Securing The Application Layer

Joel M Snyder
jms@opus1.com
Senior Partner
Opus One
Agenda

• What does he mean?
• What is the problem?
• What can I do?
All the Real Threats Are At The Application Layer

Because we’ve done such a good job, that’s the only place to attack!

Because app developers have done such a horrible job, that’s a great place to attack!
The Willie Sutton Strategy

• Why do you rob banks?
• “Because that’s where the money is!”
The Willie Sutton Strategy of Computer Crime

• Why do you attack applications?

• “Because that’s where the money is!”

And on the Internet, no one knows you’re there!
The Vector can Change; The Target is the Same
And Attack Applications They Have!

- Web + Spyware: 34%
- Netbios: 43%
- Email: 2%
- Databases: 4%
- Everything Else: 17%

Snort rule coverage, by area, as of 2009Q1, out of 13146 active rules.
Summary:
Applications Are Easy To Attack

- The firewall is open
- The application is poorly secured
- You’re one user out of a million
- The application represents value
The Fix Is Easy!

STOP

Buying
Writing
Adopting
Using

Poorly Secured Applications
OK, I’ll Admit It: The Fix Is Impossible

So let’s make a great leap forward with Joel’s Five Step Program to thwart the International Communist Conspiracy to Sap and Impurify our Precious Bodily Fluids
Five Simple Steps

1. Trust No One
2. Filter Your Traffic
3. Apply Sensible Limits
4. Use Snyder’s Razor
5. Start Paying Attention
Trust No One
Problem 1: Too Many Ports
Solution: Minimize Ports, VPN the Rest

By the way:
this firewall goes **next to** the server, not out at the Internet ingress point
Problem 2: Too Many Applications
If We Assume Applications Have Vulnerabilities...

• Then **fewer applications per server is better**

Remember:
Every Time You Add A New Application To A Server, Chris Hoff Kills A Kitten
**Solution:**
Partition Application Load With Security As a Metric

<table>
<thead>
<tr>
<th></th>
<th>Exchange</th>
<th>DNS Admin</th>
<th>Jan’s Picts</th>
<th>Joomla</th>
<th>Intranet</th>
<th>FTP-to-Web</th>
<th>Meter</th>
<th>tsweb</th>
<th>Web-CMS</th>
<th>What’s Up</th>
<th>.NET Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S2</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>S3</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>S4</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Solution:
Partition Application Load With Security As a Metric

<table>
<thead>
<tr>
<th></th>
<th>Exchange</th>
<th>DNS Admin</th>
<th>Jan’s Picts</th>
<th>Joomla</th>
<th>Intranet</th>
<th>FTP-to-Web</th>
<th>Meter</th>
<th>tsweb</th>
<th>Web-CMS</th>
<th>What’s Up</th>
<th>.NET Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>S2</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>S3</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>S4</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>S5</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
Filter Your Traffic
Many Web Attacks Can Be Blocked
Install an IPS *or*
Enable IPS on your Firewall

This can be a general-purpose IPS, or you may want to look at “application specific” IPS, such as Imperva
A Little Protection Goes A Long Way

How many events in how many hours?

That’d be 4658 events in 6 hours, ma’am.
Yes, an IPS Only Blocks Known Threats

• But your applications are full of vulnerabilities you don’t know about (and maybe can’t fix!)

When you know the game is fixed against you, it’s time to bring loaded dice.
Apply Sensible Limits
Clearly, Some People Are Not Paying Attention Very Well

7 January 2009, 09:46

Twitter hack explained by hacker - News - heise Security UK

The personal blog of a well-known company announcing that a 12-year-old kid has gained access to a celebrity's Twitter account on a bruteforce dictionary attack. An 18-year-old student reportedly used a password-guessing program to get into the account of a Twitter employee (see story). From there, the teenager hijacked the accounts of President-elect Barack Obama, Britney Spears, Fox News and 30 other Twitter users.
Rate Based Limits Are Easy in Many Firewalls
Rate Based Limits are Easy in Many Directory Servers

Sun Java System Directory Server Enterprise Edition 6.0 Reference

How Directory Server Provides Authentication

Authentication is the process of confirming an identity. In network interactions, authentication involves the confident identification of one party by another party. Network interactions typically take place between a client, such as browser software running on a personal computer, and a server, such as the software and hardware used to host a Web site. Client authentication refers to the confident identification of a client by a server; server authentication refers to the confident identification of a server by a client.

Global Account Lockout

Depending on the password policy settings, a client account can be locked out of an account when the number of failed bind attempts exceeds the number of allowed attempts. In a replicated topology, the client is locked out of all instances of Directory Server, not just the instance to which the client was attempting to bind. This feature is called global account lockout.

In versions of Directory Server prior to Directory Server 6, account lockout was based on integer counters. By default, these counters were not replicated.

In this version of the product, bind failures are recorded by using timestamps. By default, the timestamps are replicated, and prioritized replication is used to replicate updates to the lockout data that are caused by failed bind requests.
Rate Limits Are Even Easy in Web Servers
What’s My Point?

Hackers are up to their old tricks.

Application Developers have forgotten the old tricks (if they ever knew them).

You can block many of the old tricks by simply instrumenting the services around the application.
Sensible Limits Include...

- CPU Time
- Storage
- Bandwidth
- Connection Count
- Transactions/Second
- Transactions/IP
- Auth/Sec.
- Failed Auth/Sec.
Use Snyder’s Razor
Occam’s Razor

“All other things being equal, the simplest solution is the best.”

- (as stated by Maimonides)
Snyder’s Razor

“All other things being equal, choose the more secure option.”
A Simple Example: Which is More Secure?

Hash Algorithms

- MD-5
- SHA-1
- SHA-2
Thus, By Snyder’s Razor
Ignore Snyder’s Razor and ...

Researchers Use PlayStation Cluster to Forge a Web Skeleton Key

A powerful digital certificate that can be used to forge the identity of any website on the internet is in the hands of in international band of security researchers, thanks to a sophisticated attack on the ailing MD5 hash algorithm, a

In 2004 and 2007, cryptographers published research showing that the once-common MD5 hash function suffers weaknesses that could allow attackers to create these "collisions." Since then, most certificate authorities have moved to more secure hashes. But in an automated survey earlier this year, the researchers presenting in Berlin say they discovered a weak link at Verisign-owned RapidSSL, which was still signing certificates using MD5. Out of 38,000 website certificates the team collected, 9,485 were signed using MD5, and 97% of those were issued by RapidSSL.

At issue is the crypto technology used to ensure visitors to Amazon.com, for example, are actually connected to the online retailer and not to a fake site erected by a fraudster. That assurance comes from a digital certificate that's vouched for and digitally signed by a trusted authority like Verisign. The certificate is transmitted to a user's browser and automatically verified during SSL connections -- the high-security web links heralded by a locked-paddock icon in the browser.
Look At Your Security Profile

• Have you selected the most secure alternatives?
  • Certificates
  • Passwords & password lifetimes (SA?)
  • Crypto versus non-Crypto
  • Access Lists

• If not, fix them!
Start Paying Attention

What we say to dogs

Okay, Ginger! I've had it! You stay out of the garbage! Understand, Ginger? Stay out of the garbage, or else!

What they hear

Blah blah GINGER. Blah, blah, blah, blah, blah, blah, blah, blah
I’m running out of time, so...

• You’ve got logs, right?

• Maybe you should look at them once in a while

• Computers are good at this

‘nuff said?
Five Simple Steps

1. Trust No One
2. Filter Your Traffic
3. Apply Sensible Limits
4. Use Snyder’s Razor
5. Start Paying Attention
Thanks!

Joel M Snyder
jms@opus1.com
Senior Partner
Opus One