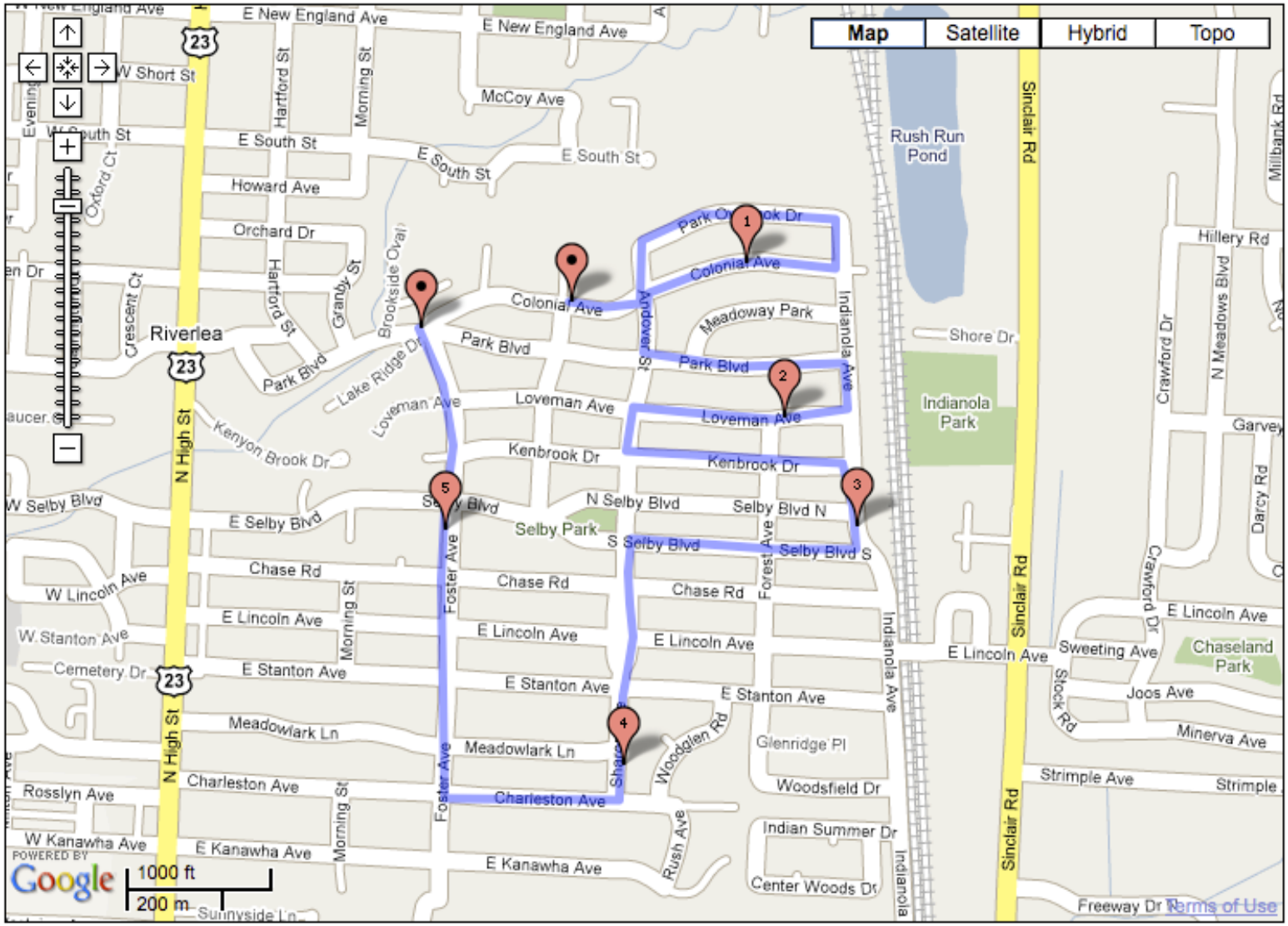
It Was The Best of Times

It Was The Worst of Times

With Apologies to Dickens

It Was The Best of Times


Street
Aerial
Hybrid
E-mail Alerts
no matching results
$862K
$788K
$1.24M
$798K
$1.89M
$2.25M
$740K
$802K
$1.41M
$1.13M
$1.32M
$911K
$1.91M
$916K
$936K
$815K
Monroe Dr
Montelena Ct
$801K
$797K
$934K
$793K
$827K
$808K
$831K
$801K
$811K
$831K
$787K
$773K
$784K
$779K
$787K
$802K
Microsoft Virtual Earth
Zillow.com


Map
Satellite
Hybrid
Topo
E New England Ave
W Short St
E South St
McCoy Ave
Howard Ave
Orchard Dr
Riverlea
Park Blvd
Lake Ridge Dr
Loveman Ave
Kenyon Brook Dr
Kenbrook Dr
W Selby Blvd
E Selby Blvd
N Selby Blvd
S Selby Blvd
Selby Blvd N
Selby Blvd S
Selby Park
Chase Rd
W Lincoln Ave
E Lincoln Ave
W Stanton Ave
Cemetery Dr
E Stanton Ave
Meadowlark Ln
Charleston Ave
Rosslyn Ave
W Kanawha Ave
E Kanawha Ave
Sunnyside Ln
Colonial Ave
Meadoway Park
Shore Dr
Indianola Park
Rush Run Pond
Glenridge Pl
Woodsfield Dr
Indian Summer Dr
Center Woods Dr
Sweeting Ave
Chaseland Park
Joos Ave
Minerva Ave
Strimple Ave
Strimple
Freeway Dr
Hillery Rd
Millbank Rd
N Meadows Blvd
Crawford Dr
Garvey
Darcy Rd
Stock Rd
Oxford Ct
Crescent Ct
Brookside Oval
Granby St
Evening
Hartford St
Morning St
Foster Ave
Forest Ave
Anderson St
Indianola Ave
Woodglen Rd
Rush Ave
Sinclair Rd
N High St
23
1
2
3
4
5
POWERED BY Google
1000 ft
200 m
Terms of Use

It Was The “Worst” of Times

Technical Issues

Cross Site Scripting

Cross Site Request Forgery

SQL Injection

Clickjacking

iFrame Injection

GIFARS

Related Technical Issues

DNS Cache Poisoning

BGP Hijacking

Architecture and Other Issues

Business Logic Flaws

Deep Linking

Data Leakage
Privacy Issues
Identity Theft

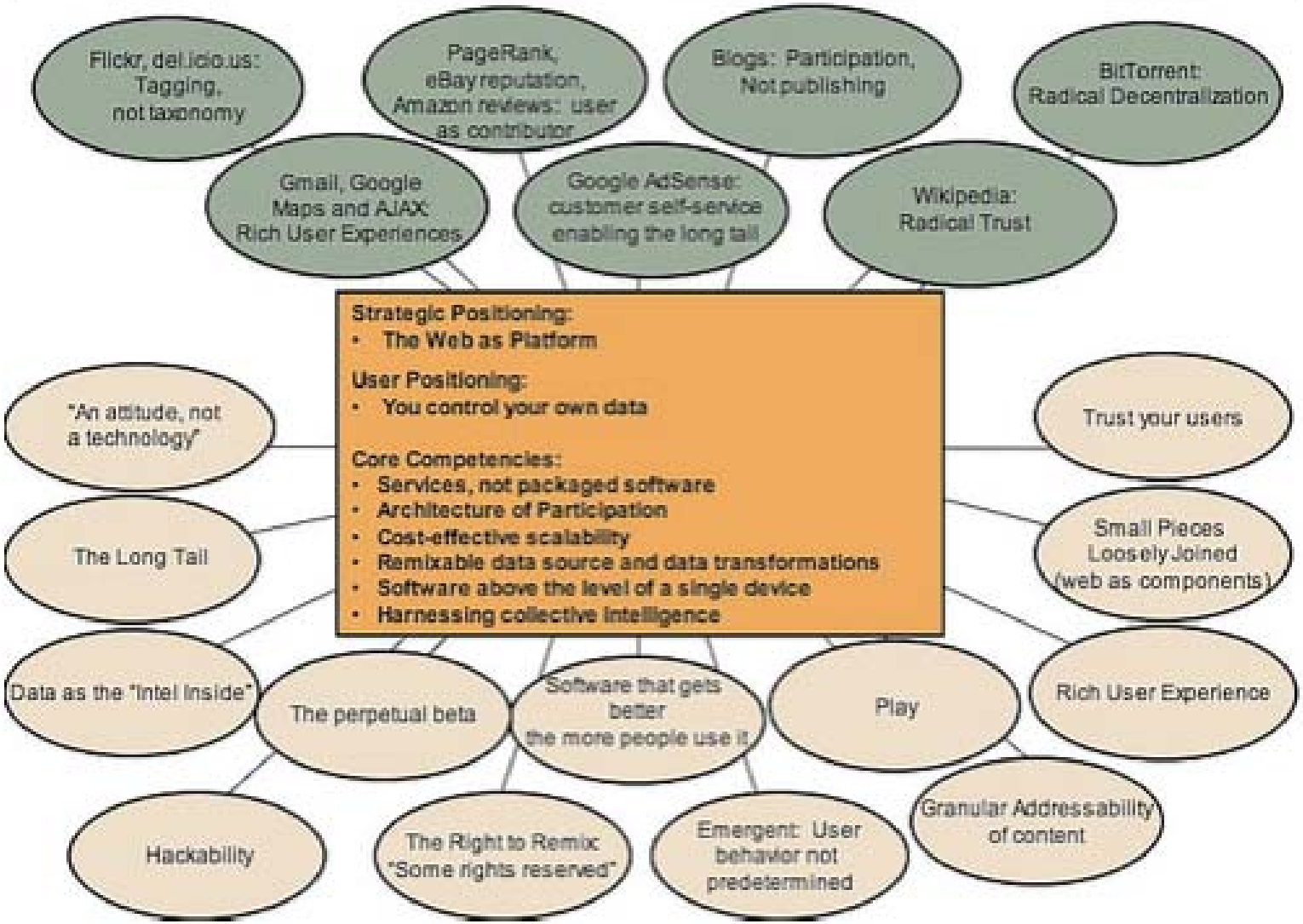
http://1raindrop.typepad.com/

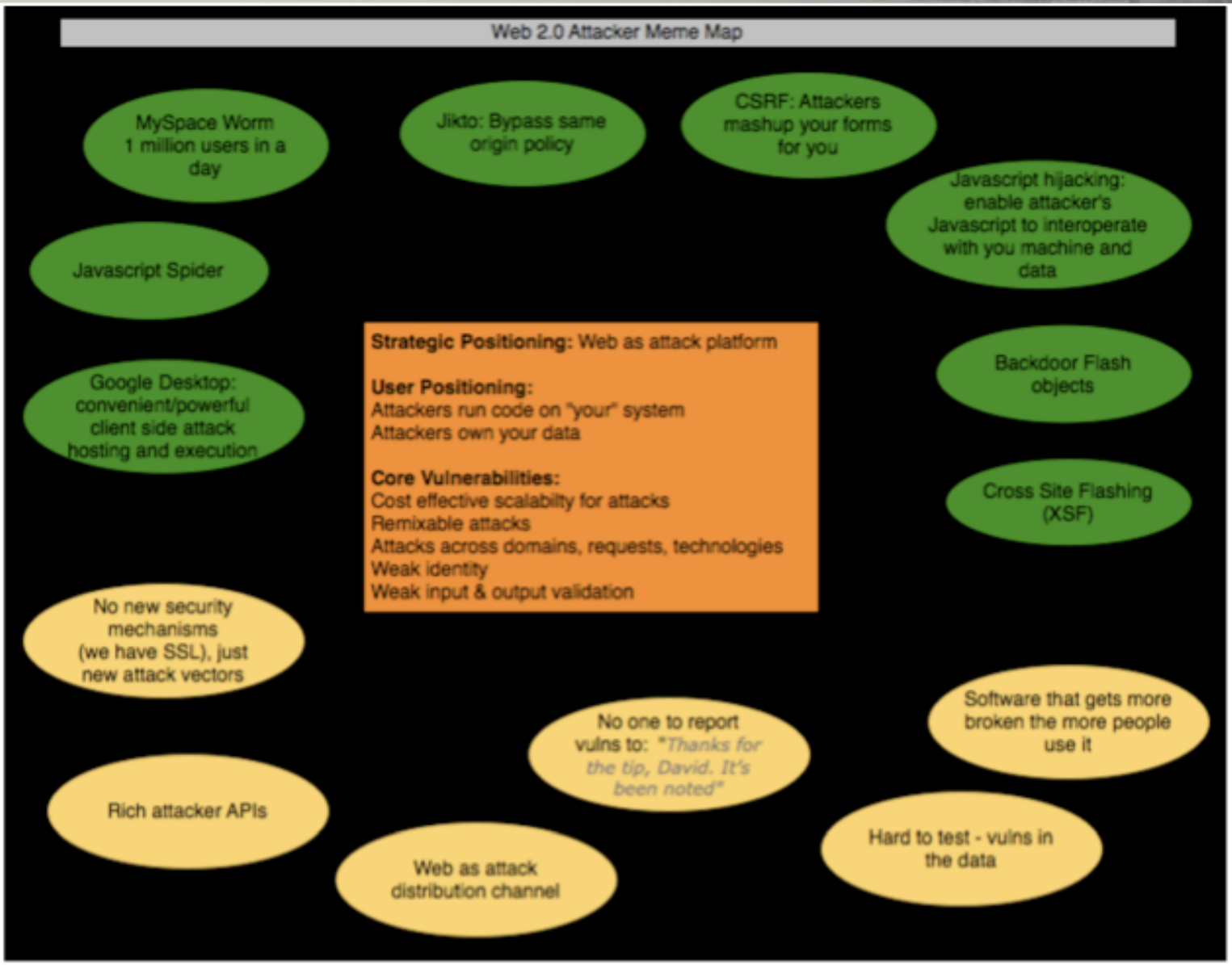
Innovation?

What Innovation?

	Developers	Security
1995	CGI, PERL	Network firewalls, SSL
1997	ASP, JSP	Network firewalls, SSL
1998	EJB, J2EE, DCOM	Network firewalls, SSL
1999	SOAP, XML	Network firewalls, SSL
2001	Rest, SOA	Network firewalls, SSL
2003	Web 2.0	Network firewalls, SSL

Web 2.0 Meme Map




Web 2.0 Attacker Meme Map
MySpace Worm 1 million users in a day
Jikto: Bypass same origin policy
CSRF: Attackers mashup your forms for you
Javascript hijacking: enable attacker's Javascript to interoperate with you machine and data
Javascript Spider
Strategic Positioning: Web as attack platform
User Positioning:
Attackers run code on "your" system
Attackers own your data
Core Vulnerabilities:
Cost effective scalabilty for attacks
Remixable attacks
Attacks across domains, requests, technologies
Weak identity
Weak input & output validation
Backdoor Flash objects
Google Desktop: convenient/powerful client side attack hosting and execution
Cross Site Flashing (XSF)
No new security mechanisms (we have SSL), just new attack vectors
Software that gets more broken the more people use it
No one to report vulns to: "Thanks for the tip, David. It's been noted"
Rich attacker APIs
Hard to test - vulns in the data
Web as attack distribution channel

But....

It Could Be A Lot Worse

Fortunately…

There Are Options

Push Vendors

When will you stop making such crappy software?

When you stop buying it.

Security In The SDLC

SDLC In 8 Slides

Educate

Design

Code

Test

Ship

Update

Books

Threat Modeling

Writing Secure Code

Software Security: Building Security In

Resources

OWASP

NoScript

BugMeNot

AdBlock

http://jeremiahgrossman.blogspot.com

http://ha.ckers.org/blog

http://1raindrop.typepad.com/

Q&A

David Mortman

CSO-in-Residence, Echelon One, LLC

A Tale of 2.0 Webs