Custom Intrusion Detection Techniques for Monitoring Web Applications

Matthew Olney
Sourcefire VRT
molney@sourcefire.com

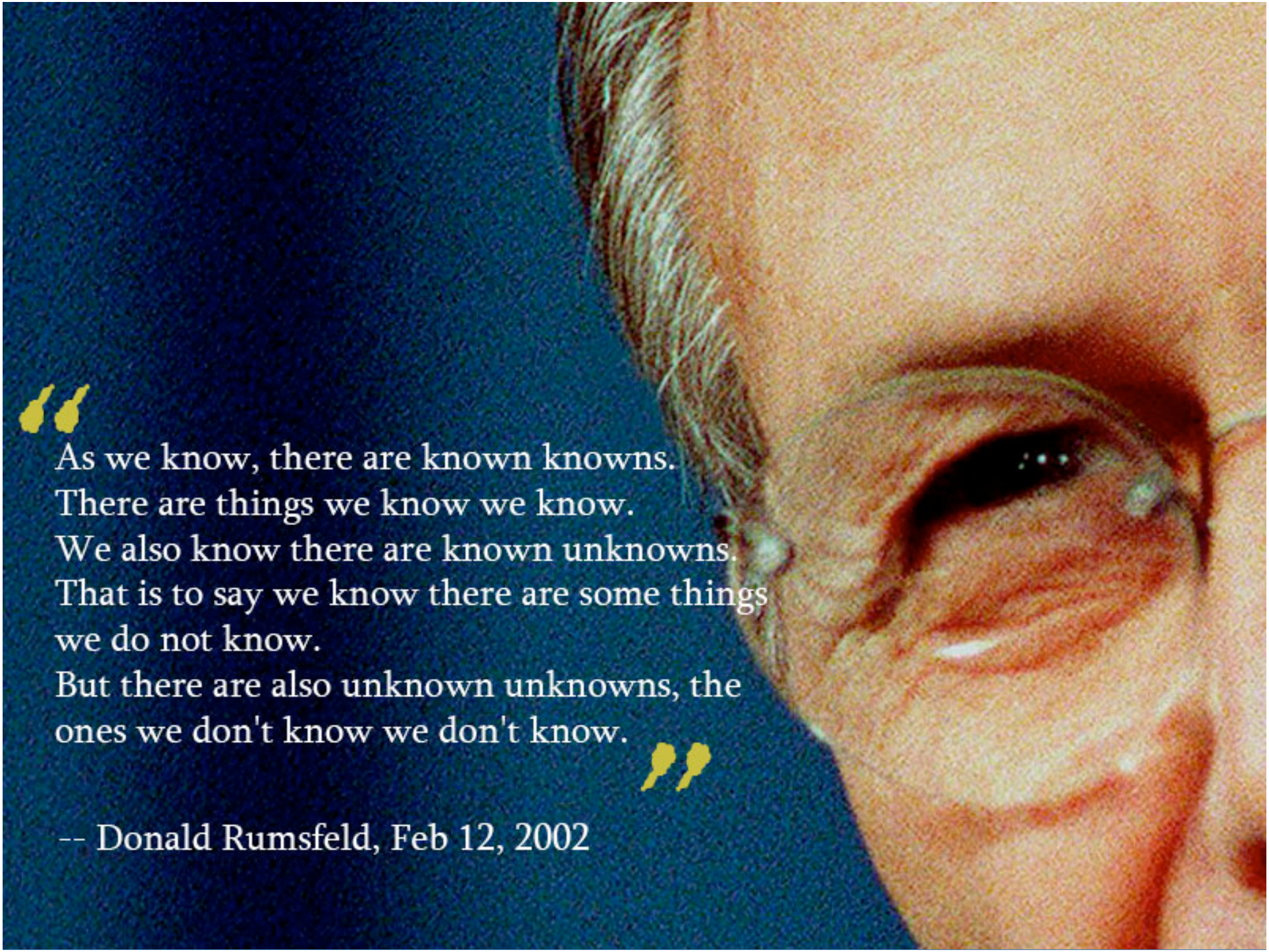
AppSec DC

November 13, 2009

The OWASP Foundation

http://www.owasp.org

GIVE YOUR ANALYST A CHANCE


"As we know, there are known knowns.
There are things we know we know.
We also know there are known unknowns.
That is to say we know there are some things
we do not know.
But there are also unknown unknowns, the
ones we don't know we don't know."
-- Donald Rumsfeld, Feb 12, 2002

The attacker holds a major information advantage

…but that makes the small advantages we do have that much more important.

Part One:
Signature Based Detection

alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:”Jesus Christ it’s a lion GET IN THE CAR”; content:”LION”; nocase; classtype: attempted-bite-your-head; sid: 1;)

But the VRT doesn't know…

your network,
your systems,
your applications

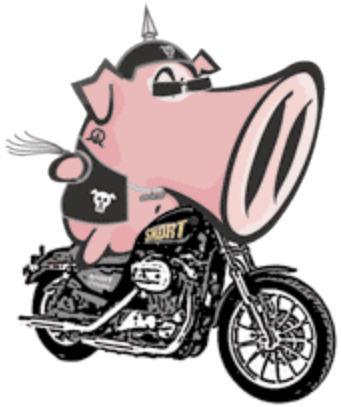
Maybe, just maybe, you do.

SNORT – The Open Source Intrusion Detection System

Signature based detection

Frag & Stream Reassembly

Substantial HTTP preprocessing



Multiple protocol decoding

http://www.snort.org

Matt's 30 Second OWASP Rule Writing Class

Part 1:
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"LOCAL #{Message}"; flow: to_server, established;

Part 2:
uricontent:"#{SecretSauce}"; nocase;

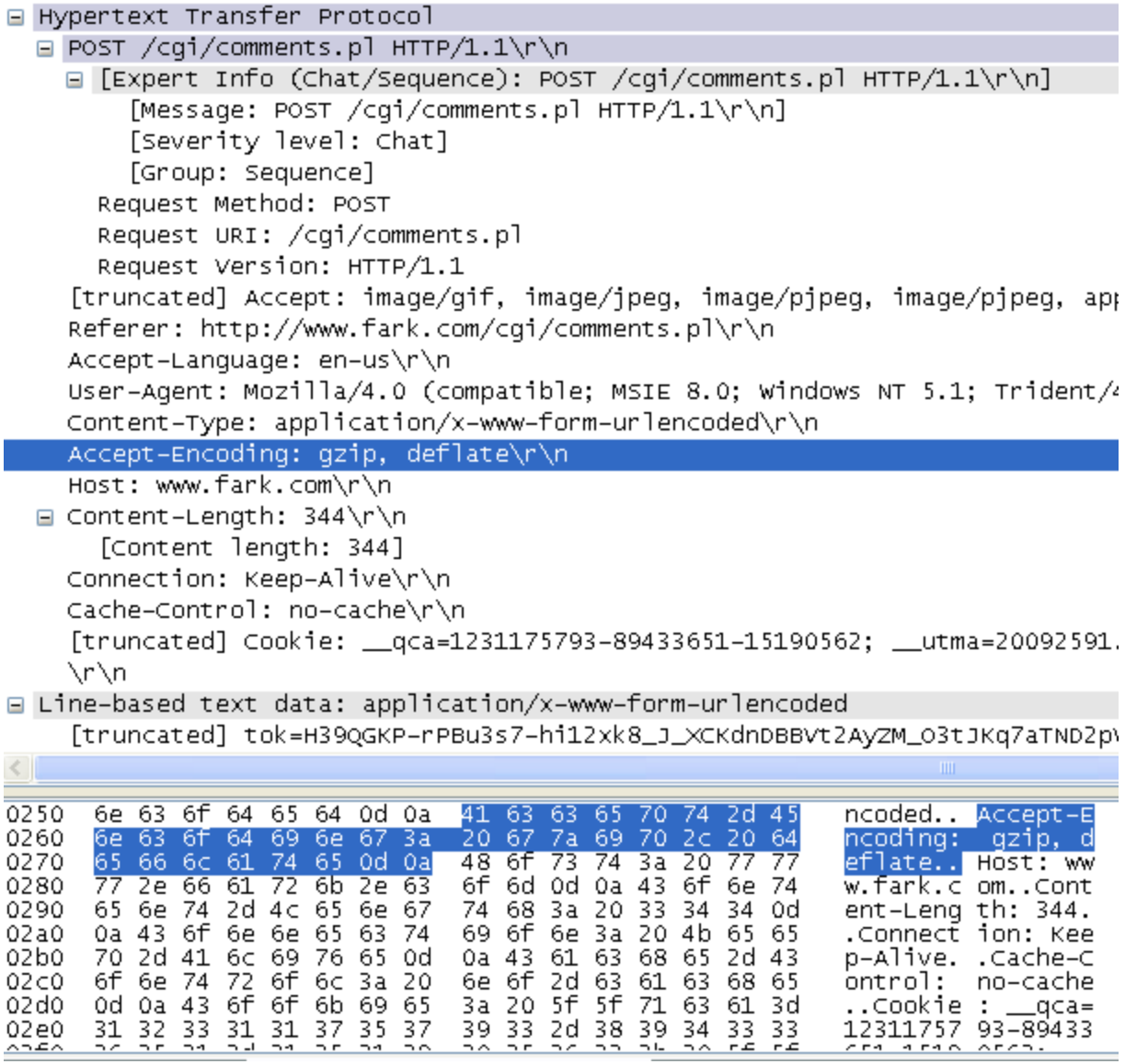
Part 3:
class-type: attempted-admin; sid: #{UniqueLocalSID};)

For Example:

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"LOCAL Admin page access attempt"; flow: to_server, established; uricontent:"admin"; nocase; class-type:attempted-admin; sid: 42098729;)

WIRESHARK:

The Lazy Rule-Writer's Friend



i.e.

(or is it e.g.)?

```
POST /cgi/comments.pl HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): POST /cgi/comments.pl HTTP/1.1\r\n]
     [Message: POST /cgi/comments.pl HTTP/1.1\r\n]
     [Severity level: Chat]
     [Group: Sequence]
   Request Method: POST
   Request URI: /cgi/comments.pl
   Request Version: HTTP/1.1
 [truncated] Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, ap
 Referer: http://www.fark.com/cgi/comments.pl\r\n
 Accept-Language: en-us\r\n
 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/
 Content-Type: application/x-www-form-urlencoded\r\n
 Accept-Encoding: gzip, deflate\r\n
 Host: www.fark.com\r\n
 Content-Length: 344\r\n
   [Content length: 344]
 Connection: Keep-Alive\r\n
 Cache-Control: no-cache\r\n
 [truncated] Cookie: __qca=1231175793-89433651-15190562; __utma=20092591
 \r\n
Line-based text data: application/x-www-form-urlencoded
 [truncated] tok=H39QGKP-rPBu3s7-hi12xk8_J_XCKdnDBBVt2AyZM_O3tJKq7aTND2p
```

```
30  2a 2f 2a 0d 0a 52 65 66  65 72 65 72 3a 20 68 74   */*..Ref erer: ht
40  74 70 3a 2f 2f 77 77 77  2e 66 61 72 6b 2e 63 6f   tp://www .fark.co
50  6d 2f 63 67 69 2f 63 6f  6d 6d 65 6e 74 73 2e 70   m/cgi/co mments.p
60  6c 0d 0a 41 63 63 65 70  74 2d 4c 61 6e 67 75 61   l..Accep t-Langua
```

HTTP_INSPECT

- If you're going to inspect http, it should be on.
- Already does some anomaly detection:
  - Directory traversal
  - Double decoding
  - Oversize URI Requests
  - Oversize chunk encoding
  - Oversize header size
- Check out the http_inspect config
- Read the README.http_inspect document (seriously)
- Remember to configure it to monitor any ports that handle HTTP traffic (80, 8080, custom web management consoles, etc…)

TEST YOUR RULES

(and find some more samples at http://vrt-sourcefire.blogspot.com/)

Where to find Snort help:

Snort-Users mailing list:
https://lists.sourceforge.net/lists/listinfo/snort-users

Snort-Sigs mailing list:
https://lists.sourceforge.net/lists/listinfo/snort-sigs

Webcasts (Writing Effective Rules Parts I and II):
http://www.sourcefire.com/resources/snort-webcast-access

IRC:
#snort on freenode

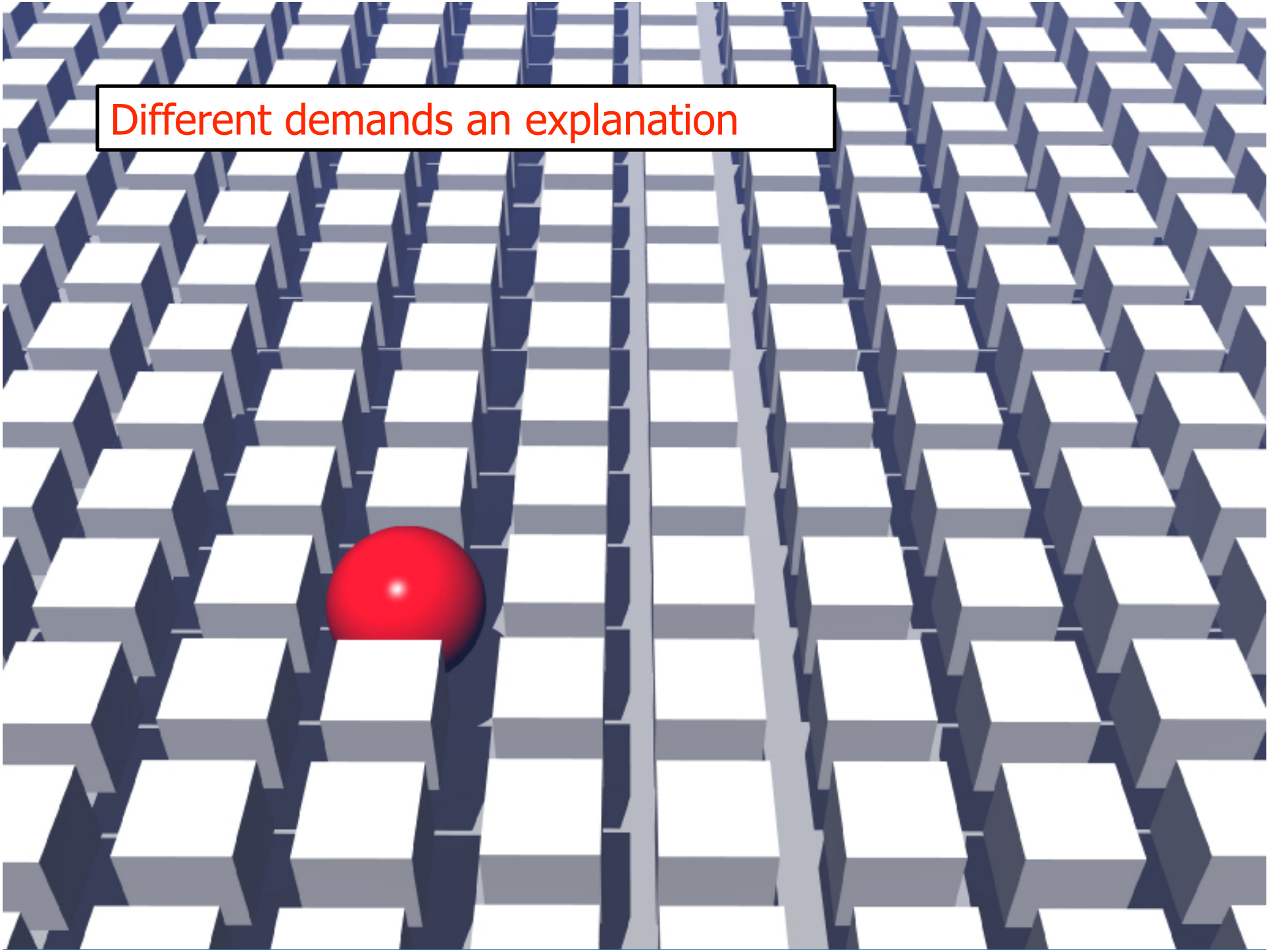
VRT Blog:
http://vrt-sourcefire.blogspot.com/

Twitter:
http://twitter.com/vrt_sourcefire

Your code and application flow defines how the client should request information.

Abuse that fact to "give your analysts a chance" at finding a problem.

Part Two:
Anomaly Based Detection


Different demands an explanation

Netflow:

The Instant WTF Generation Specialist

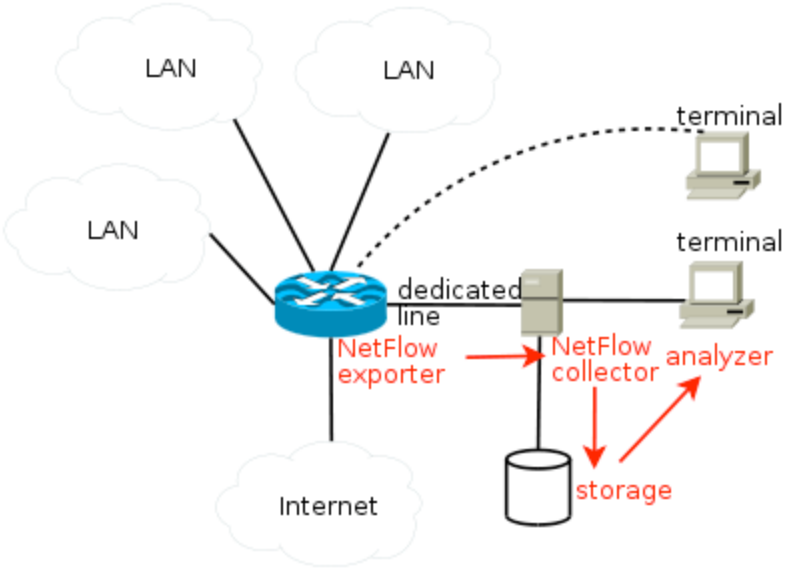
Analysis of Network Flow Statistics

For each network conversation we get the following data:

Source and destination IP address and ports
Total number of packets
Total number of layer 4 bytes
IP protocol number

Individually the information is mildly interesting. But within the context of all other data at that moment, or all other data ever gathered, individual flows can become very interesting.

Typically, you'll have to play nice with the router guys:



A simple top talker chart (by Total Octets):

Source IP	Destination IP	Total Flows	Total Octets	Total Packets
10.4.12.226	68.177.102.20	7	1252024	10413
10.4.12.60	10.4.128.99	10136	624726	10136
10.4.12.226	216.34.181.48	5167	421623	5310
10.4.12.60	216.34.181.48	4891	397892	5024
10.4.12.201	68.177.102.20	4437	358588	4673

Tools Exists to Present the Data in Different Forms:

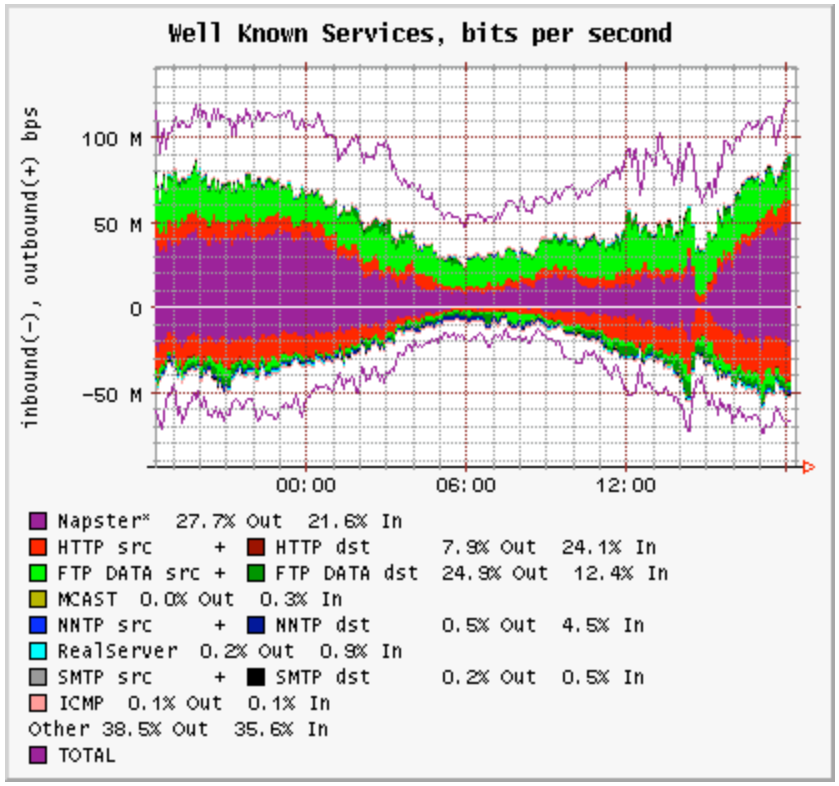


Image of FlowScan Output
Retrieved from www.caida.org 9/25/2009

```
# recn: ip-
port,flows,octets,packets,duration
0,2928,46660002,94312,1517422058
11,186,435224,1076,1383130
20,8,299832820,332792,106660
21,88,2889118,40626,2332797
22,1426,63886472,106367,32555957
23,13,38226,744,841922
25,9890,58946406,175872,13960396
7
42,1,1908,4,32
43,8713,7946017,41760,153687005
53,97353,52755666,427045,1500176
086
# stop, hit record limit.
```

Flow-Tools Suite
Flow-report output

Things to Look For:

- Service detection
- Statistical deviation from the norm
- Connections to unexpected networks
- Local Outliers (top Talker)
- External Outliers (Top Listener)
- Any condition that makes your brow furrow.

Bonus: Encrypted Traffic Doesn't Affect Netflow

Different demands an explanation

Examining an unexplained outlier may be the "break" that gives you a chance to catch the bad guy.

Some Netflow Resources

Flow Tools (PERL folks go here)
http://www.splintered.net/sw/flow-tools/

Cisco's Netflow Site
http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html

Collection of Netflow Analysis Tools
http://www.networkuptime.com/tools/netflow/

Caida's Flowscan Netflow Visualization Tool
http://www.caida.org/tools/utilities/flowscan/

Questions?