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
- Anti-Virus

OWASP
OWASP

Active and Passive Security Checks

Restricting Access

Web Application Firewalls

Intrusion Prevention

Vulnerability Assessment and Configuration

Scanning Tools

Anti-Virus
Consolidation of Security Technologies

Does it always make sense?
Security Models

- Positive Security Model
- Negative Security Model
Negative Security Model

Keep the Bad Guys out
Positive Security Model

Only allow the good guys in
## Restricting URL access

- **Block known attacks in URLs**
  - Attack Signatures

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

- Only allow configured URLs

Matching a URL:

```
/^[https?:\/\/]??
```

...the letters “http”...

...numbers, letters, dots, or hyphens...

...any number...

...a dot...

...two to six...

...letters or dots...

...one or more...

...letters, numbers, underscores, dots, or hyphens...

...zero or more...

...any letter, number, or hyphen...

...and finally the end of the line.
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
Does this apply to my deployments?

- Need a template specific to my applications!
Know Your Security Tradeoffs!