



Application Security Tradeoffs

Anoop Reddy
July, 2010
Citrix Systems

OWASP

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

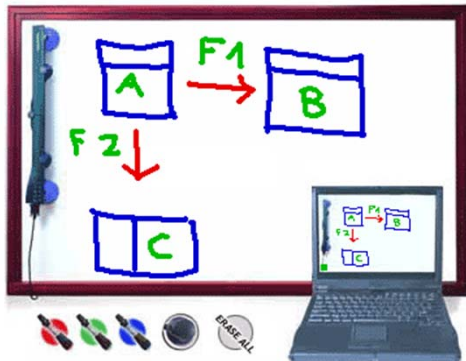
The OWASP Foundation
<http://www.owasp.org>

Security Tradeoff Decisions

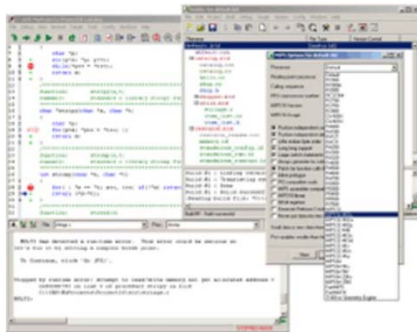
- Explicit security tradeoffs

 Panel discussion at SXSW (Meebo, Facebook etc.)

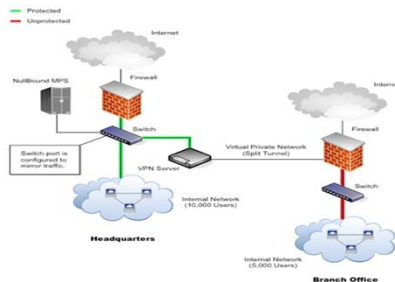
Security Tradeoffs



Design

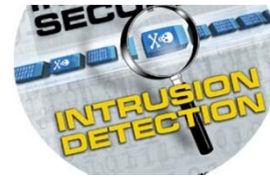
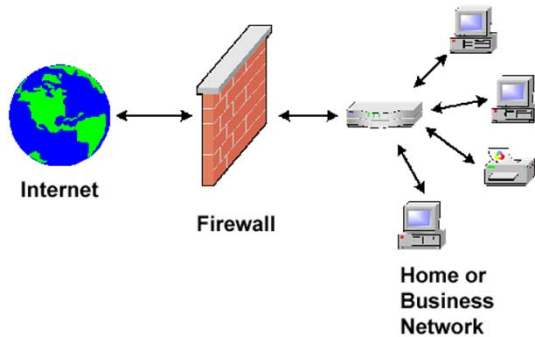


Development



Deployment

Security Deployment Technologies

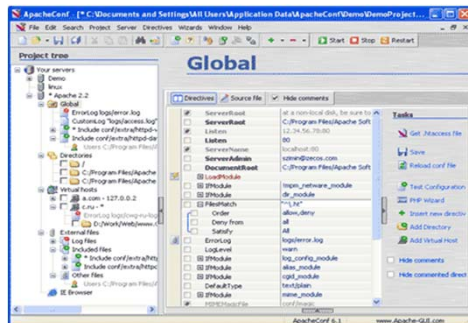


Intrusion Prevention

Web Application
Firewalls

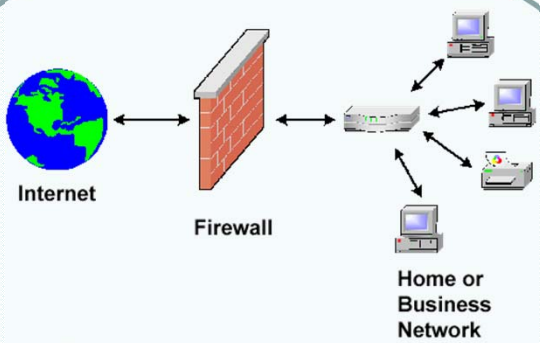


Scanning Tools



OWASP





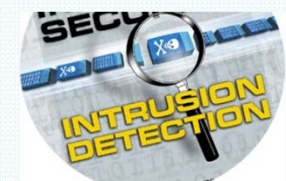
Restricting Access

Intrusion Prevention

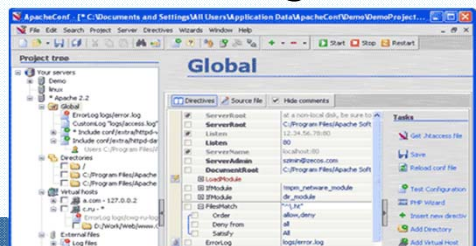


Active and Passive Security Checks

Web Application Firewalls



Scanning Tools
Vulnerability Assessment
and Configuration

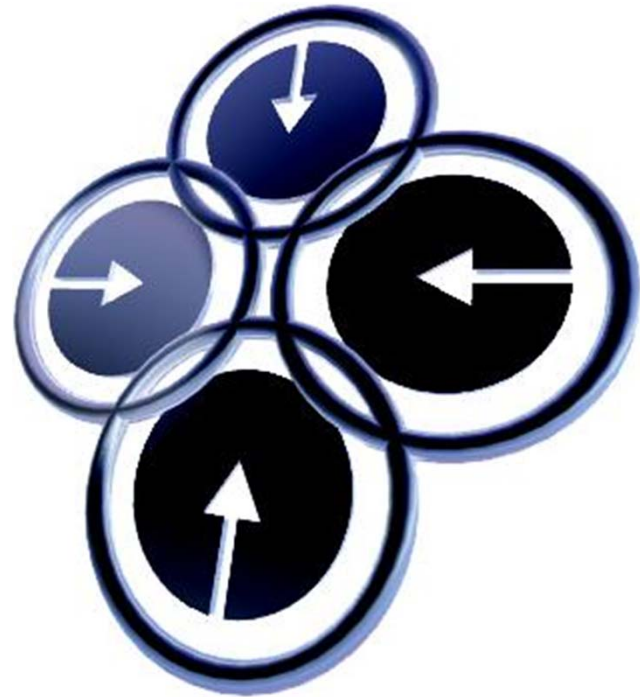


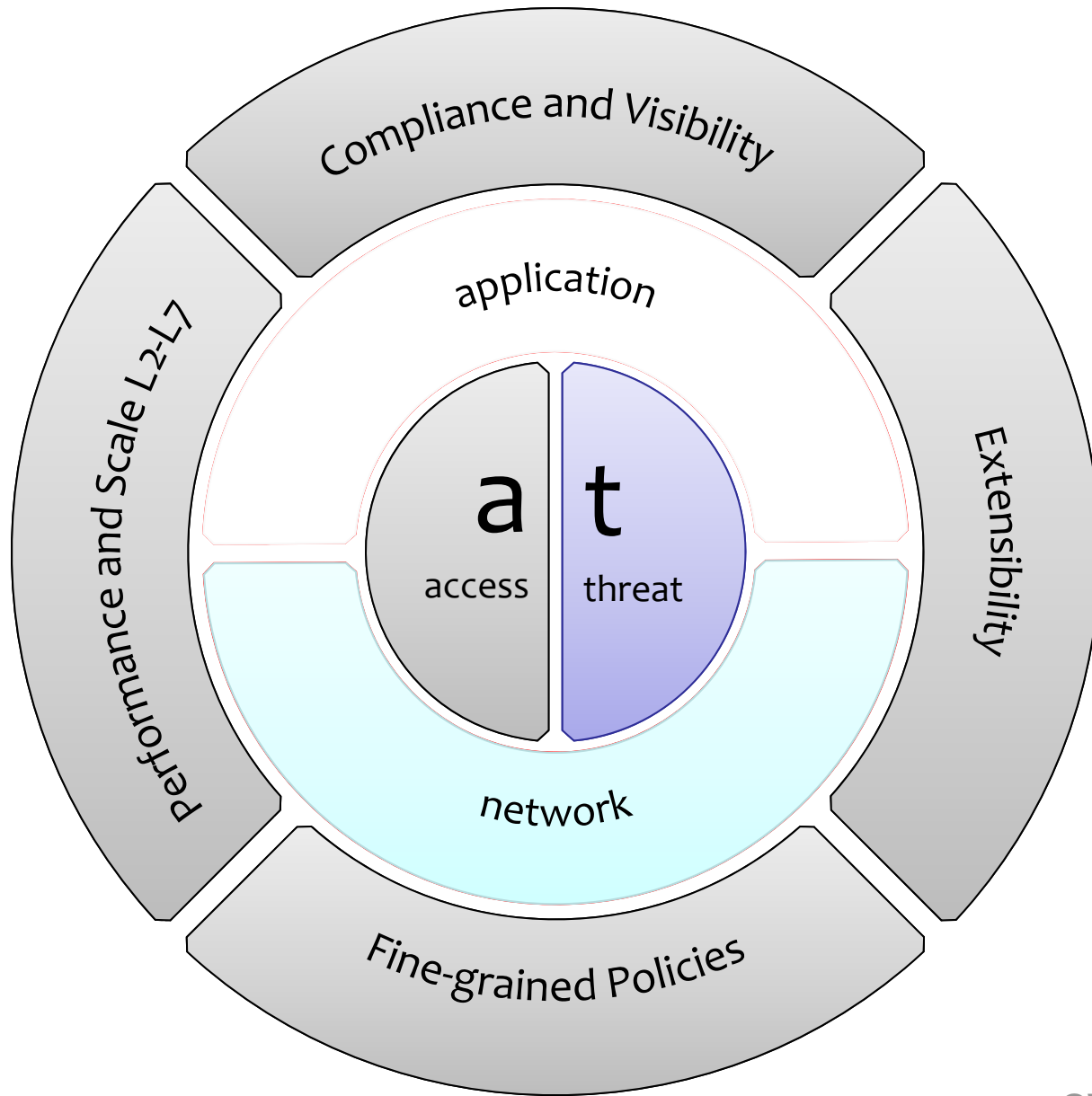
OWASP



Consolidation of Security Technologies

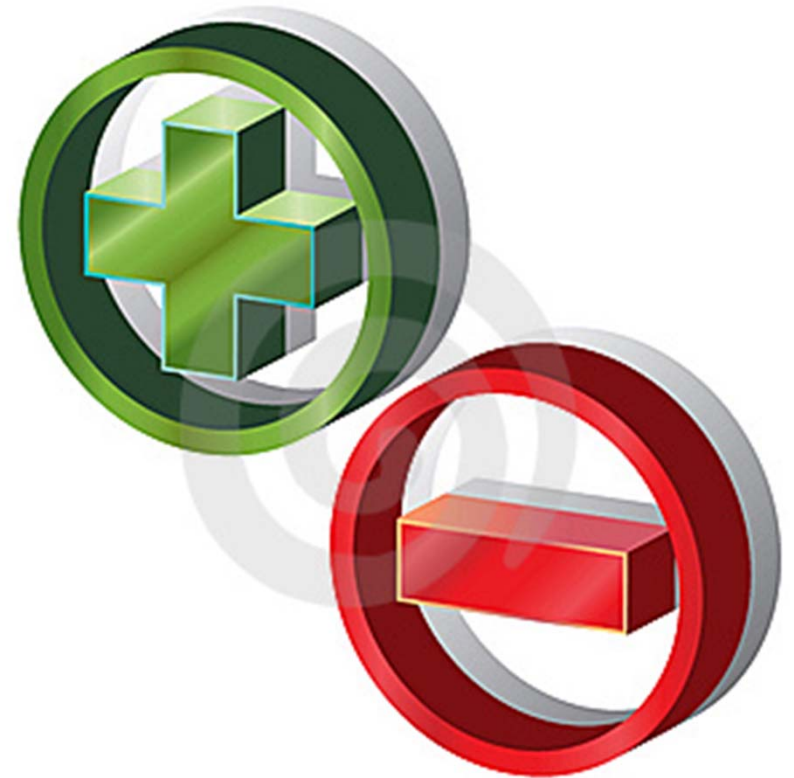
- Does it always makes sense?





Security Models

- Positive Security Model
- Negative Security Model



Negative Security Model

Keep the Back



Positive Security Model

Only allow the good guys in



A magnifying glass with a silver rim and a black handle is positioned over a white document. The document has the words "Case Studies" printed on it. "Case" is in a light green font, and "Studies" is in a light blue font. The magnifying glass is centered over the word "Studies", making it appear larger and more prominent. The background is a solid light blue color.

Case Studies

Restricting URL access

- Block known attacks in URLs
 - ▶ Attack Signatures



BLEEDING-EDGE EXPLOIT Microsoft MHTM...	any	TCP any	mhtml:file:
BLEEDING-EDGE EXPLOIT Cisco Telnet Buf...	any	TCP 23	????????????????a~ %%%%XX
BLEEDING-EDGE DOS Cisco Router HTTP DoS	any	TCP 80	{%%}
BLEEDING-EDGE EXPLOIT Catalyst SSH pr...	any	TCP 22	a%a%a%a%a%a%a%
BLEEDING-EDGE EXPLOIT Catalyst 3500 ar...	any	TCP 80	{exec/show/config
BLEEDING-EDGE EXPLOIT Cisco IOS HTTP ...	any	TCP 80	{error?}
BLEEDING-EDGE DOS Cisco 514 UDP flood ...	any	UDP 514	%%%%XX%%%
BLEEDING-EDGE DOS Catalyst memory lea...	any	TCP 23	AAA[0A]
BLEEDING-EDGE EXPLOIT Cisco %u IDS ev...	any	TCP 80	%u002F
BLEEDING-EDGE EXPLOIT Cisco IOS HTTP ...	any	TCP 80	{TEST?}
BLEEDING-EDGE VIRUS Agobot/Phatbot In...	any	TCP any	221 Goodbye, have a good infection :).[0D 0A]
BLEEDING-EDGE P2P Phatbot Control Con...	any	TCP any	Wonk- [00]#waste[00]
BLEEDING-EDGE DOS SSL Bomb DoS Attempt	any	TCP 443	[16 03 00] [01] [FF]
BLEEDING-EDGE EXPLOIT NII Microsoft AS...	any	TCP 139	[A1 05]#[03 03 01 07]
BLEEDING-EDGE Malware rcprograms	any	TCP 80	update.rcprograms.com
BLEEDING-EDGE Malware Gator Cookie	any	TCP 80	webpdpcookie .gator.com
BLEEDING-EDGE Malware Gator Agent Traffic	any	TCP 80	User-Agent: Gator
BLEEDING-EDGE EXPLOIT CVS server heap...	any	TCP 2401	Entry aaaaaaaaaa



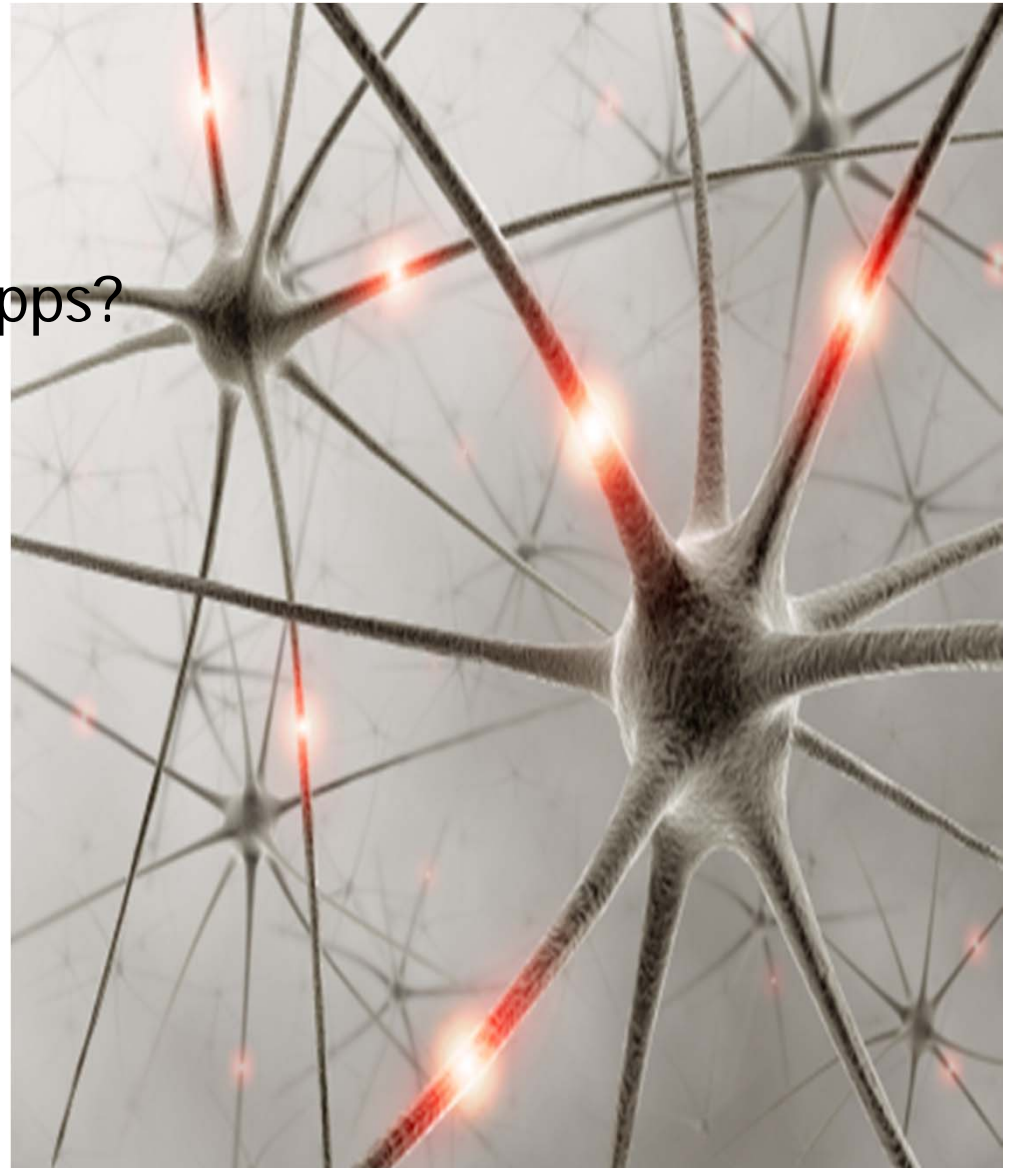
Ease Management by Learning

■ Static Learning

- ▶ Training data
- ▶ What about evolving apps?

■ Adaptive Learning

- ▶ Always learn
- ▶ User customized



The Tradeoffs

Not enough security

vs.

Maintenance Headaches



What actually gets deployed!

- First, I want to get ...



- Signatures no longer sufficient
- Fix only discovered vulnerabilities for now

Form Protections

■ Scalable State Maintenance

* Mandatory Field

1	Label <input type="text"/> Description <input type="text"/>	Type : <input checked="" type="radio"/> Single-line <input type="radio"/> Multi-line <input type="radio"/> Pick List Default Value <input type="text"/> Note: Default value will appear pre-filled in the form
2	Label <input type="text"/> Description <input type="text"/>	Type : <input type="radio"/> Single-line <input checked="" type="radio"/> Multi-line <input type="radio"/> Pick List Default Value <input type="text"/> Note: Default value will appear pre-filled in the form
3	Label <input type="text"/> Description <input type="text"/>	Type : <input type="radio"/> Single-line <input type="radio"/> Multi-line <input checked="" type="radio"/> Pick List Add items to your pick list <input type="text"/> <input type="button" value="Add Item"/> <input type="button" value="Delete"/> <input type="button" value="De-select"/> Note: Selected item is the default value
4	Label <input type="text"/> Description <input type="text"/>	Type : <input checked="" type="radio"/> Single-line <input type="radio"/> Multi-line <input type="radio"/> Pick List Default Value <input type="text"/> Note: Default value will appear pre-filled in the form
5	Label <input type="text"/> Description <input type="text"/>	Type : <input checked="" type="radio"/> Single-line <input type="radio"/> Multi-line <input type="radio"/> Pick List



OWASP

The Open Web Application Security Project

OWASP Top 10 - 2010

The Ten Most Critical Web Application Security Risks

Does this apply to my deployments?

- Need a template specific to my applications!



Know Your Security Tradeoffs!

